データセンター セキュリティ ガイドブック

2017 年版

日本データセンター協会

Japan Data Center Council

はじめに

「データセンター セキュリティ ガイドブック(2017 年版)」発行に寄せて

現在、我が国の掲げている今後の社会の方向性に Society5.0 があります。Society5.0 は、「狩猟」「農耕」「工業」「情報」に次ぐ第５の新たな社会のコンセプトであり、様々な技術や産業がサイバー空間を媒介としてつながることにより価値を創造する社会として展望されています。そして、この Society5.0 を実現する手段として、IoT(Internet of Things)/ ビッグデータ/AI(Artificial Intelligence)/ロボット等の活用が求められています。2020 年には 300 億個以上[1]になるとも言われている IoT デバイスは、フィジカル空間のさまざまな情報をサイバー空間に展開し、ビッグデータとして蓄積しています。そのビッグデータは、AI により学習され、その学習による解析結果がロボットや IoT デバイスといったアクチュエータを通じてフィジカル空間へフィードバックされていきます。これらの様々なデータの蓄積・学習・解析などの処理をおこなう場所がデータセンターです。

Society5.0 では、このようなフィジカル空間とサイバー空間の相互作用、すなわちサイバーフィジカルシステムが、さまざまな分野において活用されることが想定されています[2]。この Society5.0 におけるデータセンターは、従来のサイバー空間のインフラとしての役割だけでなく、フィジカル空間を含めた「社会の重要インフラ」としての役目を果たしていくことになります。

我々、日本データセンター協会は、このような「社会の重要インフラ」としての役割をデータセンターが担うために、それには相応しいセキュリティが求められていることを認識しています。そして、この「社会の重要インフラ」としての役割を果たすべく、近年の多くのデータセンターが提供するサービスでは、その企画・設計時点から様々なセキュリティ要件を取りこむ「セキュリティ・バイ・デザイン」が取り組まれています。

本ガイドブックは読者に「セキュリティ・バイ・デザイン」の観点からデータセンターのセキュリティを理解し、読者自身の構築するシステムにおいて「セキュリティ・バイ・デザイン」を実現できるように、「建物」「設備・システム」そして「運用」についてデータセンターのセキュリティに関する様々な情報を網羅的に扱っています。

本ガイドブックがデータセンターの利用者と事業者の双方において、データセンターのセキュリティに関する理解を深めることに活用され、データセンターが真に IT 立国の基盤を支える「社会の重要インフラ」として活用されることの一助となれば幸いです

日本データセンター協会
セキュリティワーキンググループ一同

1： http://www.soumu.go.jp/johotsusintokei/whitepaper/h28.html 参照
2： http://www.jeita.or.jp/cps/about/ 参照

目次

コラム目次

第１章　本ガイドブックの概要

この章では、「データセンターセキュリティガイドブック」(以下、本ガイドブック)を作成した背景、意図、想定する読者を説明した後、各章の概要、全体像の要約（エグゼクティブ・サマリー）を記述します。

1.1 本ガイドブック作成の背景

この節では、本ガイドブックで扱うデータセンターについてのイントロダクションと、本ガイドブック作成の背景、意図を紹介します。

1.1.1 データセンターとは

データセンターとは、様々な情報通信機器（サーバー、ネットワーク機器、ストレージ等）を設置・運用することに特化した建物と設備の総称と、その建物と設備を利用して行われるサービスを意味します。データセンターには下記のような特徴があります。

建物：

災害時にもサービスの提供に極力支障が出ないように建物自体が耐震構造、免震構造となっています。また、構内で火災が発生した場合にも設置されている機器に損傷を与えないよう、通常のスプリンクラーではなく不活性ガスまたはハロゲンガスによる消火設備を持っています。

電源：

電源供給の安定化のため、複数の受電系統と変電設備を持ち、また、商用電源供給が途絶えた場合に備え UPS（無停電電源装置）と自家発電装置等を備えています。

空調：

集約された情報通信機器を安定的かつ効率的に冷却する各種空調機器を備えています。

セキュリティ：

様々な情報システムを守るため、厳密な入退管理や館内監視が実施され、高いセキュリティを実現しています。

通信回線・設備：

電気通信事業者の光ファイバーなどの通信回線を大量に利用可能とするため、通常のオフィスビルと比べて非常に大きな帯域を持つ通信回線が、複数の電気通信事業者から引き込まれていて、利用者の情報システムをこれらの通信環境に接続するための基幹のネットワーク設備を保持し、提供しています。

人材：

専門性を持った要員が 24 時間 365 日体制で建物、電源、空調、ネットワーク、セキュリティ等の運用を実施し、加えて利用者への支援サービスを提供しています。

資源の集約と共有：

データセンターでは建物、電源、空調、ネットワーク、セキュリティといったインフラ機能やそれを提供する設備を、複数の利用者の情報システムにおいて共有することにより、高品質なインフラの提供と運用コストの削減を同時に実現しています。

これらの特徴は安全・安心、コスト削減、環境構築に必要な時間の短縮(スピード)といったデータセンターを利用する上での「価値」を実現する為に取り組まれている方法の一部となっています。このデータセンターを利用する上での「価値」を、様々なリスクから守るため、それぞれのリスクに対応する「管理策」が取り組まれています(図 1)。

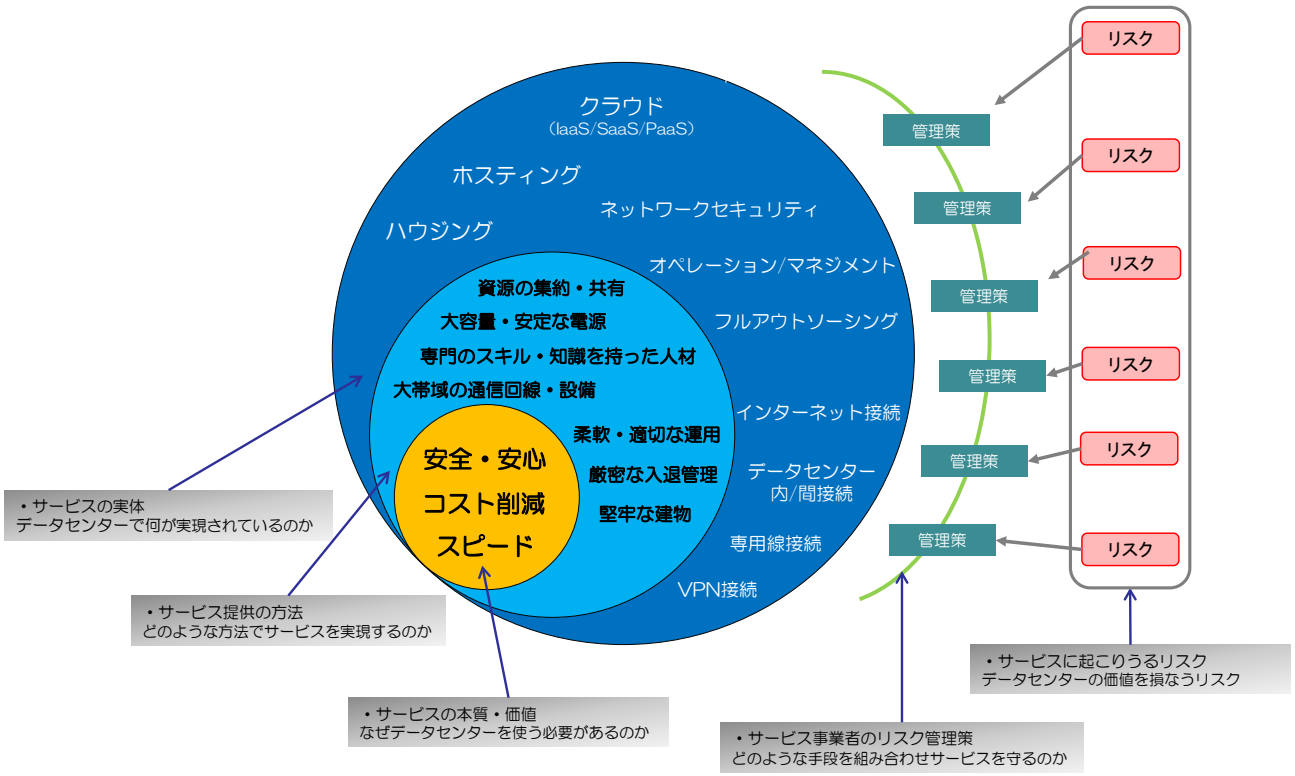


図 1　データセンターの価値、提供方法、サービスの実体とリスク、管理策の関係

1.1.2 データセンターの歴史とデータセンター事業者の責務

現在、データセンターには、様々な分野・業界の様々な情報システム資産が集中しています。ここでは、過去から現在におけるデータセンターへの情報システム資産の動きを解説します。

企業等の情報システムの導入が急速に拡大した 1970 年代後半、現在のデータセンターへの流れの一つである「大型電子計算機センター」が登場しました。この大型電子計算機センターには、非常に高価な情報システム資産であったメインフレームと呼ばれている「大型電子計算機」が設置され、情報システムは、この「大型電子計算機」を中心にして、集中管理、集中処理が行われていました。こうした「大型電子計算機センター」は、一般的に非常に堅牢な建物が使われ、現在の水準からしても高い物理セキュリティを実現していました。

1990 年頃、低価格な UNIX ワークステーション等が登場し、ダウンサイジングとクライアント・サーバーシステムへの流れが始まりました。この時期、「大型電子計算機センター」に鎮座し集中

管理、集中処理されていた大型計算機等の情報システム資産は、低価格なワークステーションと分散処理技術により置き換えられていきました。これらのワークステーション等の情報システムは、場所的にも分散し、分散管理、分散処理されるようになりました。

インターネットが爆発的な普及を果たした 90 年代後半、現在のデータセンターにつながる「インターネットデータセンター」が誕生しました。「インターネットデータセンター」は、高速なインターネットに接続するための回線を持ち、その回線に情報通信機器を接続するための機器の設置場所として発展してきました。黎明期におけるインターネットのサービスのボトルネックは、インターネットへの接続コストであり、初期のインターネットデータセンターにおいては、セキュリティよりも高速な回線とそのコストが重要視され、現在のような多様なセキュリティへの多様な要求はまだありませんでした。

2000 年以降、データセンターの大規模化、ブレードサーバー等の登場による高集積化、データセンター内部のネットワークの高速化が顕著になってきました。同時に、広域ネットワークの低価格化によって、企業内に設置されていた情報システムを遠隔地のデータセンターに設置する方がコスト的に有利になり、90 年代からのダウンサイジング以降分散していった情報システムが徐々にデータセンターへ集中されていく流れが出来ました。

そして、2017 年現在、情報システムの増加に伴う所有コストの増大やデータセンターのスケールメリットによる外部委託コストの低下等を要因として、「情報システム資産の所有」から「サービスの利用」へというクラウドサービスの流れは「クラウドファースト」という言葉が示すように、もはや当然のものとなっています。データセンターとクラウドサービスとの関係は、データセンター事業者自体がクラウドサービスを提供することもあれば、クラウドサービス事業者がデータセンターを利用してクラウドサービスを提供することもある等様々ですが、いずれにせよ、エンドユーザーがクラウドサービスを利用する機会が増えた今、多くの人が直接的・間接的にデータセンターを利用する状況になっています。

こうした状況にあって、データセンター事業者は、ビジネス上の契約として情報通信機器やデータを預かり運用可能な状態に保守するという「契約遂行の責務」のみならず、社会インフラとなる情報通信に関する重要インフラを提供する事業者としての「社会的責務」を果たす責任を負うことになりました。

一例として、近年ではデータセンターに環境負荷の低減が求められるようになっており、日本データセンター協会ではこうした社会的要求に応えるべく、環境基準 WG によるデータセンターの環境性能指標とその計測方法を策定・提案、環境政策 WG による自治体への環境政策との連携といった技術面・政策面の両面からのこの課題に取り組んでいます。

1.1.3 データセンターの適切なセキュリティ

現在の社会インフラ化したデータセンターでは、様々な課題に取り組むことが求められていますが、その中でも重要な課題の一つにデータセンターのセキュリティがあります。

データセンターに要求されているセキュリティは単純ではありません。データセンターで提供される実際のサービスには、セキュリティ、コスト、効率・利便性等のトレードオフが存在するため、過剰なセキュリティへの要求はデータセンターのコスト要因や利便性を損なう結果となります。そのため、データセンター事業者は利用者の要求に応じ、適切なコスト、適切なセキュリティ、そし

て利便性のバランスを保ちながらサービスを提供することが求められています。一方で、「適切なセキュリティ」を合理的に示すのは簡単ではありません。以下にその主な理由を示します。

(1) より多種多様な利用者からの、それぞれの分野・業界におけるセキュリティの要求

データセンターには多種多様な分野・業界から多種多様なセキュリティ対策の要求が集まっています。この背景には、2000 年以降の利用者からの情報システムのセキュリティに対する要求の多様化と、様々な情報セキュリティに関連する制度の整備があります。2010 年代に入ってからはさらに、内部統制に対する要求や、個人情報保護対する要求のもそれぞれの企業のポリシーに合わせたセキュリティの要求によってさらなる多様化が起こっています。

(2) 様々なレイヤーへのセキュリティの要求

データセンターが提供するサービスは、様々なレイヤー（ファシリティ、ネットワーク、情報通信機器等）に及びますが、セキュリティの実現に当たって攻撃者はレイヤーを問わず一番「弱い」所を攻撃するため、これらを連携させた対策が必要になります。しかしながら、これらのレイヤーはそれぞれの専門知識を持った人材によって独立に支えられていて、レイヤー間を跨いだ対策は様々な困難を伴っています。

(3) 共有サービスにおけるセキュリティ対策の難しさ

データセンターのビジネスモデルの根底を成す「建屋や設備、情報通信機器、運用といったリソースの共有」を実現するためには、セキュリティ的には、効果的な共有と利用者（共有者）間の隔離という一見相反する要求を両立する必要があります。

これら三つの課題に加えて、セキュリティ対策の対費用効果を判断することの難しさという課題もあります。これは、定量的なリスク評価の難しさに起因するデータセンターのセキュリティに限らない、セキュリティの共通の課題です。通常、データセンター事業者は、様々なセキュリティ対策を施したサービスを提供しています。ところが、この対策の前提となるリスクは利用者の立場や社会的背景等様々な影響を受けるため、定量的に評価することが難しく、それゆえに、データセンター事業者は「適切なセキュリティ」が実現するサービスを価値として訴求することが非常に難しいのです。

本ガイドブックでは、データセンターのセキュリティそのものを定性的・定量的に捉えようとするのではなく、データセンターにセキュリティを適応する際の「考え方」、特に「セキュリティ バイデザイン」の方法論に重点を置き解説しています。これは、本ガイドブックが「適切なセキュリティ」を共有する上で不可欠な「ステークホルダー間の相互理解の為の共通言語」となることを目指しているためです。

コラム① 誰が為のセキュリティ バイ デザイン

「セキュリティ バイ デザイン」は製品・サービスの企画・設計段階からセキュリティを確保すること、および、そのための方策と言われています。逆に考えるならば、従来のセキュリティは運用段階でインシデントやアクシデントが発生してから場当たり的に行われることが当然と考えられてきたということもできます。

なぜそのような状況に陥っていたかを考えてみると、情報システムの多くは情報が使われてみないと、どのような価値があるかわからない、どこまでコストを割いてセキュリティを実現すべきかわからないという課題があったためと考えることができます。この後付けのセキュリティの発想はシステムが利用される過程で高まる「価値」に合わせて守りを固めるという意味でコンカレント・フレキシブルなアプローチであり、ある意味トップダウンなデザインベースのアプローチより、より有効な取り組みと捉えることもできます。にもかかわらず、トップダウンなデザインベースのアプローチが必要とされているのでしょうか？

上記の疑問に答えるためのキーワードの一つに「安心」があります。セキュリティは一般に「安全（を保つこと）」と訳されることが多いですが、語源を辿っていくと、「気がかりを取り除くこと」（Se（分ける/取り除く）-Cure（気がかり、気づかい）-Ity（こと））という「安心（を保つこと）」に近い意味を見出すことができます。

安全と安心の違いは客観か、主観かというところにあります。課題が見つかったらその場で手当てをしていくというボトムアップなアプローチでは、その手当てが繰り返されているうちに膨大なドキュメントとしてその手当てが客観的に記録されていたとしても、個人の主観では全容を理解していくことが難しくなってしまうという課題があります。そう言った場合にトップダウンのデザインベースアプローチを用いることが出来れば、個人が全容を理解することができます。すなわち、システムが複雑化するなかで利用者の主観的な視点で一貫性を検証しやすいセキュリティを実現するために、デザインベースのアプローチが求められているという側面があります。

なお、システムの提供者側が、利用者にとって検証しやすいデザインを実現するためには、主観が「誰」によるものなのかを事前に考える必要があります（3.1 節では「データセンターを利用するサービス事業者の経営層」の視点を想定したデザイン過程（リスク分析）を紹介しています）。そして、そのデザインを実装するために「誰」の「どのような気がかりを、どのようにして取り除くか」という想像力を働かせることが必要になってきます。本書はその想像力を培うための知識を読者に与え、役立てることができるようにつくられています。

1.1.4 日本データセンター協会の取り組み

日本データセンター協会ではデータセンターに関するさまざまなドキュメントを作成し、その一部を広く一般に公開しています。

表 1　日本データセンター協会の作成しているドキュメント類

ドキュメント名	担当WG	最新版	公開方法
データセンターファシリティスタンダード (JDCC FS-001)	ファシリティ・スタンダード	Ver. 2.3 (2017年1月)	有償 (要約版は無償)
PUE計測・計算方法に関するガイドライン (JDCC ES-001)	環境・基準	Ver. 2.7 (2015年5月)	有償 (要約版は無償)
建物設備システムリファレンスガイド	ファシリティ・インフラ	第2版 (2017 年10月(予定))	非公開
人材育成ガイドライン	人材育成	第2.5版 (2017年4月)	公開
データセンターネットワークリファレンスガイド	ネットワーク	第２版 (2014年1月)	公開
データセンターセキュリティガイドブック	**セキュリティ**	**2017年版 (2017年９月)**	**公開**

日本データセンター協会(JDCC)セキュリティ WG では、データセンターのセキュリティに関する議論の土台づくりとして、データセンターの利用者と事業者の双方において、データセンターの適切なセキュリティに関する理解を深める、日本のデータセンターの利活用のために広く参照されることを目標として本ガイドブックを作成・更新しています。

１.２ 本ガイドブックの対象読者・構成

１.２.１ 本ガイドブックの対象読者

世の中には様々なデータセンターのセキュリティに関連する物理・情報セキュリティに関するガイドライン、基準、監査・認証制度等のドキュメントが政府・団体・民間から提供されています[3]。一方でこれらのドキュメントの多くは特定の業界の利用者、あるいは特定のデータセンター事業者を想定していて、本ガイドブックの創刊以前、「セキュリティ バイ デザイン」の観点からそれらのドキュメントを俯瞰し、データセンターのセキュリティの全体像を把握することのできるドキュメントはありませんでした。

そこで、本ガイドブックは、以下の二つの使われ方を想定して刊行されました。

1. データセンター利用者が、データセンターが提供するサービスの利用を検討する際、提供されるサービスのセキュリティを理解するために活用可能な資料
2. データセンター事業者が、「適切なセキュリティ」を実現したデータセンターを設計・運用する際にステークホルダー間の共通言語として活用可能な資料

本ガイドブックでは、データセンターにおける「適切なセキュリティ」を直接示す事を目的とはしていません。本書は、読者が自分たちで「適切なセキュリティ」をデザインし、共有するために必要な知識を与えることを目指しています。

３： 付録１参照

１.２.２ 構成

本ガイドブックは以下の５つの章から構成されています。

第1章　「本ガイドブックの概要」

第１章では、本ガイドブックを作成した背景、意図、想定する読者を説明した後、各章の概要という形で全体像の要約（エグゼクティブ・サマリー）が記述されています。

第2章　「データセンターのサービス」

第２章では、データセンターが提供する一般的なサービス（ハウジングサービス、ホスティングサービス、クラウドサービス等）と、そのサービスを支える構造を説明しています。

データセンターのサービスは、データセンターの持つ様々な資源（ファシリティ、情報通信機器、データセンター要員等の人的資源）を利用者間で共有することにより、適切なコストでサービスを提供しています。セキュリティに関しても、データセンターのセキュリティに関する資源を共有することにより適切なコストで提供されることになりますが、その一方、共有に対する適切な分離が重要となります。

データセンターの利用者は、本章を読みデータセンターで提供されるサービスについて理解し、データセンターがどのような仕組みからそれらのサービスを提供しているかを知ることで、次章以降で紹介されるデータセンターのセキュリティをよりよく理解することができます。

第3章　「リスク分析と管理策」

第３章では、データセンターのサービスにおけるリスクを説明した後、このリスクに対する「管理策の考え方」を提示し、その上で、実際のデータセンターで実施されるセキュリティ管理策がどのように実現されているかを「架空のデータセンター」を元にして紹介します。

「データセンターの利用におけるリスク」の節では、典型的サービスであるハウジングサービス、ホスティングサービスそしてクラウドサービスを想定したリスク分析を提示しています。「セキュリティ管理策の考え方」の節では、主に「人為的脅威」に関する管理策の「考え方」を示しています。「実際にデータセンターで実施されるセキュリティ管理策」の節では、物理的セキュリティにフォーカスして、「架空のデータセンター」を設定し、そのデータセンターで実施される管理策を見ていくことで、データセンターにおけるセキュリティの実現がどのようになされているか理解することができるようになっています。

データセンターの利用者は、本章を読むことにより、データセンターが提供するサービスの一般的なリスクと、そのリスクの分析方法、リスクに対応する脅威への管理策の考え方、そして一般的なデータセンターにおける管理策の事例を理解することができます。

第4章　「基準・ガイドラインと認証制度」

第４章では、データセンターのセキュリティに係わる基準・ガイドラインと、これらへの準拠性を証明する認証制度等を説明します。

第 3 章では、利用者からのボトムアップでデータセンターのサービスのリスクを分析し、脅威に対する考え方を整理し、セキュリティ管理策を実施するところまでを説明しました。逆に業界に対してトップダウンで標準や制度を策定するアプローチも社会には存在しています。特に近年ではデータセンターが社会に欠かせないインフラとなっていることを背景として、データセンターのセキュリティに係わる様々な規格・基準が整備されています。また、こうした動向に加えて、前述の規格・基準等への準拠性、適合性等を客観的に評価する第三者評価制度や国による認証制度等も整備されつつあります。

しかしながら、これらの規格・基準や制度等の関係は、その歴史的経緯もあり、一般に整理・理解されているとは言えない状況にあります。更に昨今では、データセンターが様々な分野で利用されている状況にあわせ、その分野の政府機関、業界団体、民間企業等により、それら分野のガイドラインが別途、個別に整備されています。

本章では、データセンターの利用者向けに、データセンターのセキュリティに係わる基準・ガイドライン、認証制度について解説した上で、「マネジメントシステム適合性評価制度」、「情報システム安全対策適合証明制度」「その他の基準・認証制度」を紹介し、これらの基準・認証制度とは独立にそれぞれの分野に存在する「分野ごとの基準・ガイドライン」を解説することで、読者がこれらの関係を整理して理解できるよう手助けします。

第5 章　「セキュリティを実現するシステム」

第 5 章では、データセンター事業者が導入している、セキュリティに関する様々なシステムについて紹介します。

この章では、データセンターのセキュリティを実現するシステムの例として、様々なシステムを統合的に管理する「DCIM(Data Center Infrastructure Management)システム」を中心に、「異常監視システム」「アクセスコントロールシステム」「サーバーラックシステム」「ビルディングオートメーションシステム」といった様々なシステムを紹介しています。この章は、これらのシステムをデータセンターに納入しているメーカー・ベンダーの視点から、セキュリティを実現するシステムの仕組みや特徴、そして、昨今の技術トレンドを紹介しています。

なお、本ガイドブックの 2015 年版で重点的に取り組んだビルディングオートメーションシステムに関しては、2016 年に新たに刊行された「建物設備システムリファレンスガイド」にその解説を移管しているため、データセンターセキュリティガイドブックの 2017 年版ではビルディングオートメーションシステムそのものの解説にとどめています。[4]

また、セキュリティの概念には機密性、完全性、可用性が含まれていますが、本ガイドブックでは機密性、完全性の概念を中心に扱っています。この理由として、データセンターの可用性を中心的に扱った基準として前述の日本データセンター協会のファシリティスタンダード WG が作成した「ファシリティスタンダード」の存在があります。2011 年 3 月 11 日の東日本大震災に際し、外部にサービスを提供するデータセンターにおいて、サービスが停止した箇所は 1 ヵ所もなく、日本の

4：　本ガイドブックにおける基準・認証制度を含むさまざまな記載は 2017 年 6 月現在の情報を元に記載されている。情報を参照する際には本ドキュメントの付録B 関連ドキュメント一覧や、付録 C 関連団体一覧を参考に最新の情報を適宜確認のこと。

データセンターの可用性に対する高い信頼性が認識されました。この背景には「ファシリティスタンダード」の果たした役割は少なくなかったと考えられます。そこで、本書では可用性に関する資料が「ファシリティスタンダード」において既に提供されているという立場から、機密性、完全性の概念を中心に扱っています。

１.２.３ 旧版からの更新点

これまで「データセンターセキュリティガイドブック」は 2 年おきの改定を経ており、本版は 2013 年の初版以来、三つ目の版となっています。

2013 年の初版では、データセンターというサービスの仕組みを、これからデータセンターを利用しようとしている利用者を含むデータセンター利用者、事業者（さらには周辺のステークホルダー）のための共通言語となることを目指し、刊行を行いました。これにより、データセンターのセキュリティに関わる情報を網羅的に扱った本ガイドブックの方針が形作られました。当時はデータセンターのセキュリティに関する情報はあまり公開されていなかったため、本書を通じてデータセンターのセキュリティについて一定の視座を読者に提供しました。

2015 年の改定版では、「クラウドファースト」と呼ばれるようになったクラウドサービスにより力点を置き、クラウドサービスに関する記述の強化を行いました。また、当時注目を集めていたビルディングオートメーションシステムのセキュリティについて紹介するコンテンツも追加されました。同時に、データセンターの提供するサービスに関する記述の強化とそれらの内容の「利用者視点でのブラッシュアップ」も取り組みました。

そして、この 2017 年版では、Society5.0/サイバーフィジカルシステムのインフラとしてのデータセンターをコンセプトとして、技術の動向やサイバーセキュリティ・プライバシー保護といった制度の動向についてコラムを使って紹介しています。また、Society5.0/サイバーフィジカルシステムは様々なサービス・ビジネスが創出されることが想定されますが、創出されるサービス・ビジネスが社会に受容されるためには適切なリスクマネジメントが不可欠となります。そこで、この版では従来のデータセンターありきの脅威分析中心の考え方を改め、サービス・ビジネスのオーナーがデータセンターを利用する際に必要なサービス・ビジネスありきのリスク分析に焦点を当て、適切にリスクアセスメントを行えるよう必要な知見を提供しています(3 章 1 節)。

その他にも、2017 年版では、2015 年版から以下の点が更新されています。

運用の観点からの情報の増強(3 章 3 節)

これまでのデータセンターセキュリティガイドブックでは、建屋や設備によるセキュリティについて詳細に紹介してきましたが、利用者視点ではこれら以上に人の運用によるセキュリティが大きな意味を持っています。そこで、今回の改定では、この人による運用に力点を置いて解説を行っています。また、これに合わせて、架空のデータセンターのプランニングもより現実に即した形で見直しを行なっています。

基準・認証制度に関する情報の更新(4 章)

クラウド関連の認証基準の登場等、基準・認証制度の動向に合わせた改定を行いました。また、2015 年版を刊行してから 2 年が経過したことから、この期間に更新された基準・認証制度についての解説も修正・追加しています。

ビルディングオートメーションシステムに関する情報の改定(5 章)

日本データセンター協会からビルディングオートメーションシステムのセキュリティに関する解説書である「建物設備システムリファレンスガイド」が刊行されたことに伴い、「ビルディングオートメーションシステムのセキュリティ」に関する解説を同リファレンスガイドに移行し、本ガイドブックでの記述を「ビルディングオートメーションシステムの機能、要素、活用」を中心としたものに改定しました。

またこれらの他にも図表の追加や文章の見直しによって、より読みやすいガイドブックとなることを目指した改定をおこなっています。

1.3 用語解説

セキュリティ区画

「セキュリティ区画(security zone)」とは、アクセス制御等の手段によって一定のセキュリティを確保した区画を意味します。本ガイドブックでは、「領域」「エリア」等の同義語、類義語は、概ね「区画」に統一しています。本書において、この「セキュリティ区画」は物理的・論理的双方の文脈において用いられています。例えば、代表的な物理的セキュリティ区画に「鍵付きサーバーラック」の内部空間が挙げられます。鍵付きサーバーラック内は、そのサーバーラックのドアパネルや側面パネル等の構造とドアパネルに取り付けられた鍵によって外部と切り分けられています。

物理的空間に適応される区画に対して、ネットワーク等の論理的空間において用いられる区画が論理的セキュリティ区画となります。代表的な論理的セキュリティ区画としては、ファイアウォールによって外部と切り分けられるイントラネットが挙げられます。

本書では（特に断っていない場合を除き）物理的・論理的いずれのセキュリティ区画においても共通の考え方が適応できるという考え方に立っています。なお、区画(zone)を定義し、実装することを「ゾーニング(zoning)」と称しています。

セキュリティ境界

セキュリティ区画を切り分けるための物理的・論理的な境界を本書では「セキュリティ境界」と称しています。

セキュリティ境界は、選択的にアクセスを許すものと、いかなるアクセスも許さないことを目的とするものとの 2 種類に分けられます。物理的セキュリティ境界を例にとるならば、前者に関してはセキュリティゲートと本人認証・権限管理の仕組みを組み合わせたもの、後者に関してはフェンスや塀と侵入検知システムによる境界などがそれに当たります。

事業者

本ガイドブックにおける「データセンター事業者」は、自社データセンターを保有し、そのデータセンターを活用してコロケーション/クラウド/ホスティング/仮想サーバー等のサービスを提供する事業者のことを示します。こういった事業者には、他のデータセンター事業者から利用者としてデータセンターサービスの提供を受け、さらにそれを、自身が事業者となり他の利用者へ提供する形態(DC in DC)でビジネスをおこなっている事業者もあります。

利用者

本ガイドブックにおける「利用者」は、データセンターのサービスの利用契約者、並びに、その契約者から委託を受けてデータセンターの利用をおこなう者を意味します。データセンターの契約

者が、データセンターを利用して提供するサービスの利用者は、「エンドユーザー」として記載しています。

要員

本ガイドブックでは、データセンターのサービスの提供に携わるデータセンター事業者の人的資源全般を「データセンター要員」と称しています。対して、データセンター事業者に所属せず、データセンターのサービスに係る人々は、「データセンター出入り業者」と称しています。

第２章 データセンターのサービス

この章では、データセンター事業者が提供する一般的なサービス（ハウジングサービス、ホスティングサービス、クラウドサービス等）と、そのサービスを支える構造を説明しています。

データセンター事業者は、データセンターの持つ様々な資源（ファシリティ、情報通信機器、データセンター要員等の人的資源）を利用者間で共有することにより、適切なコストでサービスを提供しています。セキュリティに関しても、データセンターのセキュリティに関する資源を共有することにより適切なコストで提供されることになります。その一方、データセンターの利用者は、資源を共有することにより生じるリスクを把握し、利用の用途に合わせて適切な対策を考慮することが重要です。

本章を読むことでデータセンター事業者がどのようにして、データセンターのサービス基盤を支え、利用者の利便性を高めながら、安定したサービスの提供を行っているのかを理解することができます。

２.１基本サービス

この節では、データセンターの提供する基本サービスとなるハウジングサービス、ホスティングサービス、クラウドサービスについて紹介します。

２.１.１ ハウジングサービス

ハウジングサービスは、データセンターの一部を借りて利用者の所有する情報通信機器を設置、稼働させることができるサービスです。一般に鍵付きサーバーラックで区画された空間を借りるサービスをハウジングサービス、専用サーバー室をして一室全部を借りるサービスや、共用サーバー室の一部を借りるサービスをコロケーションサービスと呼び、その他にもサーバー室の一部を他のサーバー室利用者から区画するために柵（ケージ）で囲い、その領域を借りるサービス等が提供されています。

事業者ごとに幅がありますが、上記のサービスに加え安定した情報システムの動作環境（電源・空調等）の提供を基本サービスとして、インターネット接続回線の提供やファイアウォール等のネットワークセキュリティサービス、データセンター事業者による機器の LED 監視や手動による情報通信機器の再起動等のサービス等も提供されています。

利用者は、ハウジングサービスを利用することで、以下のようなメリットがあります。

- 地震や火災等への対策
- 安定した電力供給（UPS や非常用発電装置等）
- 温度・湿度の管理
- セキュリティ対策（監視カメラ、入退管理システム等）
- 高速なインターネットバックボーンの利用

他にも事業者によって様々なメリットをアピールしていますので、利用の用途にあった事業者の選択が必要となります。

コラム② データセンターの顔「サーバーラック」

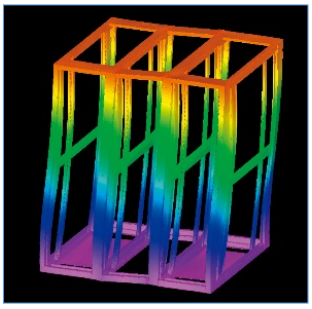
「データセンター」という言葉を聞いて多くの人が真っ先に思い浮かぶのは、サーバー室内に整然と並んだサーバーラックの姿ではないでしょうか？このように、データセンターの顔といっても過言ではないサーバーラックですが、一見画一的に見えるデータセンターのサーバーラックにも、事業者の設計思想によって様々なバリエーションが存在しています。

サーバーラックに求められる性能としては、機器を搭載した時の強度面（静荷重）や、搭載した機器の滞留熱に対処する放熱面(開口率)が代表的です。他にも、ネットワーク機器を搭載した際のサーバーラック前後面の配線スペースの確保や、機器の冗長化電源を確保するために複数本のコンセントバーを収納する構造にするなど様々な工夫が凝らされています。これらニーズに応える為、サーバーラックメーカー各社は、独自の設計基準を設け、データセンター事業者に合わせたサーバーラックを製造し納入しています。

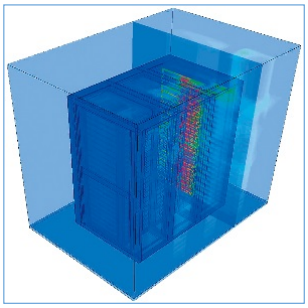
また、最近のトレンドとしては、各データセンター事業者様において、ハウジング やクラウドそれぞれに特化した仕様を個別に深化させており、サーバーラックの形状やサイズに多様化という新しい概念が生まれつつあります。

一例としては、ネットワーク配線重視の事業者/利用者向けには、サーバーラックの横幅を「＋100mm」となる 800mmとし、前後のマウント金具の周辺に大きな配線スペースを設ける仕様としたものや、逆に配線本数が少ない事業者/利用者向けには、横幅を「－100mm」となる 600mmとし、数多くのサーバーラックを収納するエリアを構築する仕様が登場しています。また、機器を搭載するユニット数を拡大するために、最近では、通常 42U や 46U のサーバーラックに対して、48-52U といった一回り高さのあるサーバーラックを導入する事業者も登場しています。

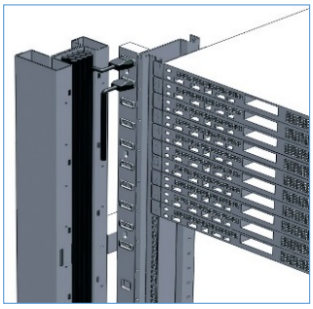
CAEによる振動解析



CFDによる熱解析



CADによる構造解析



イメージ提供：河村電器産業

2.1.2 ホスティングサービス

ホスティングサービスは、利用者に情報通信機器と回線を提供し、その機能を遠隔から利用者が利用できるサービスです。貸し出される情報通信機器には、物理的に機器を専有できる形態の専有ホスティングと機器を複数の利用者で共有する共有ホスティング等の形態が存在します。いずれのサービスもデータセンター内の専有サーバー室や共有サーバー室で運用され、専有ホスティングに関しては、加えてデータセンター要員による LED 監視や再起動サービスが提供される場合があります。共有ホスティングに関しては、データセンター事業者によりサービスの維持管理がされています。

データセンター設備と情報通信機器およびネットワーク回線の運用も提供されるため、利用者は、情報通信機器（スイッチやルータ等）を所有する必要がなくなり、また、システム運用もサービスとして提供される場合もあるため、専門的な知識がなくとも管理が可能になるといったメリットがあります。

2.1.3 クラウドサービス

クラウドサービスは、データセンターの保有するネットワーク、情報通信機器、ミドルウェア、アプリケーションといったコンピューティング資源に対して、利用者が必要に応じてアクセスし利用することができるというサービスです。クラウドサービスは一般に、サービスとしてどこまでの機能が提供されるかの違いによって「IaaS」、「PaaS」、「SaaS」等に分類されます。

IaaS （Infrastructure as a Service：イアース、アイアース）

利用者は情報通信機器の資源（仮想 CPU、メモリ、ストレージ、ネットワーク）を動的に制御し、その上で OS やアプリケーションも含め、任意のソフトウェアを導入することができます。サービス利用者はクラウド自体の管理をおこなう必要はありませんが、クラウド上で動作する OS やストレージや一部のネットワーク（ロードバランサーやファイアウォールなど）の管理を利用者自身でおこなう必要があります。

PaaS （Platform as a Service：パース）

利用者はスケールアウトする環境上で、サービスプロバイダーが提供するミドルウェア環境を利用したアプリケーションプログラムを動作させることが出来ます。

基本的に利用者で OS やハードウェア、ネットワークの管理をおこなう必要はありませんが、アプリケーション設定や一部の（アプリケーションフレームワークなどの）環境設定が利用できるサービスもあります。

SaaS （Software as a Service：サース）

利用者はスケールアウトする環境上で、サービスプロバイダーから提供される UI ベースの環境を使い、利用者独自のサービスを構築し利用することが出来ます。PaaS 同様、利用者側ではアプリケーションが動作している OS やハードウェア、ネットワーク設定などをおこなう必要がなく、

すべて事業者側で行います。類似するサービスにサービスプロバイダーの提供するサービスをそのまま使う ASP（Application Service Provider）と呼ばれるものがあります。

上記の他に NaaS（Network as a Service）や BaaS（Backend as a Service）等があります。これらのサービスでは、利用する企業において必要とする仕組みを考慮したうえで、適切なサービスを選択することが重要です。

ハウジングサービス、ホスティングサービス、クラウドサービス（IaaS・PaaS・BaaS・SaaS）の関係をまとめたのが図 2 です。図中、紫色で示されているのが事業者の提供する範囲、黄色で示されるのが利用者の用意する範囲となっています。

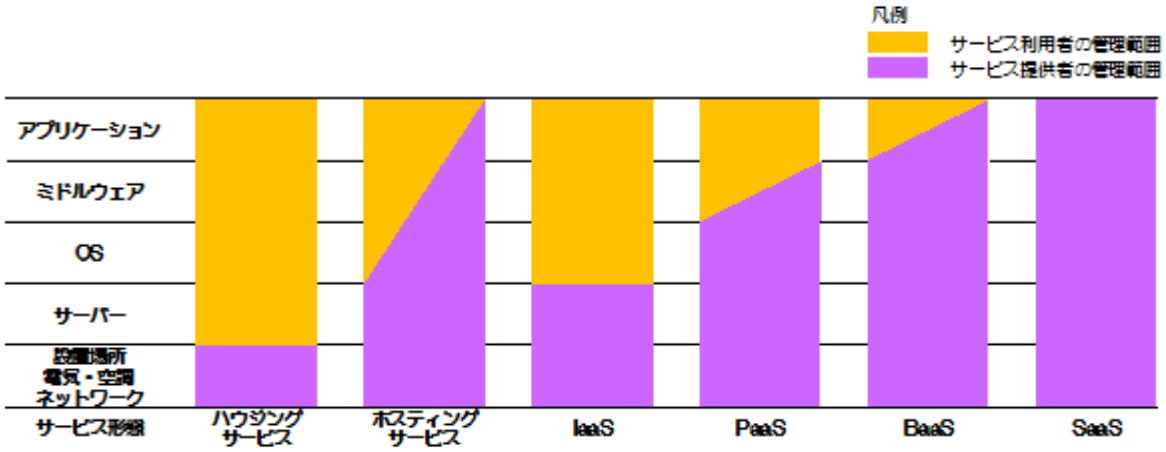


図 2　ハウジング・ホスティング・クラウドサービスの比較例

また、SaaS 事業者がサービスを提供する基盤として PaaS 事業者もしくは、IaaS 事業者を利用している場合があります。このような事業者同士の繋がりを「サプライチェーン」（図 3）と呼びます。クラウドサービスがサプライチェーンを通して提供されている場合、利用者においては、契約事業者だけでなくサプライチェーンで繋がっている事業者についても運用面・セキュリティ面を考慮することが望ましいです。

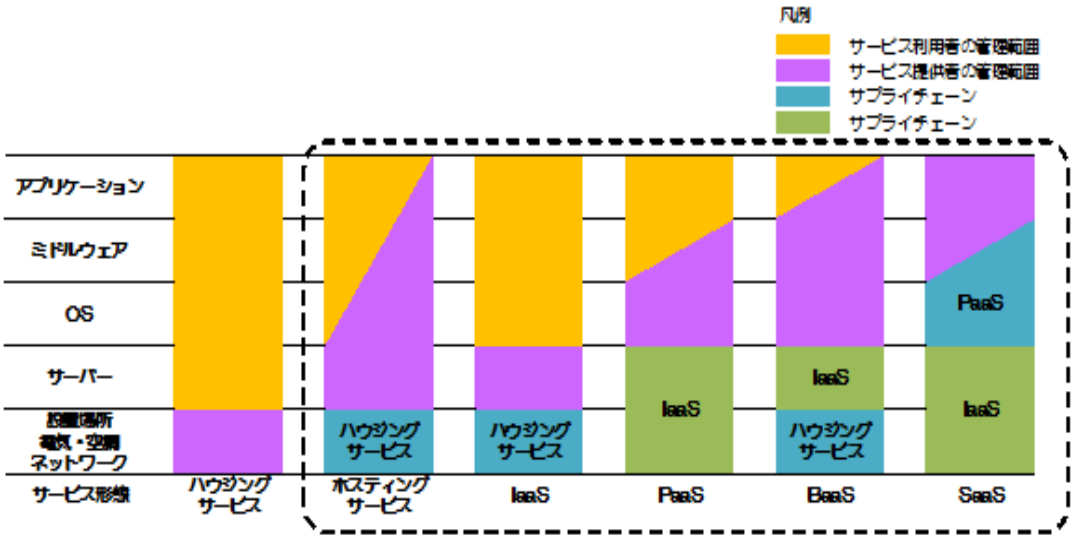


図 3　サプライチェーンの例

２.２ネットワークサービス

ハウジング、ホスティング等のサービスを利用する場合、データセンター構内及び外部と接続性を確保するため、以下のようなネットワークサービスを提供しています。

２.２.１ 内部ネットワーク

データセンター利用時の段階的な拡張により物理的に離れたサーバー室にシステムが置かれる場合や、災害時の事業継続計画(Business Continuity Plan：BCP)や災害時の復旧計画(Disaster Recovery Plan：DRP)を意識し距離的に離れたデータセンターにシステムを置く場合、もしくは同一データセンター内のパートナー企業システムへ接続する場合等、データセンターの利用には様々なケースがあります。これらのケースにおいて、通信遅延やセキュリティ面を考慮しインターネット接続等外部を経由しない方法でシステム間の直結ができるよう、データセンター事業者が予め用意した構内配線をサービスとして提供している場合があります。

データセンター構内接続（単一拠点内接続）

データセンター事業者が同一サーバー室内、データセンター内の異なるサーバー室間等の接続を構内接続サービスとして提供している場合があります。このようなサービスを活用することで、拡張時期によって隣接していないサーバーラック間の接続や、同一データセンター内の他サーバーラックに納められた情報システムとの接続等において柔軟な対応が可能になります。

データセンター間接続（多拠点及び遠距離接続）

BCP や DR を意識し、離れた地域に数ヶ所データセンターを運営・提供する事業者では、あらかじめ事業者が用意した専用線等を提供することで、利用者のビジネスリスクを軽減するサービスを提供している場合があります。利用者から見たこのサービスのもう一つの利点として、通信回線や仲介するネットワーク機器などの維持・管理の手間がなくなる点が挙げられます。

２.２.２ 外部ネットワーク

データセンターは外部との接続のために、以下のようなサービスを提供しています。

インターネット接続サービス

インターネット接続を提供するサービスはホスティングサービスの場合、利用者が外部からインターネットを経由してサービスにアクセスするため、基本的に標準のサービスとなっていて選択の余地はありません。一方でハウジングサービスを利用する場合は内部ネットワークの利用を前提に、外部ネットワークサービスがオプションとなるケースもあるため、どのような回線が必要かも含めてデータセンターの利用を検討する必要があります。

使用可能なインターネット回線の種類には、データセンターが引き込んだ電気通信事業者の回線をデータセンター利用者同士で共有するタイプや、専用に電気通信事業者の回線を引き込むタイプ等があり、共有タイプの回線では使用回線速度の増減、グローバル IP の追加等のオプションが提供されます。

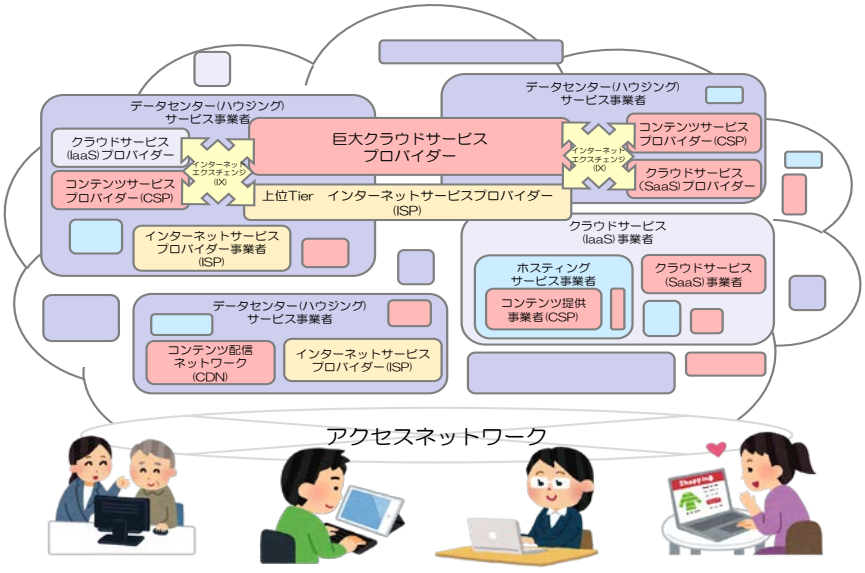
コラム③ インターネットとデータセンター

現在新設されるデータセンターの多くはインターネットに接続することを前提とした iDC(インターネットデータセンター)と呼ばれるものになっています。

社会インフラとして世界中に浸透したインターネットですが、その実態は IP(インターネットプロトコル)を利用して複数の自律ネットワーク（AS：Autonomous System）が相互接続したネットワークです。iDC は、このインターネットに接続するため、電気通信事業者の提供する光ファイバーを入線し、AS である ISP（インターネットサービスプロバイダ）や AS 同士がつながる IX（インターネットエクスチェンジ）を利用できるようになっている、あるいは、データセンター事業者自身が ISP としての機能を提供しているデータセンターということができます。

iDC の始まりは、AS 間の相互接続に不可欠な物理ネットワークのコスト（一般に距離に応じてコストが高くなる）を AS 同士が一つの場所に集まることで減らそうとしたことがきっかけでした。さらに、AS 同士が個々に相互接続（ピアリング）するメッシュ構造ではネットワークの構造が複雑、高コストになるという課題があったため、共有のネットワークのハブ（スイッチ）を設置したスター構造にすることによって相互接続をより容易にするビジネスとして IX が登場しました。IX の設置されたデータセンターはインターネットへの重要な接続拠点となり、そのデータセンターの周囲にデータセンターが建設されるデータセンター集積地（東京の大手町、大阪の堂島）となりました。現在では一般に大帯域を要する AS 同士の接続ではピアリングを、様々な AS との接続をおこなうためには IX を利用することで AS 間の接続が行われています。

なお、近年のインターネットとデータセンターの関わりとして IP のような低レイヤーのネットワークだけでなく、アプリケーションのような上位レイヤーを含めた「データエクスチェンジ」をコンセプトとするデータセンター事業者も登場しつつあります。コンテンツ配信を代行しておこなうサービス（CDN）を積極的に設置するデータセンターはその代表的なものになります。また、データセンターよりもネットワーク的にエンドユーザーの近くにコンピューティングリソースを配置するエッジコンピューティング時代を想定し、データセンター事業者がアクセスネットワークサービスを提供する動きや、逆に電気通信事業者が局舎の一部をデータセンターとして提供するという動きも登場しつつあります。



VPN サービス

VPN サービスとは Virtual Private Network の略です。その名称の通り仮想閉域網サービスで、データセンターと利用者の拠点などを接続するために使用します。VPN サービスには大きく分けて以下のサービスがあり、求められる特性や用途によって使い分けが必要となります。

- インターネット VPN（IPsec-VPN/SSL-VPN）
  - IPsec や SSL を用いて通信をカプセル化し、インターネット上に仮想ネットワークを構築するサービスです。安価に利用できる反面、インターネット上で通信を行うためベストエフォートのサービスとなります。

- IP-VPN
  - 電気通信事業者の IP 閉域網(BGP/MPLS 網)を使用して VPN を提供するサービスです。インターネットを経由するインターネット VPN とは異なり、バックボーン内の帯域を確保することで通信輻輳が発生しにくいネットワークとしています。使用できるプロトコルは IP(Internet Protocol)に限定されます。

- 広域イーサネット
  - 電気通信事業者のイーサネット閉域網を使用して VPN を提供するサービスで、IP-VPN と同様に帯域確保型のサービスです。イーサネットフレームにカプセル化されていれば IP 以外のプロトコルも使用でき、IP-VPN に比べて広帯域で安価なのが特徴です。

- イーサネット専用サービス
  - 広域イーサネットと同様に複数の拠点を接続するサービスです。トポロジーが Point-To-Point（2 拠点間接続）か Point-To-Multipoint（1 対 N 拠点接続）に限定されますが、トラフィックエンジニアリングにより他利用者の通信による輻輳の影響を受けにくくしているという点で広域イーサネットとは異なります。
    MPLS-TP、Ethernet over MPLS、PBB-TE などの論理多重技術とトラフィックエンジニアリングを組み合わせて実現するのが一般的です。

専用線サービス

専用線は電気通信事業者が提供する顧客専用の通信回線です。VPN サービスが通信輻輳の影響を受ける可能性があるのに対し、専用線サービスは OTN[5](Optical Transport Network)、WDM[6](Wavelength Division Multiplexing)などの技術を用い、OSI 参照モデルの物理層（レイヤー1）で回線多重分離を行っているため、他利用者の通信による輻輳の影響を一切受けません。

5： OTN は光ファイバーを用いて数 100-数千 km の長距離で情報を伝送するための通信規格。
6： WDM は OTN の中で用いられる技術で光の波長を多重化して光ファイバーの中を通すことで広帯域化する技術。

（MPLS[7]-TP[8]、Ethernet over MPLS[9]、PBB-TE[10]などのレイヤー2、レイヤー3 技術を使用して論理多重しているサービスでも”専用線”と謳う回線サービスがあり、区別が必要です。）

専用線サービスは、フレームロスが無く、低遅延であり、イーサネットインターフェースだけでなくファイバーチャネルなどのインターフェースも提供できるのが特徴です。1Gbps 以上の大容量のトラフィックを扱う場合に適しており、盗聴・改竄が難しく、セキュリティに優れています。電気通信事業者の中には回線暗号化サービスを提供する通信事業者もあり、更にセキュリティを高めることが可能です。

表に VPN サービスと専用線サービスの分類を示します。回線サービスの種類によって回線パフォーマンスが異なり、回線コストとのトレードオフになっています。求められる回線パフォーマンスや要件により最適な回線サービスの選択と設計が重要です。

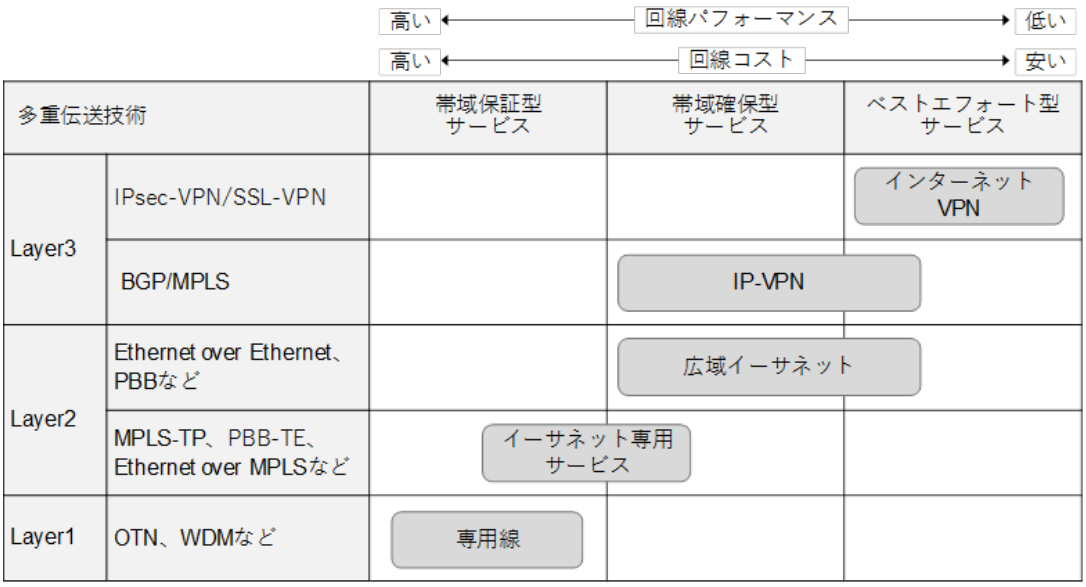


表 2　VPN サービス・専用線サービス

7： MPLS(Multi-Protocol Label Switching)は IP パケットにラベル付加(カプセル化)し、IP アドレスの代わりにラベルに基づいて転送するプロトコル。伝送経路を明示的に指示することができることを特徴とする。
8： MPLS-TP(MPLS-Transport Profile)は MPLS を簡素化し、伝送機能(トランスポート層)に特化した技術。コントロールプレーンからさまざまな管理機能を利用することが想定されている。
9： Ethernet over MPLS は MPLS 網（L3）上に Ethernet(L2)網を構築する（L2 over L3）技術。
10： PBB-TE(Provider Backbone Bridge-Traffic Engineering)は VLAN の拡張技術である PBB を元に、経路を明示的に設定できる機能や QoS（Quality of Service）機能等を付与した技術。

コラム④ マルチキャリアデータセンターの意義

複数の電気通信事業者の通信設備を有する(マルチキャリア) データセンターを利用することは、以下のようなメリットがあります。

冗長性・信頼性の向上

異なる電気通信事業者を組み合わせた経路冗長化/電気通信事業者の冗長化により、通信の高信頼性化が可能となります。また、日本データセンター協会 JDCC ファシリティスタンダード Ver.2.3 では、ティア 3 以上のデータセンターは複数回線による入線を基準要件としています（表 3）。

電気通信事業者間の競争原理による回線サービスの品質向上と価格適正化

NTT グループ、KDDI、ソフトバンクの 3 事業者以外にも数多くの電気通信事業者が国内に存在します。複数の電気通信事業者による回線サービスを利用可能とすることで、電気通信事業者間で競争原理が働き、サービスの向上と価格適正化が可能となります。

相互接続によるデータセンター付加価値の向上・ビジネス・エコシステムの拡大

複数の電気通信事業者を入線することで、相互接続可能な他のデータセンター、クラウド事業者、コンテンツ事業者などのサービス提供事業者が増加します。これにより、ビジネス・エコシステムの拡大と付加価値共創によりデータセンターの付加価値向上が狙えます。

表 3　データセンター ファシリティスタンダード 基準項目（通信設備）

	No.	評価項目	ティア1	ティア2	ティア3	ティア4
通信設備 (T)	1	引き込み経路 (※サーバー室に直接引き込む回線も一回線とする)	単一回線		複数回線	複数経路 (複数管路)
	2	建物内ネットワーク回線の冗長性 (※サーバー室に直接引き込む回線も一回線とする)	単一回線		複数回線	複数経路 (複数管路)

2.2.3 ネットワークセキュリティサービス

ハウジング、ホスティングを利用する場合、データセンターによっては以下のようなネットワークに関する論理的な[11]セキュリティサービスを追加で利用できる場合があります。

ファイアウォールサービス

ファイアウォールは、異なる論理的セキュリティ境界に設置され、論理的セキュリティ区画 A（例：外部インターネット）から論理的セキュリティ区画 B（例：内部ネットワーク）へのアクセスを制御する装置です。ファイアウォールを設置することにより、外部からの不正なアクセスを防ぐことができます。

IDS/IPS サービス

IDS（Intrusion Detection System：侵入検知システム）は、ネットワークを流れるパケットを監視し、不正アクセス（攻撃）と思われるパケットを検出して管理者等に通知する装置です。IPS（Intrusion Prevention System）は、IDS 機能を拡張したもので、不正アクセスを検知した場合に接続遮断などの防御をリアルタイムにおこなう機能を持った装置です。IDS/IPS はファイアウォールと同様に論理的セキュリティ境界に設置され、OS・ミドルウェアへの攻撃を検知・遮断します。

IDS/IPS の検知/防御方式には、シグネチャ型、アノマリ型、振る舞い検知型があります。シグネチャ型は、攻撃パターンのデータベースとのマッチングにより攻撃を検知するもので、ベンダーから提供されるデータベースに存在しない攻撃の検知・防御はできません。アノマリ型は、通常時の状態をプロファイルに設定し、違反した場合に異常とみなす方式で、未知の攻撃でも検知できる場合がありますが、誤検知を防止するためには十分なチューニングが必要となります。振る舞い検知型は、ワームや不正アクセスの振る舞いで攻撃を検知する方式で、未知のワーム・ゼロデイ攻撃にも対応可能と言われていますが、すべての不正な通信を完全に遮断できるわけではないことに留意が必要です。

WAF（Web Application Firewall）サービス

Web アプリケーションのぜい弱性をついた攻撃（SQL インジェクション、クロスサイトスクリプティングなど）を防御するための装置あるいはソフトウェアを提供するサービスです。Web アプリケーションのぜい弱性はアプリケーションの改修によって解決するのが本来の姿ですが、改修がタイムリーに行えない場合や、新たなぜい弱性への攻撃が現れた場合に有効なサービスです。

WAF の提供方法には、ブラックリスト型とホワイトリスト型の 2 種類があります。ブラックリスト型は、IDS/IPS と同様に、シグネチャを用いてあらかじめ決められたルールに則る通信パターンを検知・遮断する方法です。レポートの提供方法も似たような形式となります。一方ホワイトリスト型は、正常な通信パターンを予め WAF に登録しておくことで、正常な通信のみ通過させる方法です。ブラックリスト型はシグネチャが提供されない限り未知の攻撃の検知・防御が不可能なため対応が遅れる場合があり、予め正常な通信のみを通すよう強制するホワイトリスト型の方がセキュリティレベルは高くなります。データセンター側が利用者と連携を取りながら設定する場合は、利

11： 「侵入検知システム」はネットワークの論理的なセキュリティだけでなく、空間の物理的セキュリティ（5 章参照）においても用いられている。これらのシステムは共通のセキュリティの「考え方」に基づいて理解することが出来る

用者側とデータセンター側が綿密に連携する必要があり、頻繁に WAF で防御するシステムの Web アプリケーションを改修する場合は、利用者側とデータセンター側の負担が増加します。データセンター側が設定を全くせず、WAF の設定の利用権のみを利用者に提供するサービスもあります。

アンチウイルスサービス

アンチウイルスサービスは外部からメール等の形で侵入してくるマルウェア（ウイルスやワームなど）を防御するサービスです。ネットワーク上のゲートウェイとしてセキュリティ区画の論理的な境界に設置することにより、特定のプロトコル（主に、HTTP・SMTP・FTP）に含まれるウイルスを検知・遮断します。ウイルスをフィルタリングすることで、悪意のある Web サイト上のウイルスやメールに添付されたウイルスが情報システムへ侵入することを防ぐことができます。

アンチウイルス機能は、ベンダーが提供するパターンファイルと被疑のファイルを比較することによって、マルウェアを検出します。パターンファイルは、高頻度で更新されますので、常に最新のものになっているように管理することが必要ですが、データセンターのマネジメントサービスを利用することで、利用者はそういった管理を気にする必要がなくなります。

DoS 対策サービス

ネットワーク帯域や情報通信機器の資源を枯渇させる DoS（Denial of Service）・DDoS（Distributed Denial of Service）攻撃の検知・遮断をおこなうサービスです。DoS 攻撃はシステムのボトルネックとなる箇所の資源を枯渇させる攻撃であり、攻撃により、ファイアウォールや IDS/IPS といった他の資源が先に尽きる可能性があるため、DoS 対策サービス用のアプライアンスはそれらよりインターネット側に設置される必要があります。

メールフィルタリングサービス

メールの流通を監視し、外部への機密情報の漏えいやスパム/ウイルスメールの流入等をフィルタリングによりブロックするサービスです。機密情報の漏えいや、ウイルスの侵入といった脅威を防ぐことはもとより、スパムメールをフィルタリングすることで、メールサーバーやメール受信者の負荷を軽減することが出来ます。

UTM（Unified Threat Management：統合脅威管理）サービス

主に中堅・中小企業を意識したサービスとなりますが、ここまでに紹介したファイアウォールや VPN 接続の基本機能にウイルスチェック、不正侵入防止等の機能、さらには不正な Web サイトへのアクセスを遮断する Web フィルタリング、を統合し、コストメリット及び維持管理の利便性を追求したサービスです。幅広いレイヤーの対策が可能ですが個別の拡張要件に対応が難しい場合もあるため、サービス利用時には十分な検討が必要となります。

コラム⑤ ネットワークセキュリティのチェックポイント

ファイアウォールのような機器は一般に普及しているため、シンプルな利用方法であれば利用者が自身で運用する場合もあります。一方で、IDS/IPS や WAF、ADS といった機器の運用では高い専門知識が必要となるため、専門知識を持った事業者に運用を委託する場合も少なくありません。その際には、事業者と利用者側でサービスについて合意することが重要となります。以下では利用者側でサービスとポリシーの整合性確認の際によく参照される項目を紹介します。

容量の共有./専有

例えばファイアウォールのサービスを利用する場合、ファイアウォールには許容する帯域の容量があります。その容量を、複数の利用者で共有するか、または利用者単体で専有するかという二つのタイプのサービスがあります。容量の共有時においては、利用者毎のカスタマイズを柔軟にしようとすれば、データセンターの運用が大変になり(運用コストが上がる)、データセンターの運用コストを抑えようとすると利用者毎の柔軟性が犠牲になるというトレードオフの関係が成立します。

レポートや連絡の有無や内容

ネットワークセキュリティサービスのレポートの閲覧や、緊急時の通報等が必要となる場合があります。そういった需要に合わせて、トラフィック等の情報をデータセンター側が用意した Web ページ上で確認できる、あるいは IDS/IPS や WAF で攻撃を検知した際に、利用者にレポートを提出する、といったサービスがあります。

サービスの設定変更に伴う制限

サービスの利用の際、利用者が設定可能な範囲を明確にする必要があります。利用者が緊急で設定変更をおこなうような場面も想定されるため、設定変更可能な時間帯、設定変更までの時間、設定変更による費用の発生等を明確にしておく必要があります。

サービスを受けられるトラフィック制限の有無や限度

サービスによって、トラフィックの制限を明確にする必要があります。例えば、ある期間（一日やーヶ月等）のトラフィックに制限値を設け、制限値までしかサービスを利用できなくさせる（または保証しない）、ある値を超えた場合は別途費用が発生する等です。

サービスを受けられるプロトコルの種類、制限の有無

サービスによって、監視することの出来るプロトコルを明確にする必要があります。例えば、アンチウイルスサービスを利用する場合に HTTP、FTP、SMTP だけしか対象とせず、それ以外のプロトコルについては対象外になるような場合も考えられます。

障害対応時間

サービスによっては、障害対応可能な時間を明確にする必要があります。よくある形態としては、平日 9 時～18 時といった平日日中帯のみや、平日休日問わず 24 時間 365 日対応する形態があります。また、障害を復旧するにあたり、目標時間を定めるかどうか検討する必要があります。

2.3 運用サービス

この節では、データセンターのオペレーション・マネジメントサービスとフルアウトソーシングサービスについて紹介します。

2.3.1 オペレーション・マネジメントサービス

独自に情報システムを運営している多くの企業は、以下のような悩みをかかえています。

- 日々報告されるぜい弱性の収集に苦労している
- 24 時間・365 日の体制が確保できない
- 複数のベンダーに保守の問い合せが必要
- エンジニアを確保できない

これらに加え、ネットワーク機器、特にセキュリティに関連する機器は設定・運用・管理が複雑で、対応の即時性が求められるケースも多くあります。これら企業からの外部委託のニーズを満たすため、データセンター事業者の多くは、機器の運用から監視、障害対応に至るまでを通貫して提供しています。このようなサービスはオペレーションサービス、あるいはマネジメントサービス[12]と呼ばれ、以下のようなサービスを提供しています。

- 情報通信機器監視
  - 情報通信機器の監視を 24 時間/365 日行います。
- 温度監視
  - 情報通信機器周辺の温度が適切に保たれているか監視を行い、温度の上昇による機器の故障を未然に防ぎます。
- 電流監視
  - 情報通信機器に供給される電流を常時計測して閾値を超えていないかの監視を行い、機器の故障を未然に検知します。
- 障害対応
  - 障害検査や保守ベンダーとの窓口となり、24 時間・365 日オンサイトまたはリモート接続による障害対応を行います。
- レポーティング
  - 定期レポートの提出や、定例会での報告をおこないます。セキュリティ対応製品のぜい弱性情報の提供やパッチの運用作業をおこないます。
- リモート設定変更
  - お客様の依頼に基づき、リモートで設定変更作業を行います。

これらオペレーション・マネジメントサービスの全体像を図 4 に示します。

12： マネジメントサービスを専門に提供する事業者を特に MSP(Management Service Provider)と呼ぶことがある

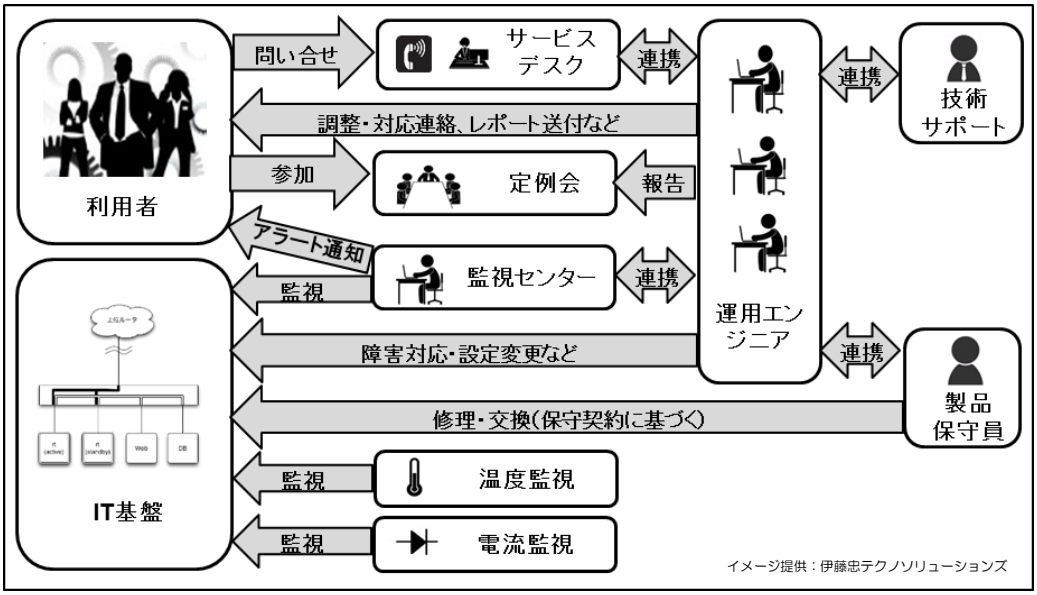


図 4　オペレーション・マネジメントサービスの構成例

2.3.2 フルアウトソーシングサービス

昨今、情報システムに関してコスト削減や省人化、効率化の観点から、自社で情報資産を持たず、情報システムに関わる企画や運営などを担当する情報システム部門（窓口）だけを残し、それ以外は外部のメーカーやベンダーなど、専門の企業に運用を任せる企業が増えています。このように「所有」から「利用」へビジネスモデルを転換する経営戦略を「フルアウトソーシング」といいます。

フルアウトソーシングを導入することで、企業の専門性を高めることに注力できるとともに情報システム部門の観点を組み入れた企業内の構造改革が進むことでコアコンピタンスが強化され、企業をより一層成長させます。

こういった背景により多くのデータセンター事業者は、情報通信機器の構築運用、OS からミドルウェアの管理や障害の一次対応はもとより、二次対応までをワンストップによるフルアウトソーシングサービスを提供しています。

データセンター事業者が提供するフルアウトソーシングサービスは、あたかも社内の情報システム部門の一部としての機能をサービスとして利用することができます。このことによって、利用者にとってはデータセンター内で作業することはもとより、構築と運用に社内の専門家を振り分けることから解放され、品質の向上を図ることができます。

また、データセンター利用者全てに対してコンシェルジュ的な要素を持ったスタッフを割り当て、運用に関する相談など、顧客の窓口となって全面的にサポートするサービスを提供している事業者もあります。

2.4 サービスを支える構造

データセンター事業者は、前節で紹介したように様々なサービスを提供していますが、事業者がこうしたサービスを適切なコストで提供できる大きな理由は、データセンターのサービスを提供するための設備（建物設備、ネットワーク設備等）、データセンター要員等の資源をデータセンターの利用者間で共有していることにあります。

一方で、セキュリティの観点からは、資源が必要な部分で共有されているだけではなく、適切に分離されていることが重要になります。そのため、データセンターの利用者とデータセンター要員は、サービス内容に応じた設備的資源への適切なアクセス権限や、利用者自身の資源に対する適切なアクセス権限を、厳密に規定・運用して、サービスを提供していく必要があります。

データセンターのサービスでは、このデータセンターの利用者とデータセンター要員等に付与したアクセス権限によるアクセス制御だけでなく、何らかの形で証跡を保持し、監査できることが重要な要件となる場合もあります。

これらの点を鑑みると、データセンターのセキュリティを理解するにあたっては、データセンターの資源を共有するサービスがどのような構造から提供されているかを、まず十分に理解する必要があります。

そこで、本節ではデータセンターがサービスを提供する構造を４つの側面から説明します。一つ目の側面は物理的な「アクセス制御」や「外周監視」の考え方を理解するための「空間構造」、二つ目の側面はデータセンター内の設備(ビル設備)とそれを制御・管理するビルディングオートメーションの側面から見た「設備システム構造」、三つ目の側面はデータセンターの基本的なサービスであるネットワークサービスを標準化されたモデルから紹介する「ネットワーク構造」、そして、四つ目の側面は、データセンターのより基本的なサービス（下位のレイヤーのサービス）が、利用者の様々なレイヤーのサービスを支える構造であるデータセンターの「サービスレイヤー構造」を説明します。

2.4.1 空間構造

データセンターのサービス、特にハウジング（コロケーション）サービスの側面の一つに 「建屋・設備・運用・人材の共有」があります。ハウジングサービスを提供するデータセンターでは、様々な情報システムが設置可能な汎用の空間と、それを運用するための様々な設備を保有していますが、これらをセキュリティ面から考えた場合、利用者への場所貸しの区画や、設備等が設置される区画は、物理的アクセス制御と監視が行われるべき「セキュリティ区画」と考えることができます。この「セキュリティ区画」を空間の性質から複数設定（ゾーニング）し、「正当な目的を持たない要員や利用者、その他のデータセンター内で活動する人をセキュリティ区画の中に入れない」よう設計することがセキュリティのアプローチとして広く一般的に用いられています。以下に、このゾーニングを考えるために、データセンターを構成する空間構造の要素を紹介します。

立地

データセンターの立地はデータセンターの性質を理解する上で重要な項目となっています。例えば、利用者が直接来訪することを想定しているデータセンターの場合、アクセスの利便のよい都市

部に立地し[13]、それを訴求していることが多いようです。対して、利用者がデータセンターに直接来る必要のないホスティングサービスやクラウドサービス等のタイプのサービスを志向している場合、アクセスが多少不利であっても郊外に立地することで地価を抑え、サービスの価格を低減すること等を目指しているデータセンターが見られます。また、可用性の観点からは地震や津波のリスクに着目し、立地している地盤や海抜高度について訴求しているケースが見られます。

敷地

データセンターの敷地はデータセンターの規模を決めると同時に、外部からの緩衝区画としても機能します。データセンター来館者のための駐車スペースや、サーバーラックや大型計算機のような特殊なサイズの資材を搬入するための区画の有無はデータセンター利用時における利便を左右します。また、近年注目を浴びているモジュール/コンテナ型データセンターにおいては、敷地面積がデータセンターの将来の拡張性に直結します。

建屋

データセンターの建屋はデータセンター専用の建屋と、他の目的（一般的にはオフィス利用）で建設された建屋に分類することができます。データセンター専用の建屋の場合、サーバーラックへの高い密度での実装を実現するための高い床耐荷重や階高が確保されていて将来の拡張性を確保しやすくなっていることが特徴として挙げられます。対して他の目的で建築される建屋の場合は、オフィスにデータセンター内のシステムの開発・運用要員を配置することでより効率的な開発・運用が可能になる一方で、拡張性や、付随する電源面、空調面、セキュリティ面での設計が最適化されていないため効率が悪くなってしまっている可能性があります。

エントランス区画

エントランス区画とは建屋に入ってから最初の本人認証を受ける検査区画までの区画です。このエントランス区画は、打ち合わせや物品の受け渡し等、必要に応じて利用者以外が利用できる場合があり、待合室や、簡単な打ち合わせのためのスペースが用意されていることがあります。

検査区画

検査区画はオフィスビルには無いデータセンター特有の区画で、入館時・退館時の本人確認や持ち物検査等が実施されます。これらの検査をクリアできないとゲートによって次の区画（共用区画）へと進むことができない構造になっています。より高いセキュリティが要求されるデータセンターでは、検査区画の前後をゲートで区切って「逃げられない区画」としている場合もあります。

13： 他のメリットとして都市部に集中するIX（Internet Exchange）との距離が近く、インターネット接続の遅延時間が低減できるといった点が訴求されることがある。

共用区画

検査区画での検査を終え、サーバー室にアクセスするまでの廊下、エレベータ等の他、利用者等が共通に利用する休憩室などの区画になります。多くのデータセンターにおいてこの区画には、一定の本人認証を受けた権限者しかいないため、そのことを確認するために ID カードの提示義務等が生じる場合があります。

サーバー室（専用区画）

サーバー室は、利用者の情報通信機器が設置される区画として設計されていて、空調・電気設備を含めた室全体が情報通信機器の運用に特化され、かつ、情報通信機器を守るための区画です。

サーバー室は、大きく二つの種類に分けることができます。一つはハウジングサービスを提供する複数のサーバーラックを収容し、電源や空調、ネットワークをそれぞれサーバーラックやケージへと分配する共有空間としての役割を担っている「共有サーバー室」です。もう一方は、サーバー室自体も複数のサーバーラックや大型計算機等を使う情報システム一式を預けるための空間として、サーバーラックのように一つの「専有区画[14]」として利用者に提供される「専有サーバー室[15]」と呼ばれるものになります。

高いセキュリティを要求されるデータセンターのサーバー室では、塵芥がサーバー室へ入り込むことや共連れを防止するために前室が設置されている場合があります。

サーバーラック

サーバーラックは情報通信機器を格納する空間として提供される最小単位です。多くのハウジングサービスにおいては、その中だけが利用者に専有されることから、サーバーラックの内外はセキュリティのために十分区画されている必要があります。また、サーバーラックは利用者とデータセンター事業者の責任分界ともなるため、セキュリティ上のみならず、電源やネットワークの提供単位として契約上でも非常に重要な意味を持ちます。

オフィス

データセンターには事業者がシステムの運用・監視を行う部屋としてオフィススペースが用意されている場合があります。また、一部の部屋を利用者向けのオフィススペース[16]として提供している場合もあります。このオフィススペースでは構内配線を使ってサーバー室内のサーバーラックと専用のネットワークを構築しシステムの運用・監視室として利用できる他、災害時の事業継続のためのオフィススペースとしても用いることができます。

14： 本ガイドブックでは「専用」は特定の目的のために用いられる物を示すことに用い、「専有」は特定の利用者によって用いられる物を示す。

15： 専有区画をサーバー室単位とするか、サーバー室内のケージ単位とするか、サーバーラック単位とするかは、契約やポリシーによってさまざまとなっている。また、セキュリティレベル間の境界においても、運用の利便や消防法との整合の為に壁の設定などで物理的に区画することが出来ていない場合がある。

16： プロジェクトルームやレンタルオフィスとも呼ばれる

設備室（電源室、空調機械室、MDF 室、ネットワーク室等）

設備室は変電、蓄電、発電といった電源に関係する機能を持った電源室や、サーバー室の空調設備を納める空調機械室、外部ネットワーク回線を導入分岐する MDF 室/ネットワーク室といった、データセンターで複数の利用者が共有する機能を提供する室です。この室は、利用者が直接アクセスすることはありませんが、データセンター要員やデータセンター出入り業者等が入室します。データセンター事業にとって、最も重要なインフラであり、厳密な管理が行われるべき領域であると言えます。

監視室(防災センター等)

監視室(防災センター等)では、データセンター全体のファシリティ管理等が行われます。

これらの要素を含む典型的なデータセンターの空間構造を図 5 に示します。

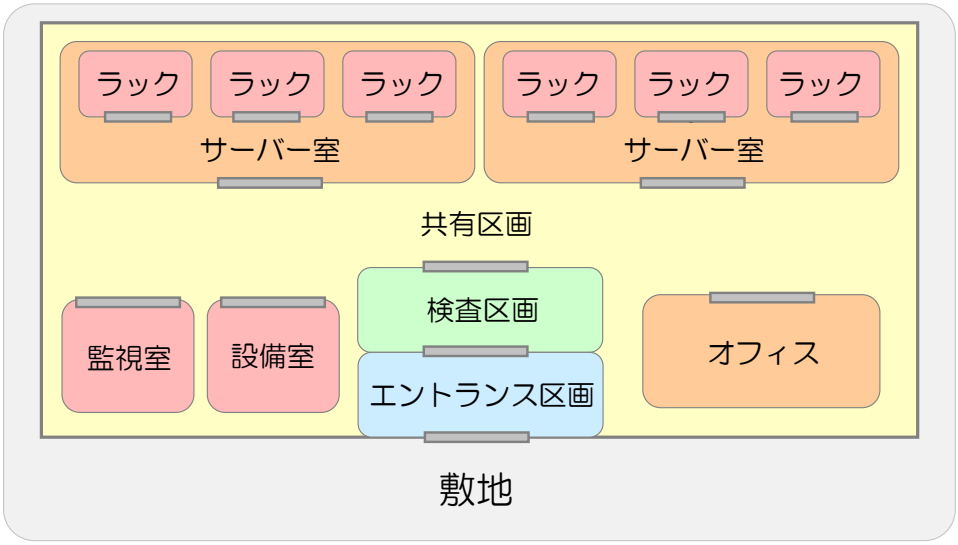


図 5　典型的なデータセンターの空間構造

データセンターでは、こうした「空間構造」をベースとして、正当な目的を持たない要員や利用者、その他のデータセンター内で活動する人をセキュリティ区画の中に入らせないための物理的アクセス制御と監視が行われています。データセンターにおいては、主にこの「空間構造」の構成要素を壁により区画することで物理的なセキュリティを実現します。また、データセンターでは図 5 における「共有区画」-「サーバー室」-「サーバーラック」の関係のように、構成要素を重要度の順に入れ子構造とすることで、空間の効率的な共有と、アクセス制限を実現しています。

データセンターのサービスの特徴は「共有」にあることから、「空間構造」に基づいてセキュリティ区画を明確にし、利用者等が共有する区画と専有する区画の間の物理的アクセス制御を実現することは、重要な役割を担っています。一方で、空間構造間の区画が十分になされているだけでは、権限を詐称するなどしてアクセス制御を回避することで攻撃者が侵入できてしまうため、データセンター内の権限管理と組み合わされて初めてセキュリティの確保が実現できる、という点にも留意が必要です。

コラム⑥ データセンターの地域分散と BCP 対策

データセンターの選定は、企業にとって難しい選択事項のひとつです。利用を検討している企業のビジネスモデルやセキュリティに関する規定など様々な検討を重ね選定を行っていると思いますが、多くの場合、運用に携わる従業員が勤務するオフィスから近くにある交通の便が良いデータセンターを選択されていることでしょう。管理している情報通信機器に何らかの障害が発生した場合など、すぐに駆けつけることができるというメリットは、手放しにくい条件です。

しかしながら、日本は地震大国であり阪神淡路大震災や東日本大震災など、大都市が被災するようなことも発生しています。データセンターは、地震や停電などの災害に対する備えも行なっていますが、データセンターだけ堅牢であれば、利用企業の事業活動は継続できるのでしょうか？

もちろん、違います。データセンターだけが堅牢であっても周辺の環境に何らかの変化によって、事業活動に影響が出ることもあります。

そのため各企業では、震災などの有事に備え BCP(事業継続計画)を策定していることと思います。利用するデータセンターの BCP を考慮する場合、「同時に被害を受けない」ということが一番重要です。そのためには、主に以下を点について考慮することが望ましいです。

- データセンターは、異なる地域に立地しているか
- 電力は異なる事業者から供給されているか

また、データセンターの地域分散を考慮する上では、電力会社がどこに発電所を設置しているのか把握することも大切です。たとえば東京電力は、新潟県や福島県などでも発電し、首都圏に届けています。言い換えれば、新潟県や福島県で発生した災害によって首都圏への電力供給能力が低下する恐れ（リスク）があるということです。したがって、首都圏にあるデータセンターと、新潟県や福島県にあるデータセンターで地域分散とする場合には、残留リスクを考慮する必要があります。

近年多くのデータセンター事業者は、三大都市圏だけでなく本州以外の九州や沖縄、北海道などの地方にもデータセンターを構えており、利用企業の選択肢も増えてきています。事業活動を継続させるためにも、データセンターの地域分散は、理にかなった BCP 対策です。

2.4.2 設備システムの構造

データセンターのサービスにおいて、利用者間で共有される資源・設備には空調、電源設備などがあります。空調、電源設備等の稼働状態を監視、管理、制御、記録するためにビルディングオートメーションシステム（BAS：Building Automation System）[17]が稼働しています。ビルディングオートメーションシステムは、ビルにおける空調・衛生設備、電気・照明設備、防災設備、セキュリティ設備（物理セキュリティが対象）などの建築設備を対象とし、各種センサー、メーターにより、室内環境や設備の状況をモニタリングし、運転管理、および自動制御を行います。

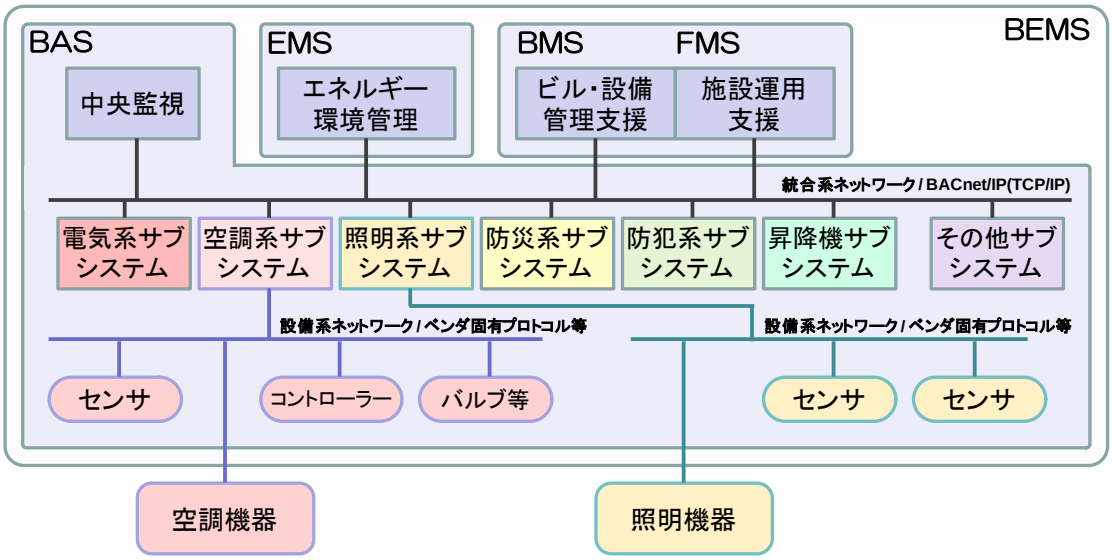


図 6　BEMSの全体イメージ

また近年で BEMS（Building and Energy Management System）と呼ばれるシステムを導入しているデータセンターもあります。BEMS は、室内環境とエネルギー性能の最適化を図るためのビルの管理システムのことをいいます。図 6 に全体イメージを示します。

基本機能であるビル管理の自動化を実現するビルディングオートメーションシステムの他に、エネルギー環境管理システム、設備管理支援システム、施設運用支援システムまで含めた範囲が BEMS と定義されています。表 4 に公益社団法人空気調和・衛生工学会による BEMS 機能の分類を示します。

17：　一部の学会等では Building Automation and Control System（BACS）という呼称も使われている

表 4　ＢＥＭＳの各要素と機能

	BEMS			
一般的な名称	ビルディング オートメーション システム	エネルギー 環境管理 システム	設備管理支援 システム	施設運用支援 システム
	Building Automation System	Energy Management System	Building Management System	Facility Management System
利用者	ビル管理技術者	ビル管理技術者	ビル管理技術者	ビルオーナー
		設計・施工者		ビル管理技術者
		性能検証担当者		
主な機能	設備機器状態監視	エネルギー管理	設備機器台帳管理	資産管理
	警報監視	室内環境管理	修繕履歴管理	ライフサイクル マネジメント
	運転管理	設備運用管理	保全スケジュール 管理	図面管理(CAD)
	設備の自動制御		課金データ	

ビルディングオートメーションシステムに接続する設備には以下のようなものがあります。

- *空調設備*
  - 室内の温度、湿度、清浄度を調整する空気調和機、冷凍機、搬送ポンプ等の熱源設備、配管、ダクト、自動制御設備等を含んだ設備。
- *衛生設備*
  - 建物及び人の活動に必要な水や生活排水等を供給、処理する設備。給水設備、排水設備、給湯設備、排水を再利用する中水設備、雨水処理設備等。
- *電気設備*
  - 建物に電力を安全に供給するための設備。受変電設備、自家発電設備、無停電電源設備、幹線設備、分電盤設備等。データセンターにおいては、一般に電源設備を示す。
- *照明設備*
  - 建物の照明を提供する設備。
- *防災設備*
  - 人為的不注意や地震等の天災に伴い発生する火災の予防、早期発見、警報発報、消火等をおこなうための設備。消防法や建築基準法で規制されている。
- *セキュリティ設備*
  - 窃盗や破壊等の意図をもった者の侵入等を防止するための物理セキュリティ設備。現在は IT セキュリティ等も含んだものへ解釈が拡大している。

これらの設備の多くは前述の設備室に設置され、必要のない人間がアクセスできないよう区画されています。

2.4.3 ネットワーク構造

データセンターのサービスにおいて、利用者間で共有される資源・設備には、空調、電源そしてネットワークサービスを提供するためのネットワークがあります。現在の多くのデータセンターは、インターネット接続を前提した設備・サービスを提供しています。また、近年では、企業内の基幹業務、イントラネットを丸ごとデータセンターにアウトソーシングすることも多くなってきており、そのため企業と高速な専用線で接続するサービス形態も多くなっています。

データセンターは様々なネットワークサービスを提供するために、データセンター内部に非常に高速で、大容量、そしてフレキシブルなネットワーク設備を持っています。こうしたデータセンターの内部ネットワーク設備は非常に高価なものですが、データセンターではこうしたネットワークサービスのためのネットワーク設備とその運用を利用者間で「共有」することにより適切なコストでサービスを提供しています。

データセンターにおけるネットワークサービスは、共有によるコスト削減が可能な一方、共有によるセキュリティ上の問題がないような仕組みや運用が必要になります。特にセキュリティ上の秘匿性、完全性等のためには、適切な分離、物理的・論理的アクセス制御が重要になります。

データセンターのネットワークの概念は、大きく二つのレイヤー で表現することができます。一つは物理的なケーブル配線（ケーブリング）等により実現される「物理ネットワーク」、もう一つは「物理ネットワーク」上のスイッチ・ルーター等のネットワーク機器で実現される「論理ネットワーク」です。

「物理ネットワーク」は、物理的なケーブルとケーブル配線等で実現されますが、データセンターにおいては、この物理的なケーブルを大量に使用します。データセンターにおける物理ネットワークの構造、構成の標準には、2005 年 4 月に米国規格協会（ANSI）等が発行した ANSI/TIA-942（Data Center Design Guidelines and Structured Cabling Standards）があります。図 7 に ANSI/TIA-942 において代表的なデータセンターの配線トポロジーとして紹介されているモデルを示します。

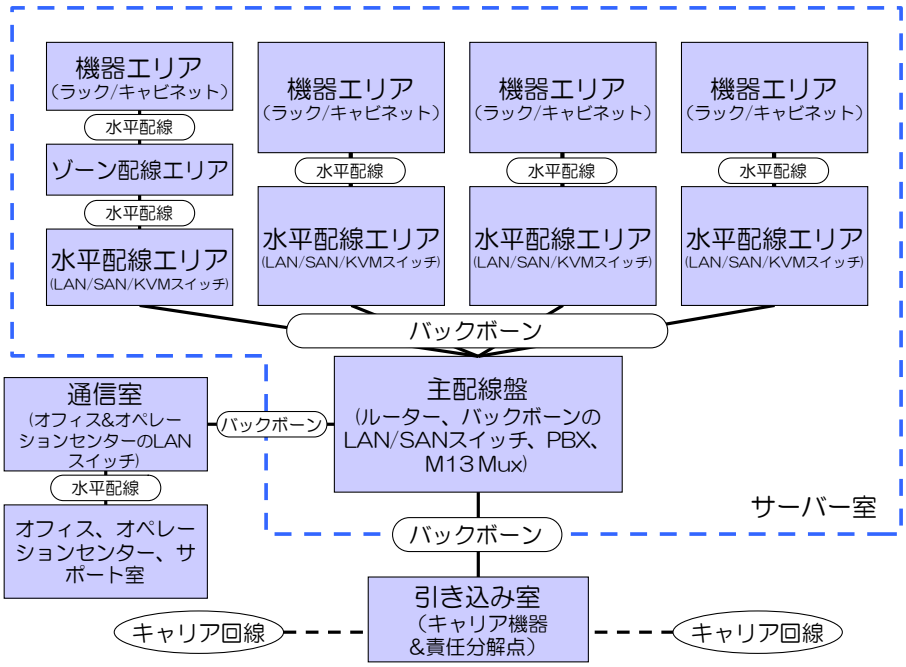


図 7 ANSI/TIA-942 におけるデータセンターのケーブル配線のモデル

このような物理ネットワークにおける一般的な脅威には、物理的なケーブルの切断や、タッピング等による盗聴等があります。そして、これらの脅威に対する対策の例として、物理ネットワークを担当するデータセンター要員のみがアクセス可能な「セキュリティ区画」に物理的なケーブルを敷設する、といった「空間構造」に基づく物理的アクセス制御が考えられます。しかし、現在のデータセンターのネットワークは、人体における神経の如く、データセンターの隅々まで張り巡らされているために、注意深くその設計がなされている必要があります。図 8 に「物理ネットワーク」とデータセンターの「物理セキュリティ区画」と、この「セキュリティ区画」にアクセスできる[18]「人」の関係の例を示します。

データセンターのネットワーク設備は、物理的な配線を担う「物理ネットワーク」だけで構成されている訳ではなく、ルーター、スイッチ等のネットワーク機器から構成される論理的接続を担う「論理ネットワーク」も重要な役割を果たしています。

現在のデータセンターはその規模から非常に大量の物理配線を扱う必要がありますが、利用者の契約変更等の際の物理ネットワーク構成の変更コストを最小限にするために、ルーター・スイッチ等のネットワーク機器の「論理ネットワーク」の構成変更、構成管理を中心にネットワークが構築されています。この「論理ネットワーク」によるネットワークの構成変更、構成管理への要求は、近年、クラウドサービス等の提供等の要求から更に複雑になりつつあり、「論理ネットワーク」の進化に加え、サーバー仮想化に対応した「ネットワークの仮想化」が進んでいます[19]。

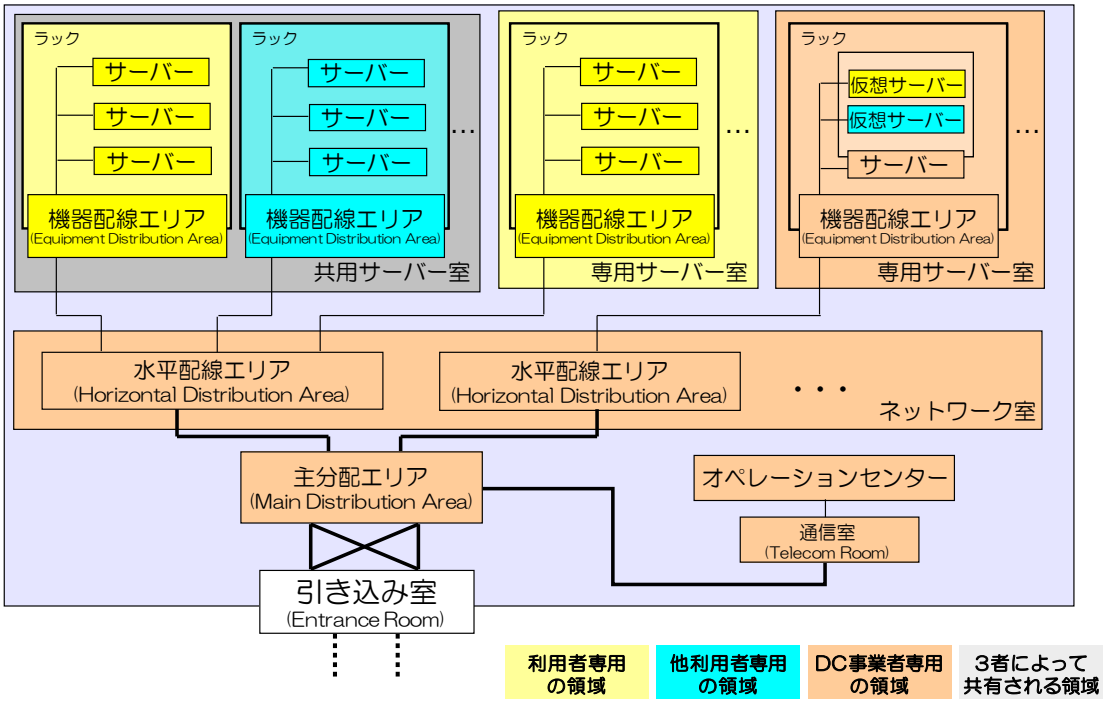


図 8 物理ネットワークと物理セキュリティ区画の関係

一方で、この「論理ネットワーク」のセキュリティは「物理ネットワーク」のセキュリティに依存しています。例えば、「論理ネットワーク」のセキュリティは物理的な実体としての情報通信機器のセキュリティとネットワーク管理担当データセンター要員による運用にも依存する、といった

18： セキュリティ区画内を物理ネットワーク配線が通っているからと言って、必ずしもその配線にアクセスできるわけではない（手の届かない/届きにくいところに設置する等の工夫が施されている場合が多い）点にも留意が必要です

19：クラウド時代に要求されるデータセンターのネットワークについては、日本データセンター協会の「データセンターネットワークリファレンスガイド」において詳細な解説があります

関係があります。逆に、「物理ネットワーク」のセキュリティ、例えば、物理的なケーブルの盗聴を「論理ネットワーク」における暗号化で防ぐといった考え方に立つこともできますが、データセンターの内部においては「物理ネットワーク」のセキュリティを保つことが重要であることには変わりません。

以上のように、データセンターのネットワークサービスは、より基本的なインフラサービスが、その上のレイヤーのサービスを支えるという構造になっています。レイヤー構造とそれぞれのレイヤーを管理するデータセンター内の主体の関係を図 9 に示します。

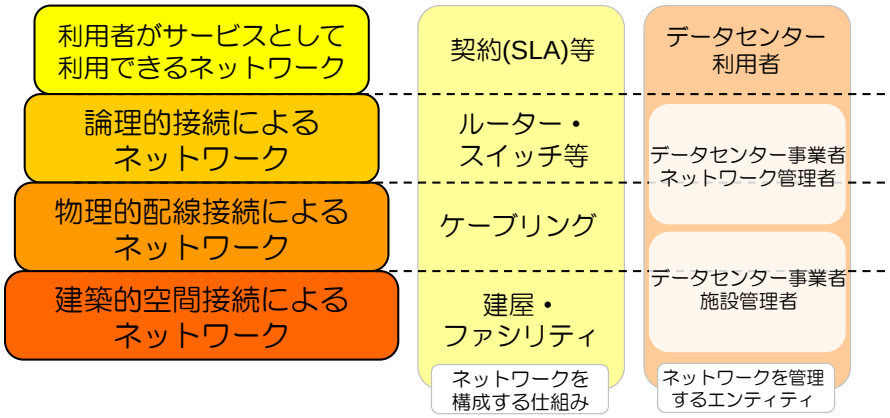


図 9　データセンターインフラのレイヤー構造

2.4.4 サービスレイヤー構造

データセンターのサービスは、ネットワークサービスに限らず、より基本的なデータセンターのサービスがその上のレイヤーのサービスを支えるという構造になっています。このことは現在大きなトレンドとなっているクラウドサービスにも当てはまり、クラウドサービスは、データセンターの基本サービスの上でサービスが提供されていると言えます。

クラウドサービスと呼ばれるサービスの中には、従来データセンターが提供してきたホスティングサービスの進化系である IaaS があります。IaaS は、ハウジング、ネットワークといったデータセンターの基本サービスの上で物理サーバーを運用し、この物理サーバー上で仮想サーバーを実行し、利用者に提供しています。図 10 に典型的な多目的なデータセンターにおけるサービスのレイヤー構造を示します。

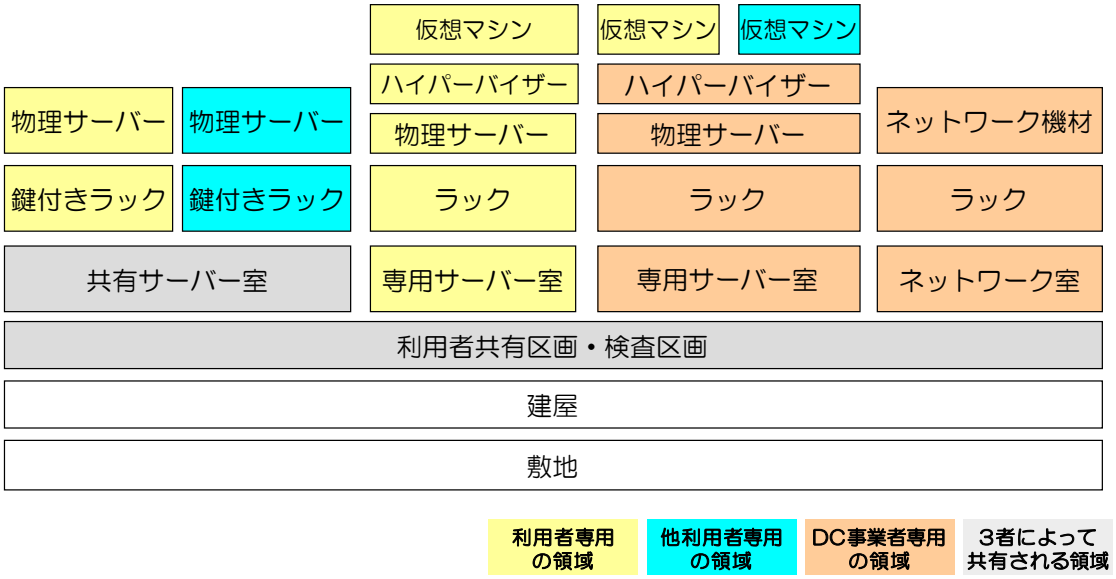


図 10　データセンターの提供するサービスのレイヤー構造

データセンターのセキュリティを考えた場合、空間構造による多段の「セキュリティ区画」がデータセンターのサービスのレイヤー構造とそのセキュリティを提供していると考えられます。

また、こうしたことはクラウドサービスである IaaS のセキュリティにも当てはまります。「仮想サーバー貸し」の場合、「利用者」と「データセンター事業者」の「セキュリティ境界」に当たるのは「仮想マシン」のインターフェースになります。同様に、考えるならば、コロケーションでサーバーラックが設置されるサーバー室は IaaS における仮想マシンの実行環境であるハイパーバイザーにあたります。

つまり、仮想マシンはハイパーバイザー上でそれぞれ隔離され提供されるため、仮想マシンを利用者が専有する「論理的なセキュリティ区画」として考えることができます。

一方で、ハイパーバイザー上の仮想マシンは（必要に応じていつでもホストの物理サーバーを移動できるとは言え）特定の物理サーバー上で実行されることになります。そして、この物理サーバーは、IaaS を提供するデータセンターのサーバー室内のサーバーラックに格納されます。すなわち、仮想マシンであっても、仮想マシンが実行される実体としての物理サーバーは、データセンターのサーバー室内のサーバーラックという「セキュリティ区画」に置かれることになります。

クラウドサービスというと、全ての資源は抽象化され、物理的環境とは切り離されると考えられがちですが、実際は様々な物理的な仕組みによって支えられていて、そのひとつには「(ホストとなる物理サーバーが設置される)サーバーラックの物理的セキュリティ」のような、コロケーションサービスと変わらない項目が含まれていることに留意が必要です。

第３章　リスク分析と管理策

この章では、データセンターのサービスにおけるリスクを説明した後、このリスクに対する「管理策の考え方」を提示し、その上で、実際のデータセンターで実施されるセキュリティ管理策がどのように実現されているかを「架空のデータセンター」を元にして紹介します。

「データセンターの利用におけるリスク」の節では、典型的サービスであるハウジングサービス、ホスティングサービスそしてクラウドサービスを想定したリスク分析を提示しています。「セキュリティ管理策の考え方」の節では、主に「人為的脅威」に関する管理策の「考え方」を示しています。「実際にデータセンターで実施されるセキュリティ管理策」の節では、物理的セキュリティにフォーカスして、「架空のデータセンター」を設定し、そのデータセンターで実施される管理策を見ていくことで、データセンターにおけるセキュリティの実現がどのようになされているか理解することができるようになっています。

データセンターの利用者は、本章を読むことにより、データセンターが提供するサービスの一般的なリスクと、そのリスクの分析方法、リスクに対応する脅威への管理策の考え方、そして一般的なデータセンターにおける管理策の事例を理解することができます。

3.1 データセンターの利用におけるリスクの分析

データセンターを利用して情報システムを構築する際のリスク分析には、資源の共有や組織間の情報開示の問題といった特有の勘所や難しさがあります。本節では、データセンターを利用する際のリスク分析について、リスク分析の手法について紹介したうえで、ハウジングサービス、ホスティングサービス、クラウドサービスの三つのタイプのサービス例を元に紹介します。

なお、本節ではデータセンターにおける脅威として、人によって巻き起こされる脅威(人為的脅威)に注目してリスク分析の手法を紹介しています[20]。

3.1.1 リスク分析の手法

一言にリスク分析と言っても、その背景や目的から様々な取り組み方が考えられます[21]。本書でのリスク分析では、情報システムに的を絞ったリスクマネジメント手法を紹介している NIST(National Institute of Standards and Technology：アメリカ国立標準技術研究所)の「Guide for Conducting Risk Assessments （SP800-30）」に基づき、以下の手順でリスク分析をおこないます。

手順.1	システムの特徴定義
手順.2	システムの**脅威**を特定する
手順.3	システムの「ぜい弱性」を特定する
手順.4	既に実施されている管理策を分析する
手順.5	事件・事故の**発生可能性**を判断する
手順.6	事件・事故の発生した場合の**影響**を分析する
手順.7	リスクの判断をする

3.1.2 リスク分析に必要な情報とその考え方

前述したリスク分析の手法のうち、システムの設計の影響が比較的少なく、一般的な知見として取り扱いやすい「システムの脅威の特定」、「事件・事故の発生可能性の判断」、「事件・事故の発生した場合の影響」の 3 点について、それらを検討するにあたっての考え方・アプローチを紹介します。

システムの脅威の特定における考え方

リスク分析においてはその初期のステップとしてシステムの脅威を特定することが必要になります。前述の「Guide for Conducting Risk Assessments （SP800-30）」ではシステムの脅威となる事象を以下のように分類しています。

20：自然の脅威や環境の脅威に関しては「JDCC ファシリティスタンダード」において管理策を中心に解説されている
21：本書で紹介するリスクマネジメントの手法を紹介するドキュメントとしては NIST SP800-30 Rev.1 の他にも ISO/IEC27010 や ISO/IEC31000 が知られている。

1. 自然の脅威
2. 環境の脅威
3. 人為的脅威
    - 偶発的行為
    - 意図的な悪意ある試み
    - 悪意はないが故意にセキュリティを迂回する試み

この分類では人為的な脅威について、偶発的-意図的、悪意の有無によってより細かく分類していますが、同じ人為的脅威であっても、属性によって発生可能性や影響の程度が異なるため、その属性を分けて扱う必要がある場合があります。

データセンターにおける人為的脅威源の分類には、例えば以下のような分類が考えられます。

1. データセンター利用者
    (ア) 自社の社員(作業要員)
    (イ) 自社で契約した委託作業要員
2. データセンター事業者
    (ア) データセンター事業者の社員(作業要員)
    (イ) データセンター事業者の委託作業要員
3. データセンターの共同利用者
    (ア) サーバー室の共同利用者
    (イ) データセンター(建屋)の共同利用者
4. 1～3 の何れにもあてはまらない者（部外者）

この分類は、「何をもって」それぞれの人をコントロールすることができるかによって行われています。例えば、データセンター利用者の自社の社員に対するコントロールは一般に雇用契約や就業規則で行われます。対して、データセンター利用者が契約する委託作業要員のコントロールは業務委託契約によって行われます。同様に、データセンター事業者の関係者も業務委託契約コントロールされ、データセンターの自社外利用者に対するコントロールはデータセンター事業者が定めるデータセンターの利用規約などによって行われます。さらには、データセンターの非利用者に関しては、データセンターの所在する国の法律等によってコントロールされることになります。

なお、データセンターのサービスは様々なスケールのハウジング、ホスティング、クラウドサービス等が階層的に組み合わされて提供されているため、例えばクラウドサービスの利用者においては、上の分類における「データセンター事業者の関係者」に相当する「クラウドサービス事業者の関係者」や、「データセンターの自社外利用者」に相当する「クラウドサービスの自社外利用者」といった脅威源に加え、「クラウドサービス利用者が利用しているデータセンターのクラウドサービス事業者外利用者」といった脅威源も、場合によっては想定する必要があります。

事件・事故の発生可能性の判断における考え方

事件・事故の発生可能性を見積もるには大きく二つの視点からのアプローチが考えられます。一つには、これまでに、どのような事件・事故が実際に発生しているか、という視点があります。もう一方の視点として、事故・事件の発生を予見させる環境の変化(例：情報システムに使われている技術・製品のぜい弱性が広く知られるようになる、治安の悪化、事件が社会に及ぼすインパクトの拡大等)があります。

事件・事故の発生頻度を理解する一つの目安の例として、以下のような分類が考えられます。

-緊急対応組織を立ち上げて対応を行う	(数年に 1 回)
-業務見直しや、監査などで対応を行う	(年に 1～数回)
-定常的な業務改善活動を通じて対応を行う	(日常業務の一部)
-日常業務に対応が組み込まれている	(主要な日常業務)

事件・事故発生した場合の影響における考え方

事故・事件発生時に想定される被害は、その被害を評価する人がどのような立場にいるかによって、同じ事象であっても様々に変化します。一つの例として、データセンター利用者の経営者の視点からは以下のような影響の分類が考えられます。

-資産の喪失
-信用失墜
-売上機会の減少/事業運営コストの増加
-人的損害・過大な業務負荷

また、事件・事故の発生によって、どの程度の影響が及ぼされるかも重要な指標となります。前述の影響の分類同様、データセンター利用者の経営者の視点を例によるならば、

-経営危機
-営業利益の減少(1 割未満)
-売り上げの減少/間接費(販売管理費)の増加
-担当者の業務負荷の増加

といった形で影響の程度を分類することが考えられます。

3.1.3 ハウジングサービスにおけるリスク例

ハウジングサービスは、データセンターの一部を借りて利用者の所有する情報通信機器を設置、稼働させることができるサービスです。ここでは、ハウジングサービスのリスク分析をおこなうために、典型的なハウジングサービスの以下の契約を想定することにします。

- 共有サーバー室の物理的なサーバーラックを契約
- 利用者（契約先）は、管理者と作業者の登録がなされる
- 基本サービスとして
  - -電源サービス
  - -容量に応じた空調サービス
  - -インターネット接続サービス

この契約において、守るべき資産は、以下を想定します。

- サーバーラックの中の情報通信機器・システム（物理的資産）
- 電源設備
- 空調設備
- インターネット接続　（ネットワーク上の情報を含む）

ハウジングサービスの場合、データセンター事業者としては、契約利用者（作業者）がサーバーラックの中の情報システムについておこなう作業については関知しませんが、契約利用者（作業者）自体がデータセンター内において内部不正を起こしにくい仕組みを提供することはあります。次に、ハウジングサービスにおける人的脅威源には次のようのものが考えられます。

1. データセンター利用者
   (ア) 自社の社員(作業要員)
   (イ) 自社で契約した委託作業要員
2. データセンター事業者
   (ア) データセンター事業者の社員(作業要員)
   (イ) データセンター事業者の委託作業要員
3. データセンターの共同利用者
   (ア) サーバー室の共同利用者
   (イ) データセンター(建屋)の共同利用者
4. １～3 の何れにもあてはまらない者（部外者）

ハウジングサービスにおける人的脅威源を想定した典型的なリスクの例について紹介します。

データセンターの利用者・事業者・サーバー室の共同利用者が脅威源となるリスクの例

〇機器・環境の共有がリスクとなる例

脅威事象例	電源の抜線による電源停止
発生の頻度	定常的な業務改善活動を通じて対応を行なう（日常業務の一部）
発生時の影響	売上機会の減少、資産の喪失（システム停止の他、急激な電流の変化によるシステム機器の破損）

データセンターで提供する機器や環境は、多くの場合において複数の利用者が共有するため、共有利用者による故意・過失による被害を受けるリスクがあります。

想定されるケース：

- 高密度に情報通信機器を稼動させたことで、空調能力以上に発熱してしまいシステム停止を誘発した。
- 機器追加作業中に配線を誤り、稼動中の機器の電源を停止させることによりディスク障害を引き起こした。
- 電源ケーブルの老朽化に伴う交換作業中に誤って接触ショートを起こし、スパーク発生による作業員の負傷と電源停止を引き起こした。

〇サーバーラック内へのアクセスがリスクとなる例

脅威事象例	機器の盗難や故意による破壊
発生の頻度	データセンター利用者の社内関係者発生の頻度：業務見直しや、監査などで対応を行なう（年に 1～数回）
発生時の影響	売上機会の減少、資産の喪失、信用失墜（機器盗難によるシステム停止、格納されている情報資産の流出）

データセンター利用者（利用者の作業者）やデータセンター要員（情報通信機器の保守部品交換や再起動操作など、データセンター要員にサーバーラック内の機器へのアクセスを求めるサービスを契約している場合）がデータセンター利用者の機器へのアクセス権限を有することで、過失による不正なアクセスや、故意の機器破壊をおこなうリスクがあります。

想定されるケース：

- データセンター利用者の従業員が情報通信機器に取り付けられていたストレージ機器を盗み出し、格納されていた個人情報を流出させ、機器を転売した。

〇共有区画での不正がリスクとなる例

脅威事象例	専有区画からはみ出たケーブルの誤抜線
発生の頻度	定常的な業務改善活動を通じて対応を行なう（日常業務の一部）
発生時の影響	売上機会の減少（システム停止）

脅威事象例	共有区画に一時的に置いておいた機器の盗難・紛失
発生の頻度	定常的な業務改善活動を通じて対応を行なう（日常業務の一部）
発生時の影響	資産の喪失、信用失墜（機器のの喪失や内部データの流出）

ハウジングサービスではサーバー室を複数の利用者が共有するため、同じ空間領域（区画）を共有する他の利用者による故意・過失による被害を受けるリスクがあります。

想定されるケース：

- 機器追加設置作業中に一時的に作業サーバーラック前を離れた間に設定作業用の端末が盗難された。

データセンター事業者が脅威源となるリスクの例

〇機器・環境の共有がリスクとなる例

脅威事象例	過負荷による機能停止・低下
発生の頻度	定常的な業務改善活動を通じて対応を行なう（日常業務の一部）
発生時の影響	売上機会の減少、資産の喪失、人的損害（負荷増大によるブレーカートリップに伴う電源停止、放熱による空調効率の低下、放熱による機器故障による火災発生

データセンターで提供する機器や環境は、多くの場合において複数の利用者が共有するため、共有利用者による故意・過失による被害を受けるリスクがあります。

想定されるケース：

- 高密度に情報通信機器を稼動させたことで、空調調整能力以上に発熱ししてしまいシステム停止を誘発した。
- 機器追加作業中に配線を誤り、稼動中の機器の電源を停止させることによりディスク障害を引き起こした。
- 電源ケーブルの老朽化に伴う交換作業中に誤って接触ショートを起こし、スパーク発生による作業員の負傷と電源停止を引き起こした。

〇情報通信機器の動作環境の変化がリスクとなる例

脅威事象例	情報通信機器や設備機器の動作環境が設計外の状況となり動作に異常をきたした。
発生の頻度	業務見直しや、監査などで対応を行なう（年に 1～数回）
発生時の影響	売上機会の減少（温度上昇による機器停止）

サーバー室内の環境の変化（機材の追加や移動等）や環境設定（空調設定等）変更の要因により、情報通信機器の動作環境に問題が生じるリスクがあります。

想定されるケース：

- 計画外のサーバーラック増設による空調能力の不足や冷却風対流の変化による熱だまりによりシステムが非常停止した。
- 電力設備点検中に UPS が単体故障し、他の UPS で稼動可能な設計であったにもかかわらず、過電流で UPS 機能がダウンし電力停止した。

〇設備運用の体制がリスクとなる例

脅威事象例	サーバーラック配置管理ミスによる過った場所への設置や施錠の取り違え
発生の頻度	業務見直しや、監査などで対応を行う（年に 1～数回）
発生時の影響	過大な業務負荷（設計仕様とは異なることに起因する設備不足、再作業による作業負荷増、障害発生時の原因特定時間の増加）

データセンター要員の低スキルレベル、未完成な体制により、情報通信機器等の動作環境に問題が生じるリスクがあります。また、これらの要因は問題発生後のダメージ軽減などの運用品質にも影響します。

データセンターの部外者が脅威源となるリスクの例

〇データセンターへの強盗・テロリスクの例

脅威事象例	悪意をもった破壊工作による設備損壊や機能停止
発生の頻度	緊急対応組織を立ち上げて対応を行う（数年に 1 回）
発生時の影響	売上機会の減少、資産の喪失、人的損害（データセンター内一時退避による作業中断、情報通信機器等の停止、破損による資産喪失、サービスの停止）

データセンターは様々な高価な情報通信機器が設置され、様々な情報サービスを提供する重要なインフラとなっているため、それらの機器や情報の窃盗、あるいは社会を混乱に陥れるためにデータセンター自体を標的とする犯罪者・テロリストによる攻撃のリスクが考えられます[22]。

想定されるケース：

- 電源設備の破壊による停止、放火等による消火設備の発動に伴って情報通信機器が停止した。

3.1.4 ホスティングサービスにおけるリスク例

ホスティングサービスは、データセンター設備とスペースを貸し出すハウジングサービスに加え、情報通信機器とネットワーク回線を提供し、その機能を遠隔から契約利用者が利用できるサービスです。データセンター設備に加え情報通信機器およびネットワーク回線の運用も提供されるため、資産として設備を持つ必要がなくなり、また、システム運用もサービスとして提供されるため、専門的な知識がなくとも管理が可能になります。

物理的な資産を持たなくなるため、利用者にとっての脅威は、物理的な設備の故障や破壊、盗難ではなく、運用上のサービス停止による機会損失、および情報資産としての情報通信機器上のデータの流失、改竄、破壊が中心となり、情報通信機器上の論理的な区画が「セキュリティ区画」となります。

設備は基本的にすべてサービス事業者から提供されるため、データセンターに立ち入ることなく、全てリモートから運用が可能な反面、具体的な情報通信機器の設置場所や保守の状況等が把握しにくく、「セキュリティ区画」の品質管理を直接的に行いにくくなります。

また、サービス単位で設備、運用コストを他の利用者と共有することによる専門業務のアウトソースとコストの軽減が実現可能な反面、汎用的な仕様による制限、情報通信機器の設置場所や運用方法のブラックボックス化の他に、利用者による資源の奪い合いや「セキュリティ区画」の他社との混在のリスクがあります。

ここでは、ホスティングサービスのリスク分析をおこなうために、以下の契約を事例として想定することにします。

22：データセンターはテロのターゲットとしては効果が不確実なケースが多いため、実際に国内においてデータセンターを物理的攻撃の対象とした事例はない。一方で、直接攻撃対象とならない場合でも、政府重要施設や大規模商業ビルが攻撃対象となった場合の副次被害等が考えられる。

- シェアード（共有）型サーバー
- 基本サービスとして
  - -電子メール機能
  - -Web サーバー機能
  - -CGI 機能
  - -ファイルサーバー機能
  - -データベース機能
  - -FTP 機能
- 付帯サービスとして
  - -バックアップ機能
  - -セキュリティ機能
  - -SSL・サーバー証明書機能

この契約において、守るべき情報資産は、以下を想定します。

- サーバー上のアプリケーションデータ
- メールアーカイブデータ
- ファイルサーバーおよびデータベース上の利用者データ

ホスティングサービスの場合、データセンター設備の運用をサービス提供事業者がおこなう場合とデータセンター事業者の提供サービスに委託しておこなう場合がありますが、いずれの場合も利用者側からはホスティングサービス事業者との契約であり、ハウジングサービスの章で述べたリスクは、そのままホスティングサービスでも考慮する必要があります。

ただし、必要な情報通信機器は全てサービス事業者の資産であるため、利用者側では情報資産を除く物理的な資産については、運用品質および可用性に対するリスクとしてのみ考慮すればいいことになります。

ホスティングサービスのリスク分析では、以下のような人的脅威源の分類を想定します。

1. ホスティング利用者
   (ア) 自社の社員(作業要員)
   (イ) 自社で契約した委託作業要員
2. ホスティング事業者
   (ア) ホスティング事業者の社員(作業要員)
   (イ) ホスティング事業者の委託作業要員（データセンター事業者等）
3. ホスティングサービスの共同利用者
   (ア) 情報通信機器の共同利用者
   (イ) サービスの共同利用者
4. １～3 の何れにもあてはまらない者（部外者）

以下に、ホスティングサービスにおいて人的脅威源から想定されるリスクの例について紹介します。

ホスティングサービス事業者が脅威源となるリスクの例

〇情報通信機器の破壊、盗難による情報資産の喪失や流出がリスクとなる例

脅威事象例	特定のサービス、もしくは利用者を狙った情報通信機器の破壊
発生の頻度	緊急対応組織を立ち上げて対応を行う（数年に 1 回）
発生時の影響	売上機会の減少、資産の喪失、信用の失墜（リソースを共有するサービスを含む対象サービスの停止、および情報資産の喪失）

情報通信機器を管理するホスティング事業者の運用要員（管理者）やデータセンター事業者の運用要員（情報通信機器や電源設備への物理的アクセス権限を有する）が、故意・過失によってサービス提供をする情報通信機器への物理的な不正アクセスや機器破壊をおこなうことが考えられます。

機器破壊の場合は情報の消失、サービスの停止、盗難等持ち出しの場合は情報の流出の可能性が生じます。情報の流出は単に資産の喪失というだけでなく、エンドユーザーから預かっているデータの喪失であり、企業としての信用の失墜にもつながることになります。

〇情報通信機器の管理時のデータ破壊、流出がリスクとなる例

脅威事象例	メンテナンス作業中のオペレーションミスによるデータ消去
発生の頻度	緊急対応組織を立ち上げて対応を行なう（数年に 1 回）
発生時の影響	資産の喪失、信用失墜（情報資産の喪失）

情報通信機器の管理者権限を有する者（ホスティングサービス事業者の運用要員等）が、利用者データへのオペレーションミスや重過失、不正アクセス、故意によりデータ破壊または流出をおこなうリスクがあります。

想定されるケース：

- メンテナンス作業中のコマンド入力ミスにより、バックアップデータを含む利用者データを全消失した。

〇物理障害時の復旧の長期化がリスクとなる例

脅威事象例	機器固有の不具合による同時多発的な傷害発生
発生の頻度	業務見直しや、監査などで対応を行なう（年に 1～数回）
発生時の影響	売上機会の減少（多重障害発生によるサービス停止、保守交換機器不足による復旧時間の長期化）

交換部材の保管ポリシーによって、障害発生時の交換箇所、規模により、部材調達による復旧時間が長くなる場合があります。複数社に提供されるサービスのため、製品に起因する予備保全

交換のように数が多くなるケースにおいては、その作業対象規模の大きさにより障害対応時間が増加する可能性があります。

○保守によるサービス停止がリスクとなる例

脅威事象例	ぜい弱性対応のための一斉メンテナンス作業によるサービス繁忙期での高負荷
発生の頻度	定常的な業務改善活動を通じて対応を行う
発生時の影響	売上機会の減少（一時的・短時間のシステム停止や高負荷の発生）

複数利用者でサービスを共有し、事業者側が運用することで、保守時間とサービス停止可能時間との調整が困難な場合があります。一般的に保守のための計画作業はホスティングサービス事業者の通知によって指定され、利用者側が調整することはできません。

情報資産の流出・喪失には直結しませんが、短時間の停止でもサービス運用に影響がある場合には可用性に対するリスクとして考慮する必要があります。

○データバックアップ時のデータ消失がリスクとなる例

脅威事象例	ストレージ障害によるロールバック発生に伴う差分データ喪失
発生の頻度	定常的な業務改善活動を通じて対応を行う
発生時の影響	資産喪失（情報資産(障害発生時と最新バックアップの差分データ)喪失）

バックアップ取得のタイミング、方法、およびデータ保管場所は、サービス提供者の仕様に依存します。ディスクミラーリングの方式、バックアップ媒体の種別、別システム別サイトでの保管有無などにより、対障害安全性とコストが異なります。また、保管場所運用ミスや多重障害によりバックアップ取得が正常にできないリスクがあります。

○OS、セキュリティパッチ適用ポリシーの不整合がリスクとなる例

脅威事象例	セキュリティパッチ適用に伴うアプリケーション動作不安定
発生の頻度	定常的な業務改善活動を通じて対応を行う
発生時の影響	売上機会の減少（動作確認不完全でのセキュリティパッチ適用による動作不安定化）

OS の更新やセキュリティパッチの適用有無は、サービス提供者のポリシーに依存します。最新のパッチ適用の有無によりセキュリティぜい弱性を内包することや、逆に適用によりアプリケーションの動作不安が発生するリスクがあります。

〇共有情報通信機器設定のためのオペレーション回数の増加がリスクとなる例

脅威事象例	メンテナンス作業増加に伴う人為的ミスの増加
発生の頻度	定常的な業務改善活動を通じて対応を行う（日常業務の一部）
発生時の影響	過大な業務負荷（システム停止/データ喪失インシデントの発生）

直接的なリスクではありませんが、共有する利用者の数が多い情報システムは一般的に、専有するシステムに比較して管理者側の情報通信機器の設定変更や追加プロビジョニング作業の頻度が増加します。これに合わせてオペレーションミスの発生確率も情報システムに対する作業頻度の増加に比例する可能性があります。

ホスティングサービスの共同利用者が脅威源となるリスクの例

〇共用利用者による資源圧迫がリスクとなる例

脅威事象例	情報通信機器およびネットワークトラフィックに高負荷が発生
発生の頻度	定常的な業務改善活動を通じて対応を行う（日常業務の一部）
発生時の影響	売上機会の減少（システム高負荷によるパフォーマンスの劣化、サービス拒否の増加）

CPU、メモリ、ネットワーク帯域等の資源を他利用者との共用する場合、他利用者が高負荷をかけることによる資源逼迫のため、システム仕様上のパフォーマンスを最大限利用できない場合があります。すなわち、ベストエフォートサービスでの共有資源の逼迫によるパフォーマンス低下が起こり、可用性への影響を受けることがあります。

想定されるケース：

- 他利用者が大量のスパムメールを一斉配信し、情報通信機器とネットワークに高負荷をかけた。
- 他利用者自身が第三者に不正に管理者権限を奪われ、攻撃の踏み台にされた。

〇障害からの復旧時作業がリスクとなる例

脅威事象例	ストレージ障害復旧時にデータ復旧状態の確認が不十分だったことによって、利用者間でデータ誤参照・情報漏えいが発生した
発生の頻度	緊急対応組織を立ち上げて対応を行う（数年に 1 回）
発生時の影響	資産の喪失、信用の失墜、売上機会の減少（多重作業ミスと二次災害による情報流出、障害復旧の長期化）

物理ストレージを共有する場合、管理オペレーションミスや障害が原因で他利用者による情報参照が意図せずできてしまう可能性があります。また、物理障害からの復旧時に物理ストレージを共有する他利用者とのデータ混在を回避するため、データ修復作業に制限を受けることや、セキュリティ区画の分離により多くの時間を費やす可能性があります。

ホスティングサービスの部外者が脅威源となるリスクの例

〇情報通信機器のぜい弱性がリスクとなる例

脅威事象例	管理者権限乗っ取りによる情報システムへの不正アクセス
発生の頻度	業務見直しや、監視などで対応を行う（年に 1～数回）
発生時の影響	資産の喪失、売上機会の減少（不正アクセスによる情報流出、改ざん、破壊）

情報通信機器へのアクセス、特に管理コンソールへのアクセスについて、一般にインターネット回線を経由する場合が多いため、通信経路からの情報漏えい、盗聴、ログインアカウントの漏えい、成りすましといった脅威が考えられます。セキュリティ強度は通信経路の暗号強度や本人認証方法により変化します。

想定されるケース：

- 情報通信機器のぜい弱性対応遅れにより第三者が認証情報を盗聴し、管理者権限で不正にアクセスし、情報資産の流出が発生した。

3.1.5 クラウドサービスにおけるリスク例

クラウドサービスは、データセンター設備とスペースを貸し出すハウジングサービスとは異なり、仮想化された情報通信機器と通信回線を提供するため、より柔軟な性能変更や増設をいつでもオンラインで行なえることが特徴です。仮想化された環境はシステム全体が冗長化されているため情報通信機器単体の故障を意識せず、高い耐障害性や可用性の確保された環境を利用することができます。一方で基盤となるシステムが複雑でブラックボックス化されているため、障害ポイントが判別しにくい、障害発生時の原因確認や切り分けが複雑になる場合があります。

また、冗長性や拡張性を確保するため情報通信機器の配置が国内外の複数拠点にまたがる場合があり、データの物理的な保管場所が把握しにくいこともあります。

サービスによっては自動拡張など、必要に応じた柔軟で即応性のある利用が可能ですが、その分コストの見積もりが難しく、CPU の負荷が急激に上がる場合や、データ転送量が急増した場合にはそれに応じた追加料金が発生します。

ここでは、クラウドサービスのリスク分析をおこなうために、以下の契約を事例として想定します。

- Infrastructure as a Service （IaaS）型サービス
- パブリッククラウド（ハードウェアは共有）
- システムリソース（CPU/メモリ/ストレージ）は増減可能
- 従量課金
- 物理的な情報通信機器は国内 2 箇所、海外 1 箇所に配置

この契約において、守るべき情報資産は、以下を想定します。

- 情報通信機器上のアプリケーションデータ/利用者データ

クラウドサービスの場合、ホスティングサービスと同様、データセンター設備の運用は全てデータセンター事業者側で行なわれ、利用者はリモートからのアクセスのみでシステム運用に関与することはありません。また、必要な情報通信機器は全てサービス事業者の資産であるため、利用者側では情報資産を除く物理的な資産については、運用品質および可用性に対するリスクとしてのみ考慮すればいいことになります。

クラウドサービスのリスク分析では、以下のような人的脅威源の分類を想定します。

1. クラウドサービス利用者
   (ア) 自社の社員(作業要員)
   (イ) 自社で契約した委託作業要員
2. クラウドサービス事業者
   (ア) クラウドサービス事業者の社員(作業要員)
   (イ) クラウドサービス事業者の委託作業要員（データセンター事業者等）
3. クラウドサービス(基盤)の共同利用者
4. １～3 の何れにもあてはまらない者（部外者）

以下に、クラウドサービスにおいて人的脅威源から想定されるリスクの例について紹介します。

クラウドサービス利用者が脅威源となるリスクの例

〇データの越境がリスクとなる例

脅威事象例	海外のクラウドサービスを利用していたところ、海外では違法となる情報を誤ってクラウドサービスに保存してしまい、海外警察機関からの差押え、起訴を受けた
発生の頻度	業務見直しや、監視などで対応を行う（年に 1～数回）
発生時の影響	信用の失墜

クラウドサービスを利用する場合において、データが保存される情報通信機器の設置場所が国外である場合、司法権の異なる海外の法律の適用を受ける可能性によるリスクが発生する場合が

あります。主な例として米国における e-ディスカバリー法[23]や児童オンラインプライバシー保護法（COPPA[24]）などがあります。データの流出や損失への直接の脅威ではありませんが、サービス提供をおこなう際に適用される法律の違いからの法的リスクを考慮する必要があります。

クラウドサービス事業者が脅威源となるリスクの例

〇仮想化環境のアクセス権管理がリスクとなる例

脅威事象例	クラウドサービス基盤のぜい弱性から、悪意を持ったクラウドサービス利用者がクラウドサービス基盤への侵入に成功し、メモリに格納された利用者の認証情報などを窃取された。
発生の頻度	業務見直しや、監視などで対応を行う（年に 1～数回）
発生時の影響	資産の喪失

1 台の物理マシン上に複数の仮想マシンが集約されているため、ハイパーバイザー特権等を奪われた場合や仮想マシン環境において未知のぜい弱性が存在した場合に、即座に影響を受ける範囲が拡大する可能性があります。

システム運用に対する脅威ということではホスティングサービスと類似のリスクとなりますが、より広範囲への影響拡大と、悪意ある第三者によるリモートからの攻撃対象がより多くなります。

クラウドサービスの部外者が脅威源となるリスクの例

〇IT リソースの奪取がリスクとなる例

脅威事象例	管理者権限乗っ取りによるシステムへの不正アクセス
発生の頻度	業務見直しや、監視などで対応を行う（年に 1～数回）
発生時の影響	事業運営コストの増加

クラウド上にプールされた IT リソースを必要なときに必要な量だけ容易に追加できるため、不正にアカウントを奪われた場合、大量スパム配信、仮想通貨の発掘など、第三者への攻撃の踏み台や大量不正利用による高額な利用料が検知までの短時間で生じるリスクがあります。

想定されるケース：

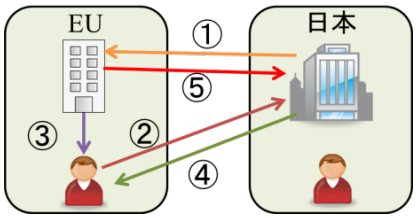
23：米国の連邦民事訴訟法規則に規定される証拠開示制度。訴訟当事者は存在するすべての電子データから訴訟に関係する電子データを収集し提出しなくてはならないと規定されている。違反した場合には懲罰的な罰則が科された事例もある。

24：13 歳以下の子供に対するインターネット上での個人情報の収集に関して、親に対する通知と、同意の取得を義務付ける米国の法律

- 誤ってクラウドサービス利用のための認証情報を流出させてしまい、それを入手した攻撃者が高性能なクラウドのインスタンスを立ち上げ仮想通貨の発掘を行った。翌月、クラウドの利用料として莫大な金額が請求された。

コラム⑦ データ越境と欧州一般データ保護規則

本文中でリスク例として紹介した国内データの海外への移転(図中①)の他にもデータの越境には様々なパターンがあります。これらのうち、近年では特に EU からのデータ越境に関しては大きな状況の変化がおきています。



2018 年 5 月から EU での適用が開始される「欧州一般データ保護規則」（General Data Protection Regulation:以下、GDPR）は、EU の外(域外)にも適応される規則となっているため、日本の法人においても配慮が必要になる場合があります。GPDR には権利侵害などの重大な違反対して 2000 万ユーロ、または前年売上高の 4%を上限とした制裁が規定されています。

GPDR が域外適応される例としては EU 域内で個人データを収集し、日本で処理をおこなうケース（図中②）、日本企業であっても EU 域内に業務遂行に必要な機器があるケース（図中③）。EU 域内へ日本から直接、商品やサービスを提供するケース（図中④）、グループ会社の現地法人が EU 域内に設置されているケース（図中③）が該当します。

GDPR では個人データの越境（図中⑤）のためには以下の何れかを満たす必要があります。

1. 十分な保護措置を講じている国として認定を受ける（十分性認定）。
2. 業界団体等が GDPR の遵守を目的とした拘束力及び執行力のある公約を伴う行動規範を　作成し、欧州データ保護会議の承認を得る。
3. EU 内の監督機関の承認を得た認証機関による、データ保護認証メカニズムの認証（欧州データ保護シール）を得る。
4. 多国籍企業間でのデータ流通を認める BCR（binding corporate rules：拘束的企業準則）を申請し、EU 内の監督機関の承認を得る。
5. 欧州委員会で採択または承認された SDPC（standard data protection clauses：標準データ保護条項）を移転元と移転先の間で締結する。
6. 本人の明確な同意を得る。

これらのうち、1 については、日本は十分性を認められていません。2、3 についても、個人情報保護法の改正により、個人情報保護委員会が設置され、日 EU 間での個人データの越境移転促進に向けた協力対話が開始されるなど進展を見せつつありますが、現時点では EU との調整が整っているとは言えない状況です。従って、現時点で取れる対策は 4、5、6 となります。

個人データ越境移転については、APEC の「越境プライバシールール」（CBPR：Cross Border Privacy Rules）との相互運用を視野に入れた調整が日本政府と EU の間で進められています。そのため、将来的には国内での CBPR 認証を得れば、EU とのデータ流通もスムーズに行えるようになる可能性があり、こうした動きを注視していく必要があります。

3.2 管理策における考え方

前節で述べたように、データセンターで提供されるサービスに応じて、リスクのもととなる様々な脅威が存在します。セキュリティを保つためには、それらの脅威に対応した管理策をとる必要があります。

セキュリティのための管理策は、一つだけで全てをまかなおうとするのではなく、複数の管理策を組み合わせて補完し強化するのが効果的です。一方で、管理策の組み合わせは、データセンターによって様々であり、データセンター利用者は、自分が守るべき情報の重要性に応じて適切な管理策が施されたデータセンターサービスを選択する必要があります。

セキュリティ管理策にはどのような観点があるのか、その分類軸を系統立てて把握しておくことは、ある管理策の組み合わせが自分の求めるサービスに対して適切かどうか判断するのに役立ちます。そこで、本節では、この管理策の分類軸について紹介します。

3.2.1 物理セキュリティと情報セキュリティ

情報システムを収容し、そこからサービスを提供する器としてのデータセンターにとって、もっとも基本的なセキュリティ管理策は、収容する情報システムへの物理的なアクセスを制御することです。建物構造、ゲートや鍵付きサーバーラックによる区画などがこれに該当します。利用するデータセンターのサービスがハウジング、ホスティング、あるいはクラウドのいずれにかかわらず、物理セキュリティはデータセンターサービスのセキュリティの基本となります。

一方、セキュリティ全体から見ると、データセンターの物理的セキュリティはほんの一部に過ぎません。例えば、ネットワーク経由での情報システムへの不正なログインによる情報漏えいを阻止するには、ネットワークセキュリティの設計・構築・運用、情報システムの ID・パスワード管理、ディスク上での機密情報の暗号化など、各種の情報セキュリティの管理策が重要です。

情報セキュリティに対する管理策をデータセンターがおこなうか利用者が自らおこなうかは、データセンターのサービス提供/利用形態により異なります。ハウジングサービスなら情報システムの大部分が利用者の管理範囲であり、SaaS のようなクラウドサービスのケースでは大部分がデータセンター事業者の管理範囲となります。サービスを選択する際は、自らが管理しなければならない範囲、サービス提供者に管理を任せないといけない範囲をよく見極めることが重要です。

3.2.2 機密性・完全性・可用性

セキュリティと言えば、一般的に権限の無いものに対して、不必要なアクセスを制限することが思い浮べられますが、広義のセキュリティが意味するのはそれだけではありません。情報セキュリティに関する用語を定義する JIS Q 27000 では情報セキュリティを”情報の機密性、完全性及び可用性を維持すること”と説明しています。これらはまとめて”情報セキュリティの 3 要素”、あるいはその英語の頭文字をとって、”情報セキュリティの CIA”と呼ばれます。個々の要素は以下のような性質を指します。

機密性（Confidentiality）

許可されていない者に資産へのアクセスを許さない性質

完全性（Integrity）

資産の正確さや完全さが保たれている性質

可用性（Availability）

許可された者が必要とする時に資産にアクセスできる性質

これらの要素では、機密性を高めるためにアクセス制限の仕組みやプロセスを複雑にすると、可用性が低下して障害時の緊急対応が遅れてしまう等、トレードオフの関係が成立することが経験的に知られているため、セキュリティ管理策を実施するに当たってはどの側面を重視するかを決定し、各要素をバランス良く考慮することが重要です。

また、完全性や可用性については、人が故意にまたは誤ってデータや情報システムを破壊してしまうような人的脅威だけでなく、地震や洪水があってもデータや情報システムが失われず利用し続けられるように、自然や環境の脅威にも対応する必要があります。

3.2.3 真正性・責任追跡性・信頼性・否認防止

情報セキュリティの CIA の 3 要素を補う情報セキュリティの 4 つの構成要素として真正性・責任追跡性・信頼性・否認防止性があります[25]。

真正性 (Authenticity)

ある主体または資源が主張どおりのものであることを確実にする性質です。真正性は利用者、プロセス、システム、情報などのエンティティ(実在物)に対して適用されます。例えば、ある利用者が、あるリソースへのアクセス権限があるとして、権限を持った者以外の知りえない認証情報を提示し、その認証情報を元にリソースへのアクセス権限があることが確認出来た場合、これを「真正性」を示すことが出来た、ということが出来ます。

責任追跡性 (Accountability)

あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性です．例えば、監視カメラの画像に対して、データ圧縮のため、人の動きの無い余分な時間帯の動画を削除する編集を加えていた場合に、誰がどのような理由で動画を削除したのか、後に確認できるようになっていればこの責任追跡性を満たしているということが出来ます。

信頼性 (Reliability)

システムを設計・構築時に意図した動作とシステムが動作した際の結果が一致する性質のことです。例えばサーバーラックの扉開閉状態を取得することを意図して設置したセンサーが、接点不良によって開閉されていないにも関わらず通知を送ってしまう場合、そのシステムの信頼性は保たれていないということになります。

25：前述の JIS Q 27000 にも「注記」として記載がある

否認防止 (Non-repudiation)

ある活動または事象が起きたことを，後になって否認されないように証明する能力のことです。例えば入室時のバイオメトリクス認証情報にタイムスタンプを付けて保管しておくことで、ある人が入室したことを否認することは難しくなります

情報セキュリティの CIA と真正性・責任追跡性・信頼性・否認防止性、これらにプライバシーを加えた 8 要素はセキュリティの目標(Goals of Security)とも呼ばれています。

3.2.4 防犯環境設計理論に基づく分類

場所の物理的な特徴、維持管理の内容、利用のされ方等に対して、意図的な変更を加えることによって「防犯」を実現する際の基礎的な理論として「防犯環境設計理論」が存在します。ここでは管理策を防犯環境設計の視点に基づいて「監視性の確保」「接近の制御」「領域性（区画性）の強化」「被害対象の強化・保護」の 4 つに分類することを紹介します。

監視性の確保

犯罪を起こそうとする者に監視の目を注ぐことで犯行を萎縮させ、あるいは監視証跡を残すことで犯行後の対応を可能にするアプローチです。具体的には要所に監視カメラを導入し、その画像を警備員（データセンター要員）が監視・記録するといった管理策がこれに相当します。

接近の制御

領域（区画）を確保し、その領域へのアクセス制御を施すことで犯罪を起こそうとする者が標的に対し物理的に接近することを防ぎ、犯行の機会を失わせるアプローチです。具体的には保護対象を特別の室（サーバー室、鍵付きサーバーラック）に隔離し、扉でアクセス制御を実施するような管理策がこれに相当します。

領域性の強化

特定の領域（区画）を利用する者に対し、その領域を利用する権限の有無を意識させることで無権限領域（区画）へのアクセスを委縮させ、その領域（区画）内にある保護対象へのアクセスを難しくさせるアプローチです。具体的にはデータセンター内において ID カードの提示義務を持たせる、データセンター内での不審者に対する権限確認を要員に対し義務付けるといった管理策がこれに相当します。

被害対象の強化・保護

犯罪の標的を物理的に強化し、犯行の時間・労力をかけさせることで犯行途中に露見する可能性を高め、被害を受ける前に犯行を制止する、あるいはその可能性を意識させることで犯行を委縮させることを狙ったアプローチです。具体的には情報通信機器内の部品盗難の脅威を想定し、特殊な工具を使わないとあけることのできないビスで情報通信機器のきょう体を封止するといった管理策がこれに相当します。

なお、これら 4 つの分類は物理的な管理策のみならず、論理的な管理策にも適応することが可能です。例えば、「監視性の確保」の例としては、攻撃対象となりやすい情報通信機器に負荷監視用のエージェントを導入する、「被害対象の強化・保護」の例としては、保護対象となる情報に暗号化を施すといった例が考えられます。

３.２.５ 管理策の手法による分類

セキュリティの管理策には様々な物が存在しますが、本ガイドブックではこれらを「設備」「システム」「運用」の 3 種類に分類して紹介しています。

設備管理策

主にハードウェアによって実現される管理策です（ここでは敷地外周と建物外壁等の空間も「設備」に含みます）。建屋、外周フェンス、間仕切り壁、ゲートや鍵付きサーバーラックといった管理策がこの分類に該当します。

システム管理策

複数のハードウェア・ソフトウェアとポリシー、データセンター運用要員の組み合わせによって実現される管理策です。データセンターでは本人認証システム、入退管理システム、画像監視システムといった形でこれらの管理策は実現されています。

運用管理策

設備の運用規定や体制、それらを維持する監査等により実現される管理策です。警備員による巡回や、持ち込み物検査といった管理策がこの分類に該当します。

3.3 データセンターで実施される管理策

データセンターにおける物理セキュリティは、オフィスや商業施設とは異なる厳密なアクセス制御をおこなうことが求められます。本節では「架空のデータセンター」[26]（図 11）を題材に、実際のデータセンターで実施されるセキュリティ対策を説明していきます。なお、本節で紹介する管理策を実現するシステムの一部については 5 章において詳細な解説を行っており、本節と合わせて読むことで、データセンターのセキュリティを実現している仕組みをより深く理解することが出来ます。

イメージ提供：セコム　IS 研究所

図 11　「架空のデータセンター」外観

本節で実施するセキュリティプランニングの手続きは、読者にデータセンターのセキュリティがどのように実現されているかをわかりやすく説明するためのものであり、実際のデータセンターにおいてセキュリティ実現のために同一の手続きが取られているわけではありません。

データセンターとしての利用を前提とした建物の多くにおいては、この節で紹介するゾーニングや管理策のある程度想定した空間構造が設計されています。一方で、データセンターとしての利用を前提としない建物の場合、これらの実現が難しくなっている場合があります。データセンター専用の建物では、動線を限定することで館内の人間に対して厳密なアクセス制御を施すことができますが、オフィスや商業施設のように様々な人物がアクセスするテナントと建屋を共有する場合、厳密なアクセス制御をすることができず、他の方法で攻撃者の侵入を防ぐ必要がある場合があります。

26：この節で扱う「架空のデータセンター」は
・データセンターとしての利用を前提として設計された建物
・1 階部分はエントランスとしての機能に加え、外来者との打ち合わせのユーティリティ機能を提供
・2 階以上のフロアでコロケーション機能を提供している
設定となっている。

3.3.1 全体プランニング

データセンターのセキュリティ設計時に重要なこととして、まずセキュリティ管理策を実施する空間の役割の定義（=ゾーニング）があります。建物の設計段階におけるゾーニング手法として、セキュリティレベルに基づいたゾーニングが一般的に用いられます。

セキュリティレベルに基づいたゾーニングをおこなうには、まず施設の持つ空間機能を重要度毎に分類することをおこないます。一般に、この分類の区分数が多いほど高いセキュリティが実現できるとされていて、例えば、JDCC ファシリティスタンダード[27]では、敷地、建物、サーバー室、サーバーラックといった段階ごとにセキュリティ管理を行っているかを評価しており、一つ（サーバー室のみ）の分類の場合、ティア１～２、二つ（建物内、サーバー室内）の分類の場合をティア 3、四つ（敷地内、建物内、サーバー室内、サーバーラック内）の場合をティア 4 として評価するとしています。また、実際に分類をおこなう際には、対象となる区画の重要性だけで決定することは難しく、その区画の持つ機能・運用状況・利用者の性質等をセキュリティポリシーに照らし合わせたうえで複合的に決定されます。

本章で扱う「架空のデータセンター」の例では、JDCC ファシリティスタンダードのティア 4 をベースとして、「建物内」をさらに「エントランス区画」「共用区画」と「専用区画」の三つのゾーンに分け、「セキュリティレベル」をレベル１からレベル６までの６段階でゾーニングしています。このようなセキュリティレベル分けを図にまとめたものが図 12 です。

留意すべき点として、同じセキュリティレベルの空間であっても、利用者の違いによって区別する場合がある点があります。例えば「架空のデータセンター」のレベル 5(専用区画)にはそれぞれ異なる特定の利用契約者が利用する「サーバー室」と「オフィス」、データセンター事業者の要員がアクセスする「設備室」がわけられています（ここではそれぞれの部屋のレベルをレベル 5a、5b、5c としています）。

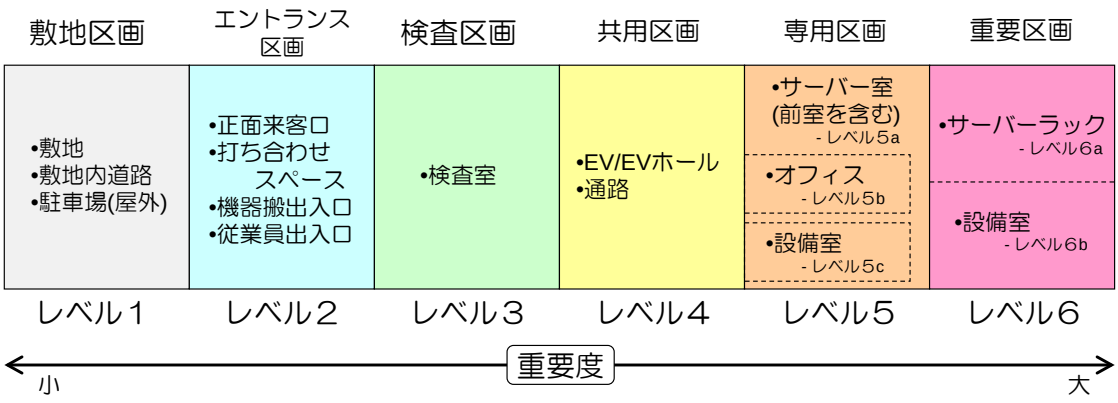
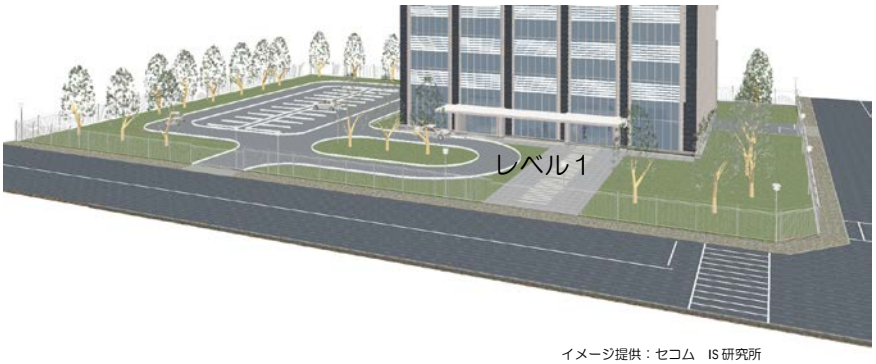


図 12　「架空のデータセンター」セキュリティレベル分け

空間機能の分類に引き続いてその機能を実際のデータセンター内の区画に当てはめていく作業を行います。この際に留意すべき点として、接続する室同士は極力隣接するセキュリティレベルとする、異なるセキュリティレベルの区画間ではアクセス制御が実施可能な構造とする、壁等を挟んで異なるセキュリティレベルの区画が隣接する場合セキュリティレベルの差に応じて隣接する壁の強度等を決定する、といった点が挙げられます。

27：4.4.1 節を参照



イメージ提供：セコム　IS 研究所

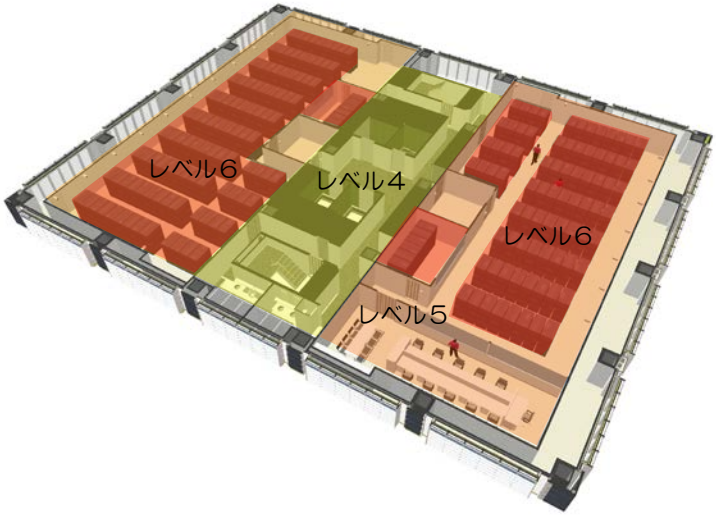
図 13　「架空のデータセンター」敷地のゾーニングイメージ

敷地外周の柵から建屋の外壁までの空間（図 13 灰色部分）を「敷地区画（レベル 1）」としています。

イメージ提供：セコム　IS 研究所

図 14　「架空のデータセンター」1 階部分のゾーニングイメージ

建屋の外壁からサーバー室に向かう経路の最初のゲートまで（図 14 青色部分）を「エントランス区画（レベル２）」、最初のゲートから検査室を経てローターゲートまで（図 14 緑色部分）を「検査区画（レベル３）」、ローターゲートから EV ホール・EV・廊下をへてサーバー室入り口の扉まで（図 14・図 15 黄色部分）を「共用区画（レベル４）」としてゾーニングしています。



イメージ提供：セコム　IS 研究所

図 15　「架空のデータセンター」サーバー室階のゾーニングイメージ

サーバー室内及びオフィス（図 15　橙色部分）を「共用区画（レベル５）」、サーバーラック内及びネットワーク室内（図 15　赤色部分）を「重要区画（レベル６）」としてゾーニングしています。

これらの区画に対し、ここまでの節で紹介したような「脅威」や「リスク」といった考えかたに基づいて管理策をあてはめた例が表 5(太文字で示される管理策は後述の節で詳しく紹介している管理策）です。これらの管理策が出来上がるまでの「過程」を知ることが、データセンターのセキュリティを理解する上で最も重要なことになります。付録.A ではこの例における管理策の根拠を複数の基準を元に示していますが、一部の管理策は基準に示されないデータセンター独自の価値基準に沿って実装されています。これらの採用された基準・データセンターのセキュリティにおける価値基準を知ることでデータセンターのセキュリティをよりよく理解することが出来ます。

また、管理策を導入する際に留意すべき点として、単に様々な管理策を導入するだけではデータセンター全体での最適なセキュリティを実現することはできず、そこには必ず運用が組み合わされることが挙げられます。例えば、様々な利用者がアクセスするデータセンターでは、それぞれの利用者の入館登録時からサーバーラック内へのアクセス時までを一貫して管理するしくみを運用することが必要となります。しかしながら、こういった、一貫した管理を全て人手でおこなうことは、特に大規模化したデータセンターにおいて大きな困難を伴います。このような複雑化する運用を支援するため、近年は様々な管理策を統合し運用を支援する「統合管理システム [28]」のようなシステムも利用されています。

28：5.8 節を参照

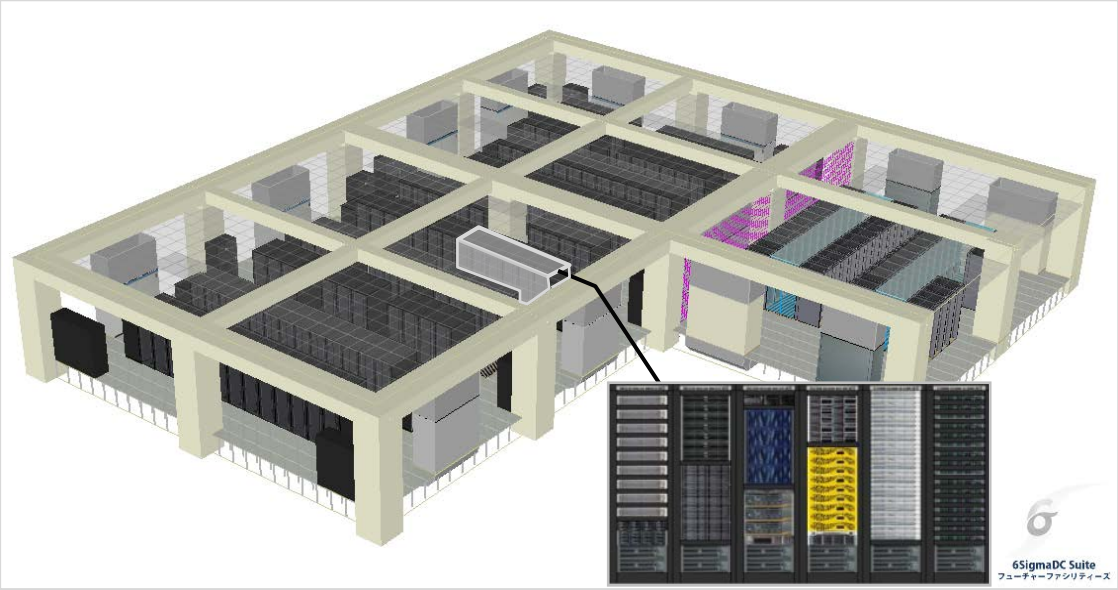
表 5　データセンターにおいて実施される管理策の例

区画	セキュリティレベル	管理策の実施場所	脅威	管理策
敷地区画	レベル1	門扉(正門、裏門)	侵入(乗り越え)	**画像監視システム(0ルクス対応、動体検知)**
				施錠可能かつ強固・十分な高さを持つ門扉
				侵入検知システム(パッシブセンサー)
				防犯灯
				カメラ付きインターフォン
				立哨警備
			侵入(破壊)	**画像監視システム(0ルクス対応、動体検知)**
				施錠可能かつ強固・十分な高さを持つ門扉
				侵入検知システム(パッシブセンサー)
				防犯灯
				カメラ付きインターフォン
				立哨警備
			車両事故(接触〔対物〕)	**画像監視システム(0ルクス対応、動体検知)**
				施錠可能かつ強固・十分な高さを持つ門扉
		駐車区画(敷地内)	不審車両	**画像監視システム(0ルクス対応、動体検知)**
				搭乗者受付
				車両受付ゲート(ナンバー識別、RFID、IC)
				巡回警備
		外周フェンス	侵入(乗り越え)	**画像監視システム(0ルクス対応、動体検知)**
				フェンス(忍び返し含む、強度のあるもの)
				防犯システム(パッシブセンサ)
				防犯システム(フェンスセンサー)
				防犯灯
				巡回警備
			侵入(破壊)	**画像監視システム(0ルクス対応、動体検知)**
				フェンス(強度のあるもの)
				防犯システム(パッシブセンサ)
				防犯システム(フェンスセンサー)
				防犯灯
				巡回警備
エントランス区画	レベル2	正面来客口	不審者の侵入(訪問内容確認含む)	**来館者受付(事前入館申請含む)**
				画像監視システム
				立哨警備
				カメラ付きインターフォン
			危険物の持ち込み	画像監視システム(置き去り、持ち込み検知)
				立哨警備
		機器搬入・搬出口	不審者侵入・危険物の持ち込み	画像監視システム
				立会い
			搬入物品の盗難	画像監視システム
				立会い
				強固かつ施錠可能なシャッター等の開口部設備
		従業員出入口	共連れ	入退管理システム(共連れ検知)
				画像監視システム
				カメラ付きインターフォン
				立哨警備
			不審者の侵入	入退管理システム
				画像監視システム
				カメラ付きインターフォン
				立哨警備
		建屋窓・外壁	(破壊による)侵入	画像監視システム(0ルクス対応、動体検知)
				防犯システム(ガラスセンサー)
				巡回警備
検査区画	レベル3	手荷物検査室	不正侵入	**フラッパーゲート**
				画像監視システム
				立哨警備
			不審物持ち込み	**持込み検査(金属探知、X線透視)**
				立哨警備
共用区画	レベル4	廊下・EV・EVホール	不正侵入	画像監視システム
				入退管理システム(ICカード・生体認証)
			共連れ	**ローターゲート**
				入退管理システム(共連れ検知)
				画像監視システム
				立哨警備
専用区画	レベル5a	オフィス	不正侵入	画像監視システム
				入退管理システム(ICカード・生体認証)
	レベル5b	サーバー室(前室含む)	不正侵入	**画像監視システム**
				入退管理システム(ICカード・生体認証)
				フリーアクセス床の特殊ボルトによる固定
			不正滞留	**画像監視システム**
				入退管理システム(在室カウント)
			共連れ	**画像監視システム**
				入退管理システム(前室での共連れ検知)
			危険物持ち込み	**画像監視システム**
				水、火気、電磁ノイズ源等の持ち込み禁止ルール
			火災	火災予兆検知
			情報の不正持ち出し	**画像監視システム**
				記録媒体の持ち込み禁止ルール
	レベル5c	設備室	不正操作(破壊)	画像監視システム
				入退管理システム(ICカード・生体認証)
			火災	火災検知システム
重要区画	レベル6a	ラック	不正操作(破壊・改ざん)	**画像監視システム**
				ラック扉管理(ICカード・生体認証)
				ラック
	レベル6b	設備室(NW、電気、空調室監視室等)	不正操作(破壊)	画像監視システム
				入退管理システム(ICカード・生体認証)
			火災	火災検知システム

コラム⑧ プランニングのためのツールとデータの規格

データセンターを設計するに際しては、プランニングの時点で部屋の役割、ならびに用途ごとにセキュリティ区画を適切にゾーニングする必要があります。また、安定した情報通信機器の動作環境を実現するために、室内の環境の変化(設備や IT 機器の増設等)や環境設定(空調設定等)変更に伴うホットスポットの削減、環境の最適化、節電対策等、空間内特性を的確に把握することも必要です。これらの検証、評価、可視化することができるツールとして、データセンターの 3 次元モデルデータを活用するシミュレーション技術があります。図 16 では専用ソフトウェアで作成したデータセンターの 3 次元シミュレーションモデルを示しています。

また、こういったシミュレーションを実施する際の基礎データとして、企画・基本設計の段階から建屋の構造や部材、配管等の複数の情報を一元管理している 3 次元建築モデルである BIM（Building Information Modeling）を用いる手法が近年注目を浴びています。BIM を活用することで、ゾーニングの最適化、セキュリティも考慮した最適な配線計画、カメラやセンサーの検知範囲を人の動線に合わせたセキュリティ機器の最適配置が可能となります。さらには、BIM をシミュレーションツールと活用することによって、データセンターのライフサイクルの中の建物の構造（躯体情報）・設備（機器情報）・運用（コスト、スケジュール、維持管理情報）といった情報を管理しつつ、将来のデータセンターの運用予測を考慮できるメリットが挙げられます。



イメージ提供：Future Facilities　6Sigma DC

図 16　データセンターの 3 次元シミュレーションモデル

3.3.2　全区画に共通する管理策

データセンターの利用をする場合には、データセンターの運用管理策に基づいた申請をおこなうことで利用支援を受けることができます。運用管理をおこなうことにより情報を証跡として保管・管理しています。データセンターでは、適切な管理と利用支援の提供のため、利用者は事業者に事前申請をおこなうことが一般的です。

データセンターでは、出入管理や巡回、鍵管理、所持品検査などの各種業務を行っているデータセンターでは、警備員を常駐配備することにより、24 時間 365 日体制でこれらのサービスを提供しています。作業等で立ち合いが必要な場合や、セキュリティ違反やセキュリティ事故が発生した場合など、「設備」や「システム」だけでは、対応しきれない様々な対応を警備員がおこないます。また、「設備」や「システム」に不具合が発生した場合には、それらが提供する機能を警備員が代わって提供します(交通整理・誘導や入館証の確認など)。

入館申請

データセンターのセキュリティ管理上、人・物の出入りに関する管理は、情報漏えいなどのリスクを防ぐ観点から非常に重要です。そのため、人・物の出入りに際し、事前に詳細情報を申請、然るべき権限を持った人物（利用者・事業者）による査閲・承認を行い、認められた人・物だけが出入り可能となっており、その全ての実績、履歴が保管されることが重要となります。

データセンターにおける人・物の出入りために必要となる各種申請、その申請情報を事業者が確認し、事業者にて承認された人・物だけがデータセンターから出入りすることを許可されます。申請を出すことが可能な人物はセキュリティ上、事前に取り決めされている事が望ましく、事業者は、認められた人物からの申請であり、その申請者の利用出来る範囲での申請であることを確認した上で、入館の許可・承認をすることが重要となります。

データセンターに出入りする人には様々なパターンがあり、入館する頻度などから申請すべきタイミングも異なり、下記の様なケース[29]が考えられます。

○都度入館申請・承認するケース
- -データセンター利用者（スポットで出入りする場合）
- -DC in DC サービスの事業利用者、及びデータセンターに常駐しない提供者
- -データセンター事業者（データセンターに非常駐）
- -データセンター事業者の委託要員（工事・清掃など、データセンターに非常駐）

○一定期間毎でまとめて申請するケース
- -データセンター利用者（貸しオフィスの利用者などで一定期間常駐する場合）
- -DC in DC サービス提供者（貸しオフィスの利用者などで一定期間常駐する場合）
- -データセンター事業者（データセンターに常駐）
- -データセンター事業者の委託要員（データセンターに常駐）

29：近年発生した内部犯行による情報漏えいの事例から、データセンター内の従業員の持ち物に関しても厳しく管理するケースもあり、各センターのセキュリティレベルに応じた運用が求められている。

入館申請や物品搬入申請など、来館前に各種申請をおこなう手段としては、以下のようなものが考えられます。

- メール
- 電話
- ポータルサイト（インターネット）　等

基本的に証跡が残り、申請元が特定できる方法で申請を受け付けることが望ましいと考えられます。通常、入館申請は査閲・承認やセキュリティカードの準備など、入館までに時間を要する場合が多く、たとえば前営業日までなどといった締め切りを設けることが多いですが、それを超えた場合の緊急時用の、24 時間 365 日で対応可能な窓口を提供しているデータセンター事業者もあります。

入館申請の際、必要な情報には表 6 のような項目があります。

表 6　申請書に記入する項目の例

項目	内容例
申請者情報	申請者の会社名、所属、氏名、電話番号、メールアドレス
入館者情報	入館者の会社名、所属、氏名、電話番号、メールアドレス
入館日時	入館日、入館予定時刻、退館予定時刻
入館目的・場所	入館する目的（打合せや作業・工事など）、出入する場所
ラック番号	解錠するラックの番号
備品・アメニティ	備品や会議室などの貸出・利用申請
持込品情報	持込品（ハンドキャリー）の種別と数量、型番やシリアル番号など持込品が一意に特定可能な情報
搬入品情報	搬入品や来客の種別と数量、荷姿やサイズなど
車両情報	搬入や来客用の車両の車両ナンバーやサイズ、車両数など

なお、データセンターでは、入室を厳格に管理するため、アクセス権限をそれぞれの入館者に付与しています。退職や異動により、データセンターへのアクセス権限がなくなった場合には、入館資格の失効を迅速に行います。

館内巡回・駆け付け対応

データセンターでは、外周や館内に異常が発生していないか、定期的に警備員が、巡回を行います。さらに、データセンターでは、セキュリティレベルに応じたアクセス権限を入館者別に付与しており、不正侵入や共連れ等から、情報システムを守るため、入退管理システムや侵入検知システム等で、データセンター館内を監視しています。一定時間以上の扉開放や共連れ入室、扉こじ開け、本人認証しないで出入り等で、異常が発生した場合には、システムから警報が出され

ます。警報が出された場合は、警備員が現場に急行し、対応を行います。また、アンチパスバックなどにより、とじ込みが発生した場合にも同様に警備員が現場に急行し、対応を行います。

画像監視

データセンターでは、侵入者や不正行為の監視・記録を目的に、データセンター内外にカメラを設置して、画像監視システムから、ライブでのモニタリング及び画像を記録保存しています。警備員が常駐しているデータセンターでは、画像監視システムのライブ映像を警備員が確認し、異常があれば、警備員が現場に急行し、対応を行います。

作業監理・立ち合い

データセンターでは、扉や門扉や機器搬入・搬出口などの入り口があり、常時施錠されているか、立哨警備により、不正侵入などが発生しないようにセキュリティ対策を実施しています。大型車両が入場する場合や、大型機器を搬入する場合には、通常、施錠されているゲートやシャッター、扉を開放する必要があります。その場合には、警備員がセキュリティを確保するために、立ち合いを行います。また、データセンター内の設備室（電気設備室、空調機械室、配管、配線、給排水、吸排気、EV、消防設備など）や運用スペース（ゴミ処分、倉庫、給湯、手洗いなど）に対する作業も含まれます。こういった区画の運用、整備、清掃などでの外部からの立ち入りに関しては、その区画の影響範囲を考慮したうえでのデータセンター要員による運用管理・入退管理・作業立ち合い・指導などが行われることが一般的です。

物品受取・預かり

物品受取・預かりは申請に則りデータセンター要員が行い、保管して管理します。受取・預かり、保管の状況は申請者に連絡されるのが一般的です。データセンターへの物品受取・預かりでは、特に正当な権限・目的をもたない物品の受取をしないように管理すること、預かり物品の所在を管理することが重要になってきます。そのために事前物品受取・預かり依頼申請の仕組みが使われることがあります。事前申請の仕組みでは利用者の中の権限者が「いつ」「何を」「何の目的で」「保管場所」「保管期間」「所有者名」「納品者名」等の情報を登録し、データセンター事業者が把握可能な環境が構築され、これらの情報は証跡として保管・管理、必要に応じて開示されます。この際利用される申請の手段としてはＷｅｂ、電話等による来館前申請の他、現地での書面による申請などが考えられます。

破棄

データセンターによっては物品の破棄依頼に対応しています。このような破棄業務では物品の所有者以外の判断で破棄できないように管理することが重要になってきます。そのために物品破棄依頼申請の仕組みが使われることがあります。事前申請の仕組みでは利用者の中の権限者が「いつ」「どこの」「物品名」「破棄方法」「所有者名」「産廃廃棄物指定会社」等の情報を登録し、データセンター事業者が把握可能な環境が構築され、これらの情報は証跡として廃棄依頼完了後に廃棄証明の送付と併せて申請者に連絡されます。記憶媒体の破棄依頼の場合はデータセ

ンター要員による破棄確認が行われるのが一般的です。この際利用される申請の手段としてはＷｅｂ、電話等による来館前申請の他、現地での書面による申請などが考えられます。

コラム⑨ 運用におけるＢＣＰ的観点による手順構築

データセンターにおけるセキュリティは、様々な状況を考慮し非常時における対応方法も予め検討し、必要に応じて訓練をおこなう事が重要です。

例えば、近年システム化が進む入退管理システム障害等により機能しなくなったことを想定し、専用用紙による入館方法手順を構築しておくということもその一例です。そのような場合、例えばシステムに入力されたデータを障害時にどのように参照するかといった手順検討を行っておく事が必要です。あるいは、監視カメラにおける障害時を例にとるならば、映像保管ポリシー、ＵＰＳ電源等による停電対策、監視エリアの冗長化等の検討も行っている必要があります。

さらには、不正侵入が実際に発生した場合を考えると、一般的にそういった事案発生時には警備員が急行し対応しますが、その後の対応、例えば警察や担当者へのエスカレーションについての事前の手順の構築も重要となります。さらに、環境の変化時やインシデント発生時には事案をふまえた追加防護措置の検討をおこなうことや、模擬訓練の実施といった手順を準備しておくことも重要になります。

なお、事業継続という観点では、特に都市型のデータセンターにおいては単にセキュリティを追求するだけでなく近隣住民への配慮も重要な事項となります。例えば、監視カメラの画角について近隣住居が映りこまないように配慮する、地域の社会活動へ参加を通じて地域からの理解を深めるなど、近隣住民との関係を良好に保つこともデータセンター運営上重要な観点となります。

3.3.3 敷地区画における管理策

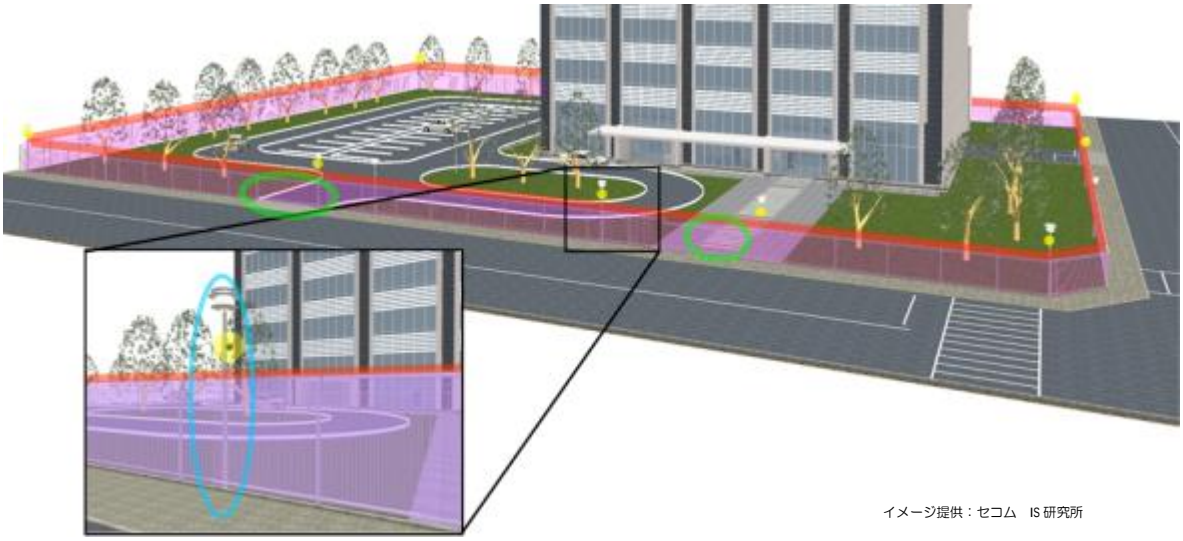


図 17　「架空のデータセンター」における敷地区画の管理策

敷地区画（セキュリティレベル１）で想定される脅威は不法侵入と破壊が考えられます。敷地区画のすぐ外はデータセンター利用者以外が自由に交通できる空間となっていることから、データセンターの所在が外部から分かりにくくするため、データセンターとしての表示を行わずに、門扉（図 17　の緑円で囲われた部分）やフェンス（図 17 紫色で示された部分）を使って（意図的・偶発的を問わず）侵入を困難にする、あるいはこれらと組み合わせて監視カメラや防犯灯（図 17 水色円で示された部分）や警備員の巡回などによって侵入阻止の意思表示する、といったことがおこなわれています。

一般的に敷地区画に施される管理策で特徴的なものを以下に紹介します。

侵入対策：検知　フェンスセンサー

フェンスセンサー（図 17 に赤線で示された部分）は敷地区画外周（敷地境界）の監視を目的に設置され、敷地内への侵入検出に有効な対策です。フェンスセンサーを用いてセキュリティ境界を監視する場合、セキュリティ境界を全周にわたってセンサーが設置されている必要があります。そのため、門扉のような可動部でフェンスセンサーの設置が難しい場合、監視カメラと動体検知ソフトウェアを組み合わせて侵入を検知する等、複数の手段を組み合わせることが必要な場合があります。また、最外周に設置されるセンサーはいたずら等を施される恐れがあることから、そういったいたずらをすることが難しくなるよう、フェンスより内側にセットバックして設置することが望ましいとされます。

侵入対策：記録・威嚇・抑止　画像監視システム

画像監視システムは敷地区画外周（敷地境界）及び敷地区画内の監視を目的に設置され、侵入者の犯行行為への威嚇や抑止、証跡の記録に効果があります。特に、外周に設置されるカメラ（図 17 黄色丸で示された部分）にはスプレー塗料や布、人為的なカメラの向きの変更など侵入者か

らの妨害行為を検知・警報する妨害検知機能を搭載したカメラを設置することがあります。この機能は、特に外周を警備員などで巡回監視していない場合重要な機能となります。動体検知機能は人や物が動いた際に自動で検知し、警報を出す機能です。広い敷地を複数のカメラで監視する場合、データセンター要員の不足等により見落としが発生する可能性がありますが、動体検知機能を持った画像監視システムを利用することで見落としをなくすことが出来ます。こういった画像監視システムの導入は、その設置環境・監視対象に応じて様々な工夫が必要なポイントですので、データセンターがどのような考え方の下、セキュリティを実施しているのか知るためのヒントとなります。

乗り入れ車両の管理

データセンターへの車両乗り入れでは、特に正当な権限・目的をもたない車両が許可無く敷地内へ侵入できないように管理することが重要となってきます。

事前申請の仕組みでは利用者の中の権限者、またはデータセンター要員の中の権限者が「いつ」「誰が」「何の目的で」「車両所有者名」「運転者名」等の情報を登録し、データセンター事業者が把握可能な環境が構築され、これらの情報は証跡として保管・管理、必要に応じて開示されます。乗り入れ時には事前登録時申請された情報に基づき乗り入れが許可され、その際の車両認証には一般に車両のナンバープレートとの照合などが用いられます。

乗り入れ許可を受けた車両に配付されるものとして、データセンター敷地内乗り入れ許可証とデータセンター敷地内運転規則要領書などが考えられます。乗り入れ車両にデータセンター敷地内乗り入れ許可証を提示させることで許可車両であることを周知させることができ、データセンター敷地内運転規則要領書を配付することで敷地内での安全を管理することができます。

3.3.4 エントランス区画における管理策

イメージ提供：セコム　IS 研究所

図 18 「架空のデータセンター」における 1 階部分の管理策

エントランス区画では、次のレベルに進入するための入館登録確認等が行われます。エントランス区画（セキュリティレベル 2）で想定される脅威は侵入や、入館権限を持った人が持たない人を不正に導き入れる行為(共連れ)などが考えられます。エントランス区画において訪問者は、予め申請した入館申請に基づき受付窓口での手続きを経て許可されます。

受付窓口では、以下のような手続きが行われます。

申請事項の確認

受付窓口担当者は、訪問者が適切な申請に基づき許可された権限であるか申請書類を確認します。確認する項目は、表 6 に示された項目となります。

本人確認

受付窓口担当者は、訪問者があらかじめ入館申請された本人であることを確認します。本人確認をする目的は、訪問者が他者になりすまして入館し、不正を働くことを未然に防ぐためです。本人確認は、公的機関[30]が発行する顔写真付きの証明書、顔写真付きの社員証、または、本人しか持ち得ないキャッシュカードや健康保険証を複数組み合せるなどして、厳格に行われます。

30：公的機関が発行する証明書は、旅券法施行規則に記載された証明書が参考になります。旅券を申請する際に提示を求める書類として運転免許証などが記載されています。

誓約書の提出

データセンター内は、監視カメラや入退室記録をはじめとして個人情報が溢れています。データセンター事業者は、館内の利用ルールや個人情報の取扱いに関する事項を訪問者に提示し同意・提出を求めます。

ID カード発行

申請事項の確認、本人確認、誓約書の同意がなされると、受付窓口担当者は、訪問者に館内用の ID カードを発行します。その際、受付時刻、担当者、ID カード番号などを記録します。また、顔写真を撮影し館内用のゲストカード証を ID カードと一緒に渡すデータセンター事業者や、ストラップの色や腕章により訪問者がどのような入室権限を持った人であるか、ひと目で判別できるよう工夫しているデータセンター事業者もあります。

生体情報登録

コンピュータ室等の重要エリアに入室する際は、生体情報による扉の開閉制御を実施する場合があります。この場合は、受付窓口での手続きの中で本人確認をして生体情報を入退管理システムに登録します。また、データセンター内で着用する ID カードに訪問者本人の顔写真を表示する場合があります。この場合は、その場で写真撮影して、ID カードとして発行します。生体情報の取扱は個人情報としてデータセンター事業者のポリシーに従い管理されます。

3.3.5 検査区画における管理策

検査区画（セキュリティレベル３）で想定される脅威は、危険物の持ち込みなどが考えられます。エントランス区画において実施される管理策で特徴的なものを以下に紹介します。

ゲート

データセンターでは様々なゲートが用いられ、入退管理システムによって管理されます。また、多くの場合は複数のタイプのゲートが組み合わせて用いられます。例えば、ここで紹介している「架空のデータセンター」では、一つ目のゲートに権限の確認を目的としてフラッパーゲートと呼ばれるタイプのゲートを設置しています。このフラッパーゲートは悪意ある侵入者の場合、容易に飛び越えられてしまうという欠点がありますが、このデータセンターでは警備員と組み合わせ運用することでそういった不正な行為を防止しています。加えて、検査区画と共用区画とのセキュリティ境界では、本人認証装置と共連れ防止機能の付いたインターロックゲートと呼ばれるタイプのゲートによって厳密な入退記録の取得を行っています。

持ち込み・持ち出し検査

データセンターでは入館時、入館者の手荷物のチェックを実施する場合があります。これは入館申請者が事前に申請し、データセンター事業者から許可された機器や荷物以外をデータセンター内に持ち込ませないことにより館内、特に情報通信機器に悪影響を与える恐れのある対象物を

排除することを目的にしています。各区画において持ち込みが禁止される物品の例を表 7 に示します。

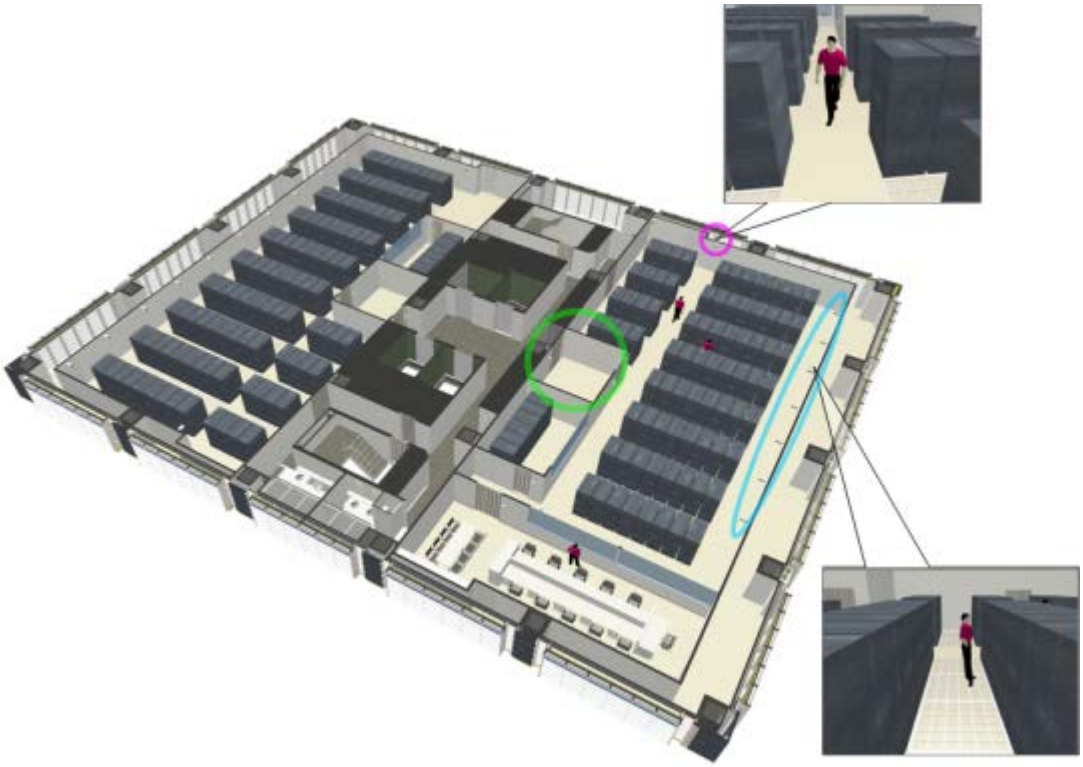
表 7　各区画において持ち込みが禁止される物品の例

品名	共用区画	専用区画	
	リフレッシュコーナー	サーバー室	事務室、倉庫等
撮影機材	×	×	×
可搬式記憶媒体(USBメモリ等)	×	×	×
パーソナルコンピューター	○	×	×
携帯電話	○	×	○
工具類	×	×	×
火気類、危険物	×	×	×
強い磁気、電波を発生する機器等	×	×	×
飲食物	○	×	×

データセンターへの持ち込みが禁止される物品では、持ち込み品申請と作業申請の内容からその区画での影響範囲を考慮したうえでデータセンター事業者による持ち込み許可、作業立会い、指導などが行われます。また、退館時に持ち出す工具や荷物の確認を行い、館内への置き忘れとならないようにしています。

また、これらの持ち込み・持ち出し管理を厳密におこなうため、例えば、X 線検査機や金属探知ゲート、３Ｄボディスキャナ等を使った持ち物検査や、タグを用いた不正持ち出し監視ゲート、利用者の入館時・退館時の体重測定により体重差を確認する、といった検査が行われる場合があります。

3.3.6 専用区画における管理策



イメージ提供：セコム　IS 研究所

図 19 「架空のデータセンター」におけるサーバー室階部分の管理策

専用区画であるサーバー室（セキュリティレベル 5）で想定される脅威には、情報の不正持ち出しと破壊、火災等による設備の被害などが考えられます。

サーバー室への入退は入退管理システムによって管理・記録されます。加えて、高いセキュリティを要求されるデータセンターのサーバー室では、共連れ防止や塵埃が室へ入り込むことを防止するための前室（図 19 の緑円で囲まれた部分）が設置されている場合があります。

サーバー室において実施される管理策の内、特徴的なものを以下に紹介します。

画像監視

サーバー室内での不正な行為を防止するために用いられる管理策として画像監視システムがあります。敷地区画で用いられる画像監視システムと異なる点として、サーバー室内で用いられる画像監視システムは証跡としての役割を果たすことが挙げられます。

例えば、データセンター事業者は、事故発生時の対応等の目的で利用者のサーバーラック内へのアクセス権を有している場合があります。こういった場合、不必要なアクセスを実施していないことを利用者に説明できる必要があることから、データセンターによってはサーバーラック列単位で撮影した画像を証跡として保管し必要に応じて開示する仕組みを構築しています。

また、こういったサーバーラックの監視は一方で、全サーバーラック列にカメラを設置すること（図 19　水色で囲われたカメラ群）は多大な設備コストとデータの保管コストがかかるため、共通通路にカメラを設置し（図 19　紫色で囲われたカメラ）サーバーラックごとに扉開閉センサーを設置することでコストを抑制している場合があります。

火災予兆監視

データセンターのサーバー室には消防法に定められるガス系消火設備が設置されていますが、この消火設備を動作させるには火災の検知が必要になります。しかしながら消防法で設置を義務付けられる自動火災報知機は、火災の規模が一定以上にならないと検出できない仕組みになっているため、火災発生後ある程度延焼してからでないと消火設備は動作しません。

そこで用いられているのが火災予兆センサーと呼ばれるセンサーで、微小な煙を検知することで重要な情報資産に延焼する前に検知することが可能になっています。この火災予兆センサーは消防法で認められる火災報知機器にはあたらないため、データセンター事業者としては２重の火災報知装置を設置するコストを負うことになりますが、データセンターの可用性確保に関する考え方を知る一つの目安となりえます。

ガス系消火設備

建物に設置される消火設備は、スプリンクラー設備や屋内消火栓設備など、水による消火設備が一般的ですが、消防法では 500 ㎡以上のサーバー室（通信機器室）には、２次被害（水損）の防止、消火後の復旧の迅速化を考慮して、不活性ガス系消火設備、ハロゲン化物消火設備などのガス系消火設備の設置が義務付けられています。

ガス系消火設備は、別室に設置される貯蔵容器、制御盤、サーバー室に設置される感知器、手動起動装置、音響警報装置、噴射ヘッド、表示灯などで構成されます。通常は、感知器の作動と連動して自動起動します。しかし、サーバー室に人が入っている場合や火災予兆センサーが早期に火災を検出した際、火災が拡大した場合は手動起動装置を操作して起動します。消火設備が起動すると、貯蔵容器内の消火剤が配管を経由してサーバー室内に設置した噴射ヘッドから放射され、消火します。

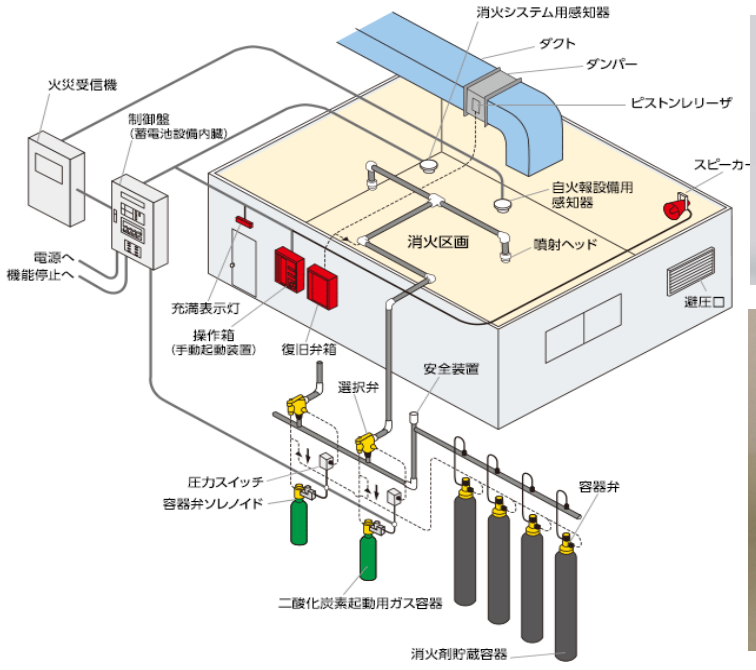
コラム⑩ データセンターのガス系消火設備における留意事項

ガス系消火設備を設置する際の主な留意事項としては、消火剤放射前の開口部閉鎖、換気装置の停止、消火剤放射中の区画内の圧力上昇防止措置（避圧措置）、消火後の消火剤排出措置などがあります。また、消防法には規定されていませんが、データセンターにおいては消火剤放射音がハードディスクドライブ（ＨＤＤ）に及ぼす影響について、特に留意する必要があります。

2016 年 9 月、欧州の金融機関のデータセンターにおいて、ガス系消火設備の定期試験の際に、情報通信機器に障害が発生しました。その原因としてガス系消火設備の動作時に発生する騒音によってハードディスクドライブに衝撃を受け、故障に至った可能性が示唆されています。

この事象は、2010 年 9 月に開催された日本建築学会で発表された「音環境が精密機器に与える影響に関する考察」と題する論文で初めて示唆されたものです。この発表を受けて、(一社)日本消火装置工業会は HP で「論文の主旨は、ガス系消火設備の消火剤（ガス」放射時の音圧レベルは、最大で 130dB を超えることがあり、ＨＤＤは 110dB 以上の音圧レベルで動作に影響を受ける可能性が高いというものです。」と情報提供しています。

消火剤放射音によるリスク対策としては、「①ＨＤＤの格納サーバーラックなどの防音や防振化対策」、「②消火剤放射開始前のＨＤＤ保護措置」、「③ＨＤＤの耐音性向上やデータ保護対策（データバックアップなど）」、「④ガス放射音の抑制」などが考えられ、④の対策として、放射音を抑制する静音形噴射ヘッドが開発・提供されています。



ガス系消火設備のシステム構成例

静音仕様噴射ヘッドの例

イメージ提供：能美防災

3.3.7 重要区画における管理策

設備室

データセンター全体の可用性を担保するための空調設備や電力設備はもちろん、構内・構外接続のために使用される通信設備は権限ある管理者のみがアクセスできる専用空間に設置する必要があります。特に電気通信事業者の回線の引き込みや、構内配線接続用のメディアコンバーターやネットワーク機器等は、多数の作業者が違う目的で作業されるケースが多いため、確実に作業目的に合ったアクセス管理を実施する必要があり、故意や誤りで通信断を起こすようなインシデントは事前に防止する必要があります。なお、これらの重要な作業時には、システムによる監視だけではなく、データセンター要員による作業立ち会い・指導がおこなわれることが一般的です。

サーバーラック

サーバーラックは、各種サービスにおいて利用者と事業者との責任分解点でもあり、またセキュリティ上でも「最後の境界」として非常に重要な役割を担っています。

近年のデータセンターではサーバーラックの前後のドアをメッシュ構造として冷却のための空気の流れを確保することが一般的です。このメッシュ構造の開口率は空気の流れを確保し、機器を冷やすという観点では大きいほうが良いのですが、大きくなりすぎると強度の低下を招いてしまうことがあり、セキュリティの観点からそのバランスが決定されます。また、サーバーラックの開口率が大きい場合、外部からサーバーラックの中の機材を判別できてしまうという可能性があります。そのため、近年ではサーバーラックの中の機材を秘匿する狙いからサーバーラックの塗装色を光の反射率の高いホワイト系に変更することでサーバーラック内部に搭載された機器の構成が見えづらくなるように配慮している事業者もあります。

また、ハウジングサービスの利用者が、複数本のサーバーラックを連続で契約した場合、各サーバーラック間の仕切り板を取り外して、容易に配線接続が可能なサーバーラックの仕様を求められることがあります。このようなニーズに応えるべく、セキュリティ境界を崩すことなく、利用者の責任において簡単にその仕切り板を取り外す構造を持たせたサーバーラックを提供している事業者もあります。

コラム⑪ 内部者に対する管理策

2012 年に発生した情報サービス事業者におけるクレジットカードの偽造事件や、2014 年に発生した通信教育サービス事業者における大規模な個人情報漏えい事件など、近年、情報システムに関わる社会的インパクトの大きい事件が、組織内に存在した内部者によって引き起こされています。

データセンターを利用するに当たっては外部犯に対する管理策だけでなく、これら内部犯に対する管理策が適切に設定・運用されているかを確認することも重要なポイントとなります。

そういった犯行に対するアプローチとして、状況的犯罪予防理論があります。状況的犯罪予防理論は、犯行者の置かれた状況を変えることによって犯行を難しくさせる、あるいは動機その物を取り除くことで犯罪を予防させる防犯理論です。この理論はそのアプローチの性質から外部犯対策のみならず、利用者自身やデータセンター要員等の内部者に潜みうる内部犯に対する管理策としても有効なものとなっています。

状況的犯罪予防理論では管理策を以下の五つに類型化しています。

- 防犯対策を技術的な対策を強化することで「犯行を難しくする」
- 管理や監視を強化することで「捕まるリスクを高める」
- 犯行のリスクと得られる見返りが釣り合わないよう「犯行の見返りを減らす」
- 犯行の動機となりうる外部からの「犯行の挑発を減らす」
- 犯人が捕まった際に言い逃れの余地を減らし「犯罪を容認する言い訳を許さない」

独立行政法人 情報処理推進機構の作成した資料「組織内部者の不正行為によるインシデント調査」ではこの五類型はさらに各々五つに細分化され合計で 25 の管理策を定義しています。

表 8 「組織内部者の不正行為によるインシデント調査」における 25 の管理策分類

犯行を難しくする	捕まるリスクを高める	犯行の見返りを減らす	犯行の挑発を減らす	犯罪を容認する言い訳を許さない
1.犯行対象を防御的に強化する ・スクリーンロックの設定 ・アクセス制御の設定 ・退職者の ID 削除/確認者設置 ・パスワードポリシーの設定 ・PC の物理チェーンロック、固定具 ・盗用防止スクリーン	6.監視者を増やす ・複数人での作業環境の設定 ・防犯ベルの設置 ・特権階級の分散化/管理者の増員 ・個人情報売買の監視 ・アクセスログの監視	11.標的を隠す ・電子ファイルのアクセス権限の設定 ・PC/USB メモリの保管場所設定	16.欲求不満やストレスを減らす ・職場での円滑なコミュニケーション の推進 ・上司や同僚に頻繁に相談できる環境整備 ・適切な人事・作業管理(業務量の軽減)	21.規則を決める ・情報セキュリティポリシーの策定 ・個人情報管理策の作成 ・就業規則 ・障害対策等の手順の明確化 ・管理/運用策の策定 ・雇用契約
2.施設への出入を制限する ・ID カード(身分証明)の確認 ・電子カードアクセス ・手荷物検査	7.自然監視を補佐する ・守りやすい空間の設計(外部から見えるガラス面積の拡大) ・オフィスのフリースペース化 ・投書箱による密告者をサポートする	12.対象を排除する ・電子ファイルのアクセス権限の設定 ・PC の持込許可制度 ・業務上で必要な閲覧項目を絞る ・紙の廃棄/溶解処理	17.対立を避ける ・情報セキュリティの管理部門を設置し、上司との対立を避ける ・適切な人事・作業管理(業務量の軽減)	22.指示を掲示する ・情報セキュリティポリシーの掲示 ・個人情報管理策の掲示 ・就業規則の掲示 ・目的外利用の禁止の掲示 ・不正事例の掲示(匿名)
3.出口で検査をする ・ID カード(身分証明)の確認 ・手荷物検査 ・メールやネットの監視	8.匿名性を減らす ・ID カード、社員バッチの携帯 ・ID による管理 ・持ち出し台帳による管理	13.所有物を特定する ・PC/USB メモリに登録番号シールをつける ・電子ファイル/紙ファイルに管理番号をつける ・複写台帳管理	18.感情の高ぶりを抑える ・パワハラの禁止 ・人種的中傷の禁止 ・適切な人事・作業管理(業務量の軽減)	23.良心に警告する ・持ち出し厳禁であることを掲示 ・管理レベルを表示/印字 ・不正競争防止法などの研修・教育 ・ルール厳守への自己サイン
4.犯罪者をそらす ・通路/出入り口の閉鎖 ・物理レベルに応じた入退制限 ・金属探知器	9.現場管理者の利用 ・CCTV(監視カメラ)の設置 ・機密情報へのアクセスは複数人による作業制限	14.市場を阻止する ・不正競争防止法 ・不正監査/不正検査 ・個人情報売買の禁止/監視	19.仲間からの圧力を緩和する ・適切な人事・作業管理(業務量の軽減)	24.遵守を補佐する ・利用 PC/USB メモリの登録管理/貸出規則を簡単にする ・施錠保管キャビネットの設置 ・シュレッダーの設置 ・相談窓口の整備
5.道具や対抗手段を制御する ・非登録の PC/CD/USB メモリの持込/持出/書出し禁止 ・携帯電話の持ち込み禁止 ・メールやネットの利用制限・禁止(フィルタリング等)	10.フォーマルな監視体制を強化する ・侵入警報装置 ・警備員	15.利益を否定する ・重要情報の暗号化 ・重要情報にノイズや電子透かし各種ウォーターマークを注入	20.模倣犯を阻止する ・インシデントの手口の公開を慎重にする ・インシデントの証跡を残さない	25.薬物・アルコールを規制する ・職場での飲酒禁止/検査 ・アルコールなしの行事

出典：情報処理推進機構レポート「組織内部者の不正行為によるインシデント調査」P.11

第４章　基準・ガイドラインと認証制度

この章では、既存のデータセンターのセキュリティにかかわるガイドライン、基準と、これらへの準拠性を証明する認証制度等を、用いられる頻度の高いものを中心に説明します。

3 章では、データセンター利用者がデータセンターのサービスのリスクを分析し、脅威に対する考え方を整理し、セキュリティ管理策を実施するところまでを説明しましたが、逆に監督官庁などがトップダウンで管理策を要求する様々なガイドライン、基準が社会には存在しています。

これらの基準は世の中に多数存在しているものの、その所在は分散していて、似たようなものも多いことから俯瞰的な理解をすることが難しいものでした。この章を読むことでデータセンターの利用者は自身に関係のある基準をピックアップし、その概要を容易に理解することができます。

特に近年ではデータセンターが国家に欠かせない社会インフラとなっていることを背景として、データセンターのセキュリティに係わる様々な規格・基準が整備されています。また、こうした動向に加えて、前述の規格・基準等への準拠性、適合性等を客観的に評価する第三者評価制度・国による認証制度等も整備されつつあります。しかしながら、これらの基準や制度等の関係は、その歴史的経緯もあり、整理して理解されているとは言えない状況にあります。更に、昨今では、データセンターが様々な分野で利用されるトレンドにあわせて、それぞれの分野においてガイドラインが整備されています。

本章では、データセンターの利用者向けに、データセンターのセキュリティに係わる基準、ガイドライン、認証制度について解説した上で、「マネジメントシステム適合性評価制度」、「安対制度」「その他のデータセンターの規格・基準等」を紹介し、最後にそれぞれの分野に存在する「分野ごとの制度・ガイドライン」を解説することで、読者がこれらの関係を整理して理解できるよう手助けします。

なお、本章で扱う基準・ガイドライン・認証制度に関する情報は 2017 年 7 月現在の情報となっています。本節を活用するに当たっては最新の情報を別途ご確認ください。

４.１ 基準・ガイドライン・認証制度の概要と関係

この節ではデータセンターに係る規格・基準、制度、ガイドラインの関係を整理、解説します。

４.１.１ 基準と認証制度

「規格・基準」とは、製品等の品質・形状・寸法を一意に定めることであり、「規格・基準」に適合する製品等を製造し、その相互運用性を高めることを目的として策定されてきました。更に、近年では相互運用性のみならず、判断のよりどころとなる社会的な位置付けを与えることで社会活動を円滑にするという目的も付与されています。

そして、データセンターが国家に欠かせない社会インフラとなっている今、「規格・基準」等への準拠性、適合性等を客観的に評価する仕組みである、第三者による「認証（certification）」も多くのデータセンターにおいて利用されています。「規格・基準」の制定、認証の仕組みや、認証の運用などをおこなう機構や組織の全体のことをまとめて「基準・認証制度」と呼ばれます。図 20 では「基準・認証制度」の仕組みを図解しています。供給者とその需要者の間で取引される製品・サービス・プロセスが認証基準を満たしていることを認証機関が認証するのが「基準・認証制度」の基本的構造となっていて、認定機関は認証機関の認証を遂行する能力を公式に認定することによって、認証制度の信頼性を保つ役割を果たしています。

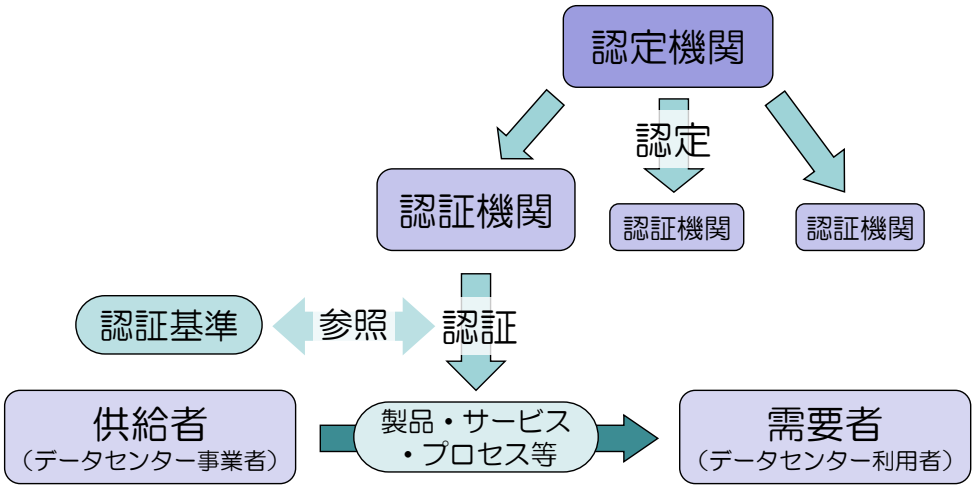


図 20　基準・認証制度の仕組み

一方、「基準・認証制度」全体を活用せず「規格・基準」のみを用いて自主的に適合/準拠を宣言することも可能であり、こういった場合を「自己適合宣言」と言います。また、監査法人などの認証業務を行っている機関が認証制度を用いない、あるいは認証制度がない基準に対して一定の手続きを通じて基準への適合性を確認するようなケースもあります。データセンター事業者が「規格・基準」への準拠を謳っている場合、どのケースに当てはまっているかを確認することも重要です。

4.1.2 データセンター事業者の掲げる認証について

データセンター事業者は様々な規格について認証の取得（あるいは、自己適合宣言）を謳っていますが、それらの規格にはどのようなものがあるかを紹介するために、ここでは４つの項目に注目します。以下にそれぞれの項目ついて説明します。

認証制度等の有無

認証制度等の有無[31]に関する分類項目です。

関連法規の有無

基準に関連する法規の有無に関する分類項目です。関連法規があるパターンとしては、法律の規定を基準が参照している場合と、法律のうち省令などで定める部分において参照される場合があります。

特定業種向けの基準-不特定業種向け基準

特定業種に紐付けられた基準であるか否かに関する分類項目です。業種が特定される場合は、その業種に適応される法令などにおいて参照される基準の場合と、業界が自主的に策定した基準の場合があります。

レベル分けの有る基準-ない基準

複数の等級を持った基準であるか否かに関する分類項目です。複数の等級を持つ基準はデータセンター事業者の多様な事業形態を許容する認証の方法として、主に民間の団体による認証の基準として策定されています。

項目に基づいて、いくつかの代表的な基準・ガイドラインを分類した表が次の表 9 になります。次に、それぞれの分類が持つ特徴と基準・ガイドラインを用いることのメリット・デメリットについて紹介します。

31：認定機関・認証機関といった枠組みを用いていない「適合性評価制度」も含んでいる

表 9　データセンター事業者の掲げる基準・ガイドラインの分類例 [32・33・34]

	認証制度	関連法規	業種	レベル分け
ISO/IEC 27001(ISMS)	○(JIPDEC)	-	-	-
ISO/IEC27017 ＋ JIP-ISMS516-1.0	○(JIPDEC)	-	-	-
ISO/IEC 20000(ITSMS)	○(JIPDEC)	-	-	-
ISO 22301(BCMS)	○(JIPDEC)	-	-	-
JIS Q 15001(PMS)	○(JIPDEC)	(個人情報保護法)	-	-
FISC 安全対策基準	△※1	銀行法等(金融機関検査マニュアル)	○(金融)	-
JEITA IT-1002A	△ (JQA)※2	-	-	-
JQA 運用基準	△	-	-	-
PCI DSS	○(PCI SSC)	-	○(金融)	-
JDCC ファシリティスタンダード	△※3	-	-	○(4段階)
政府情報セキュリティ統一基準群(2016年版)	-	IT基本法等	○(政府)	-
医療情報受託管理事業者ガイドライン	-	医師法等	○(医療)	-
⋮	⋮	⋮	⋮	⋮

分類1（水色）：マネジメントシステム基準系

マネジメントシステムの構築・運用・検査の仕組みの基準をここではマネジメントシステム基準系としています。この系には基準自体では具体的な管理策を示していないため、様々な形態の事業者に当てはめることができるといった特徴があります。

メリット：　設備等の紹介では理解されにくい、「マネジメントシステムが機能していること」を説明できます。

デメリット：設備の紹介と併用しなければ、実際の「セキュリティの程度」を伝えることが難しいという点があります。

分類2（緑色）：認証基準系

マネジメントシステム認証以外の認証に用いられる基準をここでは認証基準系としています。多くの基準はその基準が前提としている業態がある（例えば、FISC 安全対策基準では金融業）という特徴があります。また、設備に関する基準と運用に関する基準を組み合わせて適合性を評価しているという特徴もあります。

32：(表中※1) JQA の適合性評価制度においては FISC 安全対策基準の中の「設備」「運用」「技術」の三つのセクションのうち「設備」のセクションのみを基準として採用している。

33：(表中※2) △は JQA による適合性評価制度が「FISC 安全対策基準(設備)」または「JEITA　IT-1002A」と JQA 運用基準の組み合わせにより実現されていることを示す

34：(表中※3)日本データセンター協会 JDCC では 2015 年度から「環境にやさしいデータセンター認定制度」の一環として、ティア 2 水準を満たすデータセンターの認証を提供していたが、2016 年年度末をもってこの認定事業を終了している。認定基準・認定データセンターは　http://www.jdcc.or.jp/greendc/　に掲載されている(2018 年 3 月 31 日まで).

メリット：　特定の分野の利用者に対して、その分野において必要とされるセキュリティを提供していることを説明できます。
デメリット：認証基準が対象としていない分野の利用者から「過剰なセキュリティを提供している（≠過剰なコスト）」とみなされてしまう可能性があります。

分類3（黄色）：ティア系

対象を複数の等級に分け評価する基準をここではティア系基準と分類しています。この系の特徴としては、民間の企業による格付けサービスが提供されているという点があります。

メリット：　データセンター事業者がセキュリティをどのような考え方で実現しているか、データセンターの特徴を理解しやすいという点があります。
デメリット：利用者側に、一定の理解力が求められます。

分類4（赤色）：ガイドライン系

ガイドライン系は特に官公庁などが特定の業界に対し一定の水準を示すために利用されることが多い枠組みです。官から民へという流れの中で官が主導する認証制度が一般に受け入れられにくくなってきたため登場した形態と捉えることもできます。認証基準系との大きな違いは認証制度の有無がありますが、監督官庁が特定の業態を想定して作成する場合が多いため、情報の具体性が高く、事業者にとって参照しやすいものになっているといった特徴もあります。

メリット：　特定の分野における法制度と関連する物があるため、ガイドラインへの準拠を確認することで、順法性を確認することが出来ます。
デメリット：現時点では認証制度等が整備されていないため、事業者に対し、どのようにガイドラインに準拠しているか項目ごとに説明してもらう必要があります。

ここで紹介した基準や４つの分類はあくまで一つの例ですが、データセンターがどういった分類の基準への準拠を示しているかを知ることによって、そのデータセンターの考え方を知るためのヒントとすることができます。

これらの認証基準の歴史的経緯として、図 21 に示されるようにコンピュータがビジネスに用いられるようになった 70 年代から国(経済産業省)を中心として認証基準に基づいた認定制度の運用が行われてきましたが、2000 年を境に国際標準を用いたマネジメントシステム適合性評価制度への移行がおき、2010 年代に入ってから認証基準に基づいた認定制度の穴を埋める形で民間団体から新たな認証基準やティア系基準が登場し、認定制度に用いられています。

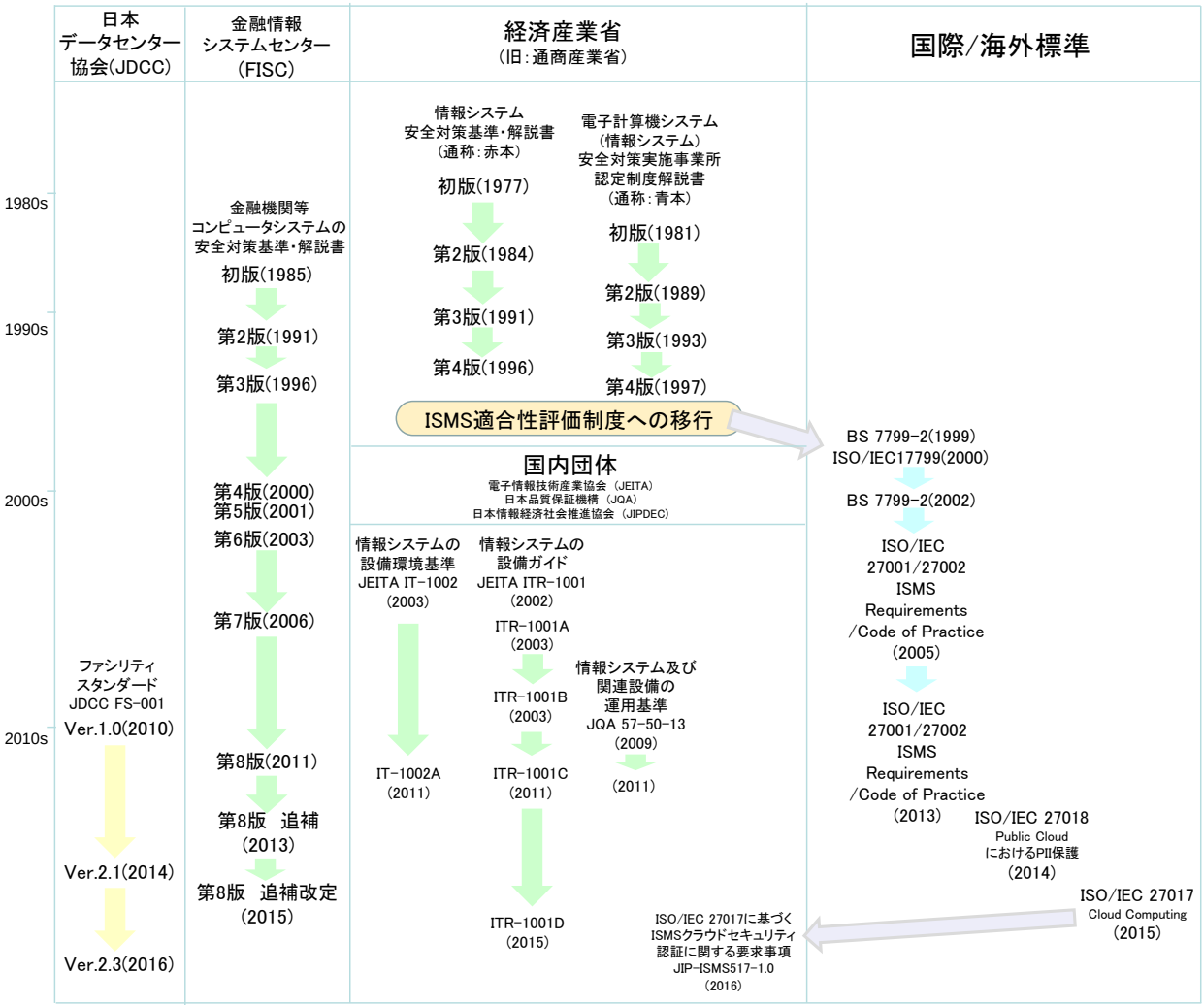


図 21　データセンターで用いられる基準の動向

コラム⑫ 内部統制の保証報告制度について

個人情報保護法と並び、データセンターに大きな影響を与えた法律として、2006 年の金融商品取引法があります。この金融商品取引法の内、内部統制報告書の提出を義務付ける部分は米国の同様の法律の名前をとり、日本版 SOX（J-SOX）法と呼ばれています。

また、企業による大規模な情報流出や不正経理問題によって、次第に消費者側も情報保護に関心を示すようになり、2000 年代後半には多くの企業において企業の社会的責任に対する意識が高まりました。

そういった環境の中でデータセンターには、複数の企業から業務の委託を受けるビジネスモデルゆえに様々な安全性に対する監査要求が企業より個別にもたらされることになりました。それらの監査要求は各社のポリシーや業界によって様々なものがあり、データセンター側の対応コストが肥大化していくことになりました。

このような背景の下で注目を集めたのが、委託業務について内部統制の整備・運用状況を示す文書である日本公認会計士協会の第 18 号報告書、米公認会計士協会の SSAE16（旧 SAS70）と呼ばれる報告書です。この報告書を共通の監査報告として使うことで、データセンター利用者はデータセンター事業者に対しておこなう内部統制の整備・運用状況の監査を省略でき、データセンター事業者は複数のデータセンター利用者による監査業務を省略できるといったメリットがあります。

なお、内部統制における保証報告については、本来財務報告に関連した統制報告のための枠組みだったのですが、SAS70 ではその汎用性から業務統制全般における報告で活用される場面が増えていました。そこで AIPCA（米国公認会計士協会）では、SSAE16 への移行に当たってその役割を明確化させるため、これまでと同じ財務報告に関する統制報告である SOC（Service Operation Control）-1、監査人同士のコミュニケーションツールに限定した財務報告以外に関する統制報告である SOC-2、監査人以外とのコミュニケーションツールとして利用可能な財務報告以外に関する統制報告である SOC-3 の 3 種類の報告書が利用可能になりました。

特に SOC-3 に関しては SysTrust、WebTrust という「Trust サービスの原則と規準（Trust Services Principles and Criteria）」に基づいた情報サービス/Web サービスの認定業務が提供されていて、国内においても一部の監査法人から取得することが可能になっています。

４.２ マネジメントシステム基準を用いた制度

企業などの広告や案内に、「ISO 9001 取得」とか「ISO/IEC 27001 取得」という表示を見ることがあります。これは、その企業や団体（以下、組織）の業務を進めるための仕組みが、定めた目標を達成するためにきちんと作られ、かつ運用されていることが、公平な立場の機関によって証明されたことを表しています。その証明（認証と呼びます）のために用いられる基準が「ISO 9001」や「ISO/IEC 27001」であり、これらは国際的に認められた「マネジメントシステムの国際規格」です。

組織は ISO 9001（品質マネジメントシステム規格）や ISO 14001（環境マネジメントシステム規格）、ISO 27001（情報セキュリティマネジメントシステム規格）に代表されるマネジメントシステム規格の要求事項に基づいてマネジメントシステムを構築し、認証（審査登録）機関は、組織が構築したマネジメントシステムが規格の要求事項に適合しているか審査し、適合していればその組織を登録し、公表します。この制度がマネジメントシステム適合性評価制度と呼ばれています。

マネジメントシステム適合性評価制度は「認証（審査登録）機関」のほかに、認証機関の審査員になるために必要な研修を実施する「審査員研修機関」、審査員の資格を付与する「審査員評価登録機関」、そしてこれらの三つの機関がその業務をおこなう能力を備えているかをみる「認定機関[35]」により制度の品質を担保しています。

マネジメントシステムの認証を得ているということによって、一般消費者や取引先などは、直接その組織の活動内容を知らなくても、そこからの結果（製品やサービスなど）に対して信頼を置くことが可能になります。ISO マネジメントシステム認証は、国際規格に基づいています。国内の法律に基づくものではありません。しかし、組織、認証・認定機関のいずれの活動も国際的な ISO 規格に基づいています。そのため、認証の価値は日本国内だけではなく国際的に認められ、全世界で合計 100 万以上の組織が認証を取得しています。

認証組織は、初回審査の後も年に 1 回以上の中間的な審査（維持審査）が、そして 3 年毎に全面的な審査（再認証）が実施され、組織のマネジメントシステムが引き続き規格に適合し、有効に維持されていることが確認されます。

現在では多くの ISO マネジメントシステム規格が発行していますが、本節では、データセンターに関連が深い三つのマネジメントシステム規格（ISO/IEC 27001、ISO/IEC 20000、ISO 22301）と、マネジメントシステム規格(ISO/IEC 27017)から発展したクラウドに関する三つの認定制度等について紹介します。

35：代表的な認定機関に一般財団法人日本情報経済社会推進協会(JIPDEC)　情報マネジメント推進センターがある。

４.２.１ 情報セキュリティマネジメントシステム：ISO/IEC 27001

ISO/IEC 27001 とは、組織が保有する情報にかかわるさまざまなリスクを適切に管理し、組織の価値向上をもたらす情報セキュリティマネジメントシステム（ISMS）の国際規格です。

今日、情報は組織にとって重要な資産であると認識されるようになってきました。しかし、価値ある情報は常に流出、改ざん、喪失などのさまざまなリスクにさらされています。ISMS の国際規格 ISO/IEC 27001 は、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の三つをバランスよくマネジメントし、情報の有効活用を可能とし、組織の社会的な価値を向上させます。また、同時に内部統制やコンプライアンスの徹底にもつながります。

ISO 27001 認証取得事業者を利用することによる利用者のメリット

情報セキュリティを通じて社会や顧客からの信頼向上や社員の意識•モラル向上を実現できるほか、さまざまな効果が期待できます。

- 情報セキュリティを通じた社会や顧客からの信頼獲得
- 社員の情報セキュリティ意識・モラルの向上
- 情報リスクの低減
- 業務効率の改善や組織体制の強化
- 継続的な改善による企業価値の向上
- 海外企業を含む取引要件の達成
- 企業競争力の強化
- 法令順守（コンプライアンス）の推進
- KPI（キーパフォーマンス指標）の管理
- リスクマネジメント

4.2.2 IT サービスマネジメントシステム：ISO/IEC 20000

ISO/IEC 20000 は、IT サービスを提供している組織が、サービスの内容やリスクを明確にすることで、IT サービスの継続的な管理、高い効率性、継続的改善を実現するための国際規格です。

今日の組織活動において、IT を用いたサービスの提供は欠かせないものとなっています。ISO/IEC 20000 は ITIL[36]をベースとして開発された IT サービスマネジメントシステムの国際規格で、組織が顧客に提供する IT サービスの内容やリスクを明確にし、IT サービスの継続的な管理、高い効率性、継続的な改善の機会を作ることを可能にするツールです。

ISO/IEC 20000 の導入は IT サービスの提供において、顧客重視のビジネス関係の維持や可用性（Availability）の改善に加え、効果的なサプライヤー管理と良好なスタッフ管理につながり、中長期的なコストを低減させる効果をもたらします。また、高品質の IT サービスを安定的に提供することを可能にし、組織の社会的な信頼や競争力を向上させます。さらに ISO/IEC 20000 の導入は内部統制の充実にも有効です。

ISO 20000 認証取得による利用者のメリット

IT サービスの内容・リスクの明確化により、サービス品質や可用性の改善、顧客重視の有効なビジネス関係維持が期待できるほか、さまざまな効果が期待できます。

- サービス内容・リスクの明確化による品質向上や可用性改善
- 顧客を重視した良好なビジネス関係の維持
- 内部統制への活用
- 業務効率の改善や組織体制の強化
- 継続的な改善による企業価値の向上
- 海外企業を含む取引要件の達成
- 企業競争力の強化
- 仕事の見える化による業務継承の円滑化
- KPI（キーパフォーマンス指標）の管理
- リスクマネジメント

36：ITIL：Information Technology Infrastructure Library、IT サービスマネジメントのベストプラクティス集

４.２.３ 事業継続マネジメントシステム：ISO 22301

ISO 22301 は、地震や火災、IT システム障害や金融危機、取引先の倒産、あるいは新型インフルエンザの感染爆発（パンデミック）など、災害や事故、事件などが現実となった場合に備えて、さまざまな企業や組織が、対策を立案し効率的かつ効果的に対応するための事業継続マネジメントシステム（BCMS）の国際規格です。

東日本大震災を機に、地震、津波、火災等の災害や、事故といった緊急事態が起こった場合でも、事業の継続が可能、または早期に再開できるよう、予め事業継続計画（BCP）を取りまとめる企業が増えてきました。データセンターを活用するデータセンター利用者にとっても、データセンター事業者が、BCP を持ち継続して改善している事業者であるかどうかの確認は、とても重要なこととなってきています。

BCMS を認証することで、事業の中断・阻害に対応する事業継続計画（BCP）の運用を経営の仕組みと一体化させ、様々な環境の変化に応じた見直しを行い、効率的・効果的に組織を維持・改善し続けることができます。

ISO 22301 認証取得による利用者のメリット

安心・安全の見える化によって顧客からの信頼を獲得できるほか、さまざまな効果が期待できます。

- 安心・安全の見える化による顧客からの信頼獲得
- 事業活動における優先順位の意識により、競争力の強化
- 業務効率の改善や組織体制の強化
- 継続的な改善による企業価値の向上
- 海外企業を含む取引要件の達成
- 企業競争力の強化
- リスクマネジメント

４.２.４ 適合性評価制度以外の制度

ここまで紹介してきたマネジメントシステム適合性評価制度の他にも、同様の基準を用いた様々な制度が存在しています。本節ではそういった制度[37]について紹介していきます。

特に近年注目を集めている制度に、ISO/IEC27002 をベースにクラウドサービス固有の管理策について記述した規格である ISO/IEC27017 を用いた制度があります。ISO/IEC 27017[38]は ISO/IEC 27001 のような要求事項ではなく、ISO/IEC 27002 と同様に実践の規範であるため、以下で紹介される ISO/IEC 27017 を用いた制度は個々に規範に基づいた要求事項を定め、制度化しています。

JASA 情報セキュリティ監査制度・クラウド情報セキュリティ監査制度

情報セキュリティマネジメントシステム（ISMS）認証制度と同様に JIS Q 27001 及び JIS Q 27002 を用いた制度に日本セキュリティ監査協会(以下、JASA)の運用している情報セキュリティ監査制度があります。

ISMS 認証制度と情報セキュリティ監査の違いは、それぞれの名前にある“認証”と“監査”の違いにあります。すなわち、認証(Certify)は対象がある共通の基準に準拠していることを第三者が認めることを目的とした仕組みであるのに対して、監査(Audit)は、対象が一定の基準を満たしているかの証拠を収集し、その証拠に基づいて評価を行い、これらの内容を利害関係者で共有することを主な目的としています。また、監査における評価は準拠性評価と有効性評価の二つがあります。準拠性評価は基準に準拠しているかを確認することであり、内容は認証における審査と同等です。一方、有効性評価は管理策が有効に機能していることを評価するものです。監査の結果、被監査主体の行為が信頼できるというためには、有効性評価をおこなうことが望ましいといえます。

監査制度では、被監査主体の基準選択の自由度が高く、「情報セキュリティ管理基準」の項目の一部のみの監査を受けることや、あるいは他の基準に基づいて監査を受けることも可能となっています。この監査の実施主体は JASA が研修と試験を通じて認定する公認情報セキュリティ監査人がおこなうことになっていていますが、監査対象となる組織内部の監査人がおこなう「内部監査」と、組織外部の監査人がおこなう「外部監査」のいずれを利用するかも被監査主体が選択出来ます。このように監査は認証制度に比べて被監査主体がその構成を選択できる自由度の高さが一つの特徴になっています。

また、情報セキュリティ監査制度をクラウド分野に適応した制度として同じ JASA が行っているクラウド情報セキュリティ監査制度があります。こちらの制度では基準として前述の ISO/IEC27017 と関係の深い「クラウド情報セキュリティ管理基準」が用いられています。

37：本節で紹介する認証制度等の他にも、ISMS クラウドセキュリティ認証制度の他にも審査機関による独自の認証として、ISO/IEC 27017 等を用いた適合性の審査が行われている。

38： ISO/IEC27017 はその対象としてクラウドサービスを提供する組織（クラウドサービスプロバイダ（CSP））とクラウドサービスを利用する組織（クラウドサービスカスタマ（CSC））を定義していて、それぞれの立場において必要となる管理策が記載されている。この規格の特徴の一つとして、CSP から CSC への情報提供が求められていることがあり、具体的には ISO/IEC 27017 の認定を受けた事業者はホームページ上の FAQ やホワイトペーパーなどを活用し、情報を開示し、その中で責任分界点を明確にする取り組みが求められる。

CSA STAR 認証制度

クラウド情報セキュリティ監査制度に近い認証制度としてクラウドセキュリティアライアンス（以下、CSA）が策定・運用している STAR 認証があります。STAR 認証は、ISO/IEC 27001 の要求事項と CSA のクラウドコントロールマトリックス（以下、CCM）を用いて、クラウドサービス事業者のセキュリティのレベルを認証する制度です。

CCM にはクラウドサービスのセキュリティの成熟度を測る具体的な基準が 16 の管理エリア[39]にわたって記載されています。認定に当たっては CSA からの認定を受けた認証機関の審査によって、被審査組織は「ブロンズ」「シルバー」「ゴールド」のいずれかのレベルで評価されます。

JIPDEC ISMS クラウドセキュリティ認証制度

ISMS クラウドセキュリティ認証は、ISMS 認証等のスキームオーナーである JIPDEC によって実施されている認証で、ISMS 認証を取得している企業がアドオンして取得する認証となっています。クラウドサービス事業者において ISO/IEC 27017 が適切に導入、実施されていることを認証するものです。JIPDEC ではこの認証制度のために ISO/IEC 27017 に基づいた JIP-ISMS517-1.0 という要求事項を定めています。

JIP-ISMS517-1.0、ISO 27017 認証取得による利用者のメリットとして、ISMS 認証取得によるメリットに追加して、以下の効果が期待できます。

- クラウドサービスプロバイダの選定基準の指標となる
- 利用者が ISMS クラウドサービス認証を取得しやすくなる

39：「アプリケーションとインターフェースのセキュリティ」、「監査保証とコンプライアンス」、「事業継続管理と運用継続性」、「変更管理と構成管理」、「データセキュリティと情報ライフサイクル管理」、「データセンターセキュリティ」、「暗号化と鍵管理」、「ガバナンスとリスク管理」、「人的資源」、「アイディンティティとアクセス管理」、「インフラと仮想化のセキュリティ」、「相互運用性とポータビリティ」、「モバイルセキュリティ」、「セキュリティインシデント管理・e ディスカバリ・クラウドフォレンジクス」、「サプライチェーンマネジメント・透明性・説明責任」、「脅威と脆弱性の管理」の 16 エリア

４.３ 情報システム安全対策適合証明制度

前節で紹介した背景から近年では、ISMS 適合性評価制度による認証取得データセンター事業者は着実に増加しています。一方で、ISMS のようなマネジメントシステム基準を対象とした評価では、リスク低減は事業者が個別に定めるセキュリティポリシーに依存します。そのため、データセンターの設備に関してデータセンター利用者は、データセンター事業者に対して提案依頼書（RFP）を要求し、事業者のセキュリティポリシーとそれに基づいた設備の状態を確認する必要があります。

データセンター事業者にとっては、全てのデータセンター利用者及び利用予定者に対してそれぞれ RFP を記載して回答しなければならず、非常に手間が掛かる作業となっています。

このような手間を簡略化するため一定程度のセキュリティを担保する設備基準を定め、それに対する準拠性を確認する制度として通商産業省による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がありました。また、近年ではその制度の後継として一般財団法人 日本品質保証機構（以下、JQA）が実施している「データセンター安全対策適合証明制度」があります。本節ではこれらの制度について紹介します。

４.３.１ 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

電子計算機システム安全対策基準

1977 年、通産省は情報システムの機密性、保全性及び可用性を確保することを目的として、「電子計算機システム安全対策基準」 を制定し公表しました。それに合わせて、同年には社団法人 日本情報センター協会より同基準の解説書（通称赤本）が発行されました。

「電子計算機システム安全対策基準」は、設備基準と運用基準の二つにより構成されていましたが、1984 年の改訂版より設備基準、技術基準、運用基準の三つの基準から構成されるようになりました。1995 年の改訂では、「電子計算機システム安全対策基準」の名称が「情報システム安全対策基準」に変更され、構成される三つの基準のうち、設備基準の名称が、設置基準に変更されました。

この基準は、「情報システムの利用者が実施する対策項目を列挙したもの」として制定されていたため、この基準による検査等はあまり実施されていません。しかしながら、日本国内で初めて情報システムに関する安全対策基準及び施策として取りまとめられたことから、国内のデータセンターの安全対策の基本的な考え方となり、この基準の果たした役割は大きいものとなりました。

さらに通産省は、我が国のコンピュータ利用による情報化の進展に伴い、情報処理サービス事業者の経済活動及び社会生活に果たす役割が重要になってきたことを踏まえ、情報処理サービス事業者の情報システムが地震、火災、水害、犯罪等により破壊され、データが破損、漏えいするといった事故を防ぎ、事業者の安全対策促進を図るため、1981 年に大臣認定制度を発足させました。大臣認定制度の「基準・認証制度」は、次のような構成になっています。

規格・基準： 情報処理サービス業電子計算機システム安全対策実施事業所認定基準
（昭和 56 年通商産業省公示 56 機第 2532 号）
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基準
（平成 9 年通商産業省告示第 406 号　平成 10 年 4 月 1 日より適用）
認定機関: 通商産業省（現 経済産業省）
指定検査機関: 財団法人 機械電子検査検定協会（JMI、現 JQA）

この制度は、認定希望事業者の申請に基づき、情報システムに関して設備基準（83 項目）と運用基準（45 項目）から構成される認定基準に合致している事業所を通産大臣が安全対策実施事業所として認定し、認定証（有効期間 3 年）を交付、官報にこの旨を公表する制度です。この認定基準は、前述した「電子計算機システム安全対策基準」を参考にして制定されました。

実施体制としては、認定の申請事業者が、通産大臣の指定検査機関である財団法人 機械電子検査検定協会（JMI）（現 JQA）より設備検査を受け、その検査結果報告書等を申請書類に添付し、管轄の通産局へ認定の申請を行います。認定の申請を受けた管轄の通産局は、申請事業所の運用に関する審査を行い、その結果を通産大臣に報告します。その結果は、通産省の認定委員会で審議され、認定基準に適合していると認められた場合は通産大臣から認定証が交付されます。

この制度の解説書（通称：青本）が、1981 年に社団法人 日本情報センター協会[40]により発行されました。1993 年には発行者が JQA に変更され、認定制度発足の初年度は 16 事業所程だった認定事業所が、1997 年 7 月時点では 200 事業所にものぼりました。

その後、大臣認定制度は 2001 年 3 月、

- 情報セキュリティの実施に関しては、国際標準でおこなうことが重要だということ。
- 適合性評価制度に関しても、国際的な流れである民間評価を導入すべきであること。
- 大臣認定制度は告示に基づく制度であり、「公益法人に対する検査等の委託等に関する基準」（1996 年 9 月に閣議決定）からみて制度の改正が必要であること。

の 3 点を理由に大幅に見直しをされることになりました。この見直しを受けて、同年に大臣認定制度は廃止[41]され、民間による BS7799[42]を取り入れた情報セキュリティマネジメントシステム（ISMS）の認証制度となりました。また、制度の移行によりこれまで活用されてきた認定基準も同じく廃止されることとなりました。

JQA 情報システム及び関連設備の運用基準

前述の大臣認定制度の廃止に伴い、廃止された認定基準のうち、運用基準は JQA によって引き継がれ、2009 年 4 月、「JQA 情報システム及び関連設備の運用基準」として制定されました。

40：現　一般社団法人 情報サービス産業協会（JISA）
41：2000 年 7 月の通産省告示第 471 号による。
42：現　ISO/IEC 27001 等

情報システムの設備環境基準及び情報システムの設備ガイド

大臣認定制度の廃止に伴い、認定基準（設備基準及び運用基準）も同時に廃止されることとなりました。しかし、民間からの「一定の対策レベルを示すガイドラインを残してほしい」という要望から、廃止された認定基準のうち、設備基準については社団法人　電子情報技術産業協会（JEITA）によって引き継がれ、「情報システムの設備ガイド（JEITA IT-1001）」として 2002 年 1 月に制定されました。

2003 年には、「情報システムの設備環境基準（JEITA IT-1002）」と「情報システムの設備ガイド（JEITA ITR-1001A[43]）」が制定され、それぞれ JEITA IT-1002A と、JEITA ITR-1001D に改訂され、現在に至っています。2014 年に行われた JEITA ITR-1001C から JEITA ITR-1001D への主な改訂ポイントは、次の通りです。

- 東北地方太平洋沖地震 (2011.03.11)の教訓を元に、システム安定稼働、事業継続、人身安全に留意し更新した。
- 参考文献として「ASHRAE 環境ガイドライン 2004, 2008, 2011」を追加した。
- 参考文献として「ガス系消火設備の放射音が精密機器に与える影響について」を追加した。
- 大地透過電流と漏えい電流の関係性を明確にした。
- 空気調和設備に関し、省エネ運転を意識した内容を追加。
- Ⅲ-13.における「内装等」について、天井、壁、スラブ及び柱の表面仕上げに加えて、巾木、窓枠等が含まれることを明確にした。

４.３.２ 情報システム安全対策適合証明制度

2009 年から JQA は「情報システム安全対策適合証明制度 [44]」を実施しています。「情報システム安全対策適合証明制度」の中には保管センター向けの「保管センター安全対策適合証明制度」、リサイクル処理センター向けの「リサイクル処理センター安全対策適合証明制度」、データセンター向けに実施している「データセンター安全対策適合証明制度」があります。

中でもデータセンター安全対策適合証明制度は、廃止された大臣認定制度の認定基準であった「情報システムの設備環境基準」と「JQA 情報システム及び関連設備の運用基準」を使用した制度になっています。データセンター安全対策適合証明制度の「基準・認証制度」としての構成を整理すると、次のようになっています。

規格・基準：　「情報システムの設備環境基準（JEITA IT-1002A）」
　　「金融機関等コンピュータシステムの安全対策基準 [45]」
　　「JQA 情報システム及び関連設備の運用基準」
適合証明機関:　一般財団法人　日本品質保証機構（JQA）

43：2006 年５月、JEITA ITR-1001B に改訂。
44：保管センター向けに「保管センター安全対策適合証明制度」、リサイクル処理センター向けに「リサイクル処理センター安全対策適合証明制度」がある。
45：設備基準[Ⅰ.コンピュータセンター]

「金融機関等コンピュータシステムの安全対策基準」については「4.5.3　金融分野の基準・ガイドライン」にて詳しく解説します。

このデータセンター安全対策適合証明制度は、

- 「情報システムの設備環境基準（JEITA IT-1002A）」と「JQA 情報システム及び関連設備の運用基準」による適合証明
- 「金融機関等コンピュータシステムの安全対策基準」の設備基準[Ⅰ.コンピュータセンター] と「JQA 情報システム及び関連設備の運用基準」による適合証明

の 2 種類で実施されています。

この制度により発行される適合証を利用することで、データセンター事業者は、上記の基準に適合したデータセンター設備であることが証明でき、各種災害に強いデータセンター設備であることもデータセンター利用者に対してアピールできる上に、利用者からの提案要望等の問い合わせに対する回答作業を圧縮することができます。

４.４ その他の基準・認証制度

ここまで紹介してきた制度に用いられている基準•規格は標準化団体や行政等が基点となって策定されてきたものですが、これらの他に業界団体や、民間企業によって策定された規格・基準等も存在しています。本節ではそういった規格・基準について紹介します。

４.４.１ JDCC データセンターファシリティスタンダード

日本の実情に即した日本独自のデータセンターにおけるファシリティスタンダードを目指して、日本データセンター協会（JDCC）が策定したのが「データセンター ファシリティ スタンダード」（以下、JDCC-FS）です。JDCC-FS は日本において大きな影響を持つ FISC 基準や JEITA 基準といった既存のファシリティ基準との整合を考慮するとともに、TIA-942A のような外国規格、ASHRAE（American Society of Heating, Refrigerating and Air-Conditioning Engineers：米国暖房冷凍空調学会）や IEEE（The Institute of Electrical and Electronic Engineers：米国電気電子学会）のガイドラインを参照して独自のティアレベルを構成しています。

JDCC-FS のベースとなった、TIA-942A Appendix G で紹介される Tier はグローバルな実情に合わせて作成されたファシリティ基準であり、日本の実情が考慮されていないという問題を持っていました。例えば、Tier では電源インフラに対する基本的な考え方として、自家発電設備をメイン（Primary）と考え、商用電源はあくまで自家発電設備のバックアップであると位置付けています。対して、日本の商用電源は世界最高レベルの信頼性を誇っており、日本の実情を考慮した場合、商用電源がメインであり、自家発電設備は商用電源のバックアップと考えることが妥当とされました。他にも日本製品の品質の高さ（故障率の低さ）の考慮や、耐震に対する規定が必要である、といった課題がありました。

JDCC-FS では、データセンターのファシリティに求められる信頼性確保に対して、最低限必要と考えられる項目「基準項目」と、信頼性確保のために採用が望まれる項目「推奨項目」に分け、規定しています。JDCC-FS に基づいてティアレベルの宣言をおこなうには、全ての任意のティアレベルにおいて「基準項目」を満足させることが必要であるとされている一方、立地地盤の安定性や災害後の早期復旧体制の構築、全体エネルギーマネジメントの実施といった項目については推奨項目とされます。推奨項目ついては全ての基準を満足させる必要はなく、各データセンターが求める信頼性に応じ、必要と考える基準を任意に選択してよいものとしています。

また、JDCC-FS では多様化するデータセンターの形態に対応するため、データセンター全体を一つのティアレベルととらえずに、同一センター内のサーバー室ごとに異なるティアレベルを設定する「マルチティア」に対応することも可能としています。

JDCC-FS の特徴的な点として、以下の三つの特徴的な評価項目があります。

地震リスク評価

データセンターの敷地が持つ地震危険度や地盤の安定性、設備の耐震性といった地震リスクに対する地震 PML・建築基準法の新耐震基準を用いた総合的評価。

ファシリティリスク評価

データセンター専用ビルかどうか。あるいは、セキュリティや通信ネットワーク、ファシリティレベルに対する評価。

運営管理リスク評価

データセンターの管理体制や運用マネジメントに対する評価。

JDCC-FS では 2011 年 3 月の東日本大震災の経験を貴重な教訓とするため、震災の経験を踏まえた検証・見直しが行われました。具体的には震災後に発生した電力不足に伴う輪番制の計画停電によって、日本においても商用電源が長時間停電するというリスクが発覚したことから、それに対する追加対策も推奨項目として含まれることになりました。

また、最新の改訂版（2017 年 6 月現在の最新版は JDCC FS-001 Ver.2.3）では、ファシリティスタンダードを使った認定事業で得られた知見を受けて、電源経路および引き込み経路の冗長性に係る評価基準の記載が修正されています。

4.4.2 ASPIC 安全・信頼性に係る情報開示認定制度

特定非営利活動法人　ASP・SaaS・IoT クラウドコンソーシアム（以下、ASPIC）では総務省と合同で「ASP・SaaS 普及促進協議会」を設立し ASP・SaaS 利用者の観点から、これらのサービスの安全・信頼性に係る情報を利用者に適切に開示させるための情報開示指針「クラウドサービスの安全・信頼性に係る情報開示指針」を策定しています。この「クラウドサービスの安全・信頼性に係る情報開示指針」は

- ASP-SaaS の安全・信頼性に係る情報開示指針（第 2 版）
- IaaS-PaaS の安全・信頼性に係る情報開示指針（第 2 版）
- データセンターの安全・信頼性に係る情報開示指針（第 3 版）

の三つの指針から構成されています。これらのうち、ASP-SaaS の安全・信頼性に係る情報開示指針に関しては 2017 年行われた個人情報保護法の改正等の制度改定に合わせて、新たに

- ASP・SaaS（特定個人情報取扱いサービス）の安全・信頼性に係る情報開示指針
- ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針

という分冊が設けられました。なお、これらの情報開示指針に関しては、一般財団法人マルチメディア振興センターを認定機関として情報開示項目の認定制度である「ASP･SaaS 安全･信頼性に係る情報開示認定制度」が実施されています。また、ASPIC からは「データセンター情報開示指針」における開示項目をわかりやすく解説した「データセンター利用ガイド」が公開されています。

コラム⑬ 海外における基準・認証制度

日本国内においてはここまで紹介したような基準や認証制度が主流ですが、海外に目を向けるとこれらの他にも様々な基準や認証制度が存在しています。このコラムではそういった海外(主に米国)で利用されている基準や認証制度を紹介します。

Uptime Institute "Tier Performance Standard"

米国では民間団体である Uptime Institute が Tier Performance Standard と呼ばれる情報システムの稼働信頼性に関する基準（Tier：ティア/階層）と、データセンターの評価サービスを提供しています。Tier Performance Standards では、データセンターに要求されるパフォーマンス・レベルに合わせ、施設要件を 4 つのティア（Tier1-4）に分類しています。Tier が公開している基準は複数あり、「Data Center Site Infrastructure Tier Standard: Topology」ではデータセンター設備の稼働信頼性を、「Data Center Site Infrastructure Tier Standard: Operational Sustainability」ではデータセンター運用の稼働信頼性を記述しています。

ANSI/TIA-942A

ANSI/TIA-942A「Telecommunications Infrastructure Standard for Data Centers」は米国 TIA（Telecommunications Industry Association）が作成したデータセンターの建築設計とネットワーク配線・設備に関して規定した規格です。この規格には様々な付属書（Appendix）が付属しています。その中でも Appendix G は Uptime Institute の Tier Performance Standards をベースとして、その Tier レベルを満たすためにはデータセンターをどのような設計にすればよいのか解説したドキュメントとなっています。

Uptime Institute の公開している基準では本書で扱う範囲のデータセンターのセキュリティに関しての言及はありませんが、ANSI/TIA-942 Appendix G ではアクセス制御や画像監視システム、TEMPEST 対策等のセキュリティに関する記述が含まれています。

ANSI/BICSI-002

BICSI(Building Industry Consulting Services International)は、米国において 1974 年に設立された情報通信技術(ICT)に関する業界団体です。ANSI/BICSI002-2014「Datacenter Design and Implementation Best Practices」は、データセンターにおける、インフラ設備の設計とその実例に主眼をおいた構成となっており、各国で設計要件の決定に使用されています。2010 年に初版が発行され、2014 年版では 500 ページを超えており、全 17 章と 8 つの付属書から構成されています。今回の改訂では、モジュラーデータセンタ、空調設備、DCIM、環境性能、アウトソースモデル、ネットワークセキュリティ等の項目が追加されました。セキュリティ分野については、40 ページの記載があります。また本書では、５つの設備領域について、それぞれを５段階のクラスに分けてデータセンターの性能を評価する指標を示しています。

４.５ 分野ごとの基準・ガイドライン

近年、様々な分野においてデータセンターの利用が進んでいますが、その理由のひとつとして、セキュリティが堅牢なデータセンターが、企業等の個人情報等を扱う情報システムのセキュリティ対策として利用されるようになったことが挙げられます。2003 年に成立し 2005 年の全面施行された個人情報保護法は、個人情報取扱事業者に対して、個人情報の安全管理措置を要求していたため、データセンターの活用を通じてこの安全管理措置を達成するアプローチが一般化しました。

こうしたことから、データセンターのセキュリティに関連する分野ごとの基準・ガイドラインの多くは、各事業分野における個人情報保護法の安全管理措置の要求が元になっています。企業にとって、個人情報保護法の影響は少なくありません。例えば、個人情報保護法の策定以降、各産業分野において策定された個人情報保護に関するガイドラインに準じた安全管理措置を講じてなかった場合、競争入札指名停止などの処分を受ける事例が起きています。さらには、社会から個人情報を適切に取り扱っていない企業として認識され、様々なレピュテーションリスクにさらされる恐れもあります。

個人情報保護法は、2014 年に改正され、2017 年 5 月に同改正法が全面施行されました。改正法では、匿名加工情報の枠組みが新設され、新たに加工方法に関する情報の安全管理措置（第 36 条 2 項）や匿名加工情報の安全管理措置（第 36 条 6 項、第 39 条）が追加されました。

改正前の個人情報保護法においては、主務大臣制と呼ばれる制度の元、事業分野毎の主務官庁が、この「法第 20 条」に沿った、個人情報取扱事業者が遵守するべき、多くの具体的なガイドラインを発行していました。対して、改正法では、主務大臣制は廃止され、権限、ガイドラインの発行等は、個人情報保護委員会に移行され、従来官庁ごとに策定されてきたガイドライン等は今後統合される方向にあります。しかしながら、2017 年 7 月時点では、産業分野ごとの事情を反映した旧法からの事業分野毎のガイドラインが引き継ぎ利用されています。

また、同改正法では企業活動のグローバル化に伴い、事業者の負担を軽減し、個人情報の国境を越えた相互移転を可能とすべく、諸外国の法制度を踏まえた国際的な調和を図るための法整備がなされました。具体的には、第 24 条において、外国にある第三者への個人データの提供について記述されています。

> 個人情報保護法　第２４条
>
> 個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

コラム⑭ 改正個人情報保護法の狙いとデータセンターの役割

2017 年 5 月 30 日、改正個人情報保護法（以下：改正法）が全面施行されました。この改正法は、データセンターの役割にも少なからず影響を及ぼすと考えられます。具体的には、例えば、個人情報が 5000 件以下の小規模事業者も、個人情報保護法の対象となることなどがありますが、一番注目するべきことは、個人情報の保護と利活用の両立が目標となっていることにあります。

2005 年全面施行された旧個人情報保護法は、企業等における情報セキュリティ対応に対して多大な影響を与えました。このことは、情報セキュリティの啓発という意味においても非常に重要な出来事であったと同時に、個人情報の取り扱いのコストを増大させ、あるべき個人情報の利活用を阻んだ面も否定できません。一方で、Society5.0 というコンセプトに代表される今後の社会において、IoT により広く大量に集められた個人情報をいかに活用し、かつ保護するかということは、 日本だけではなく世界的な課題となっていると言えます。

旧法の第一条では、その法律の目的について「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」とされていたのに対し、改正法においては加えて「個人情報の適正かつ効果的な利活用が新たな産業の創出並びに 活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の（個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。）」という文言が追記されています。また、改正法では、「匿名加工情報」という個人情報の２次利用を進めるための枠組みも用意されました。改正法１条の記述に見られるような理念や、「匿名加工情報」といった枠組みは、個人情報を保護した上で利活用することが社会から要求となっており、そのための法改正だったと言えます。

もう一点、改正法が及ぼした大きな変化の一つに個人情報保護委員会の設置があります。個人情報保護委員会は、独立した第三者機関として国内の個人情報保護法制を統一的に監督する三条委員会(国家行政組織法の 3 条に規定され、国家の意思を決定し外部に表示する強力な権限を持つ)として設置された機関です。この個人情報保護委員会の設置によって、保護すべきデータと利用可能なデータの線引きが明確化され、個人情報の保護と利活用の両立をけん引していくものと期待されます。また、個人情報保護委員会が国際的な個人データ流通に向けた執行協力の窓口として機能することで世界規模での個人データ移転の枠組み構築も進められています(コラム⑦参照)。

このような状況の変化によって、データセンター事業者の提供するサービスも、従来の個人情報の保護中心のサービスから、様々な「個人情報の保護と利活用の両立」のためのサービスへと様々に展開していくことが期待されます。

４.５.１ 政府分野の基準・ガイドライン

政府機関において外部委託先としてデータセンターを利用する場合に順守しなくてはならない基準として、内閣官房 内閣サイバーセキュリティセンター(通称、NISC)の定めた「政府機関の情報セキュリティ対策のための統一基準群(以下、政府統一基準群)」があります。この統一基準群は政府機関のとるべき対策の統一的な枠組みを定めた「政府機関の情報セキュリティ対策のための統一規範」、政府機関全体の統一的な枠組みを構築することを目的とした具体的な情報セキュリティ対策のための基準である「政府機関の情報セキュリティ対策のための統一基準（平成28年度版）」、この基準に基づいて個々の政府省庁・機関等の基準を策定する際の手順や統一基準の遵守事項を満たすために採られるべき基本的な対策事項の例示や、考え方等を示した「府省庁対策基準策定のためのガイドライン（平成28年度版）」から構成されています。

この政府統一基準群では、政府省庁・機関等によるデータセンターの利用を外部委託の例として扱っています。そして外部委託の契約に当たっては以下の事項を順守するように規定しています。

(a) 外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
  (ア) 委託先に提供する情報の委託先における目的外利用の禁止
  (イ) 委託先における情報セキュリティ対策の実施内容及び管理体制
  (ウ) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制
  (エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
  (オ) 情報セキュリティインシデントへの対処方法
  (カ) 情報セキュリティ対策その他の契約の履行状況の確認方法
  (キ) 情報セキュリティ対策の履行が不十分な場合の対処方法
(b) 委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。
  (ア) 情報セキュリティ監査の受入れ
  (イ) サービスレベルの保証
(c) 委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させること。

4.5.2 医療分野の基準・ガイドライン

医療分野に関連した情報システムやサービスは、従来、医療機関内において構築、運用されてきました。これは、医療機関における最も重要な情報である医療記録を医療機関外に置くことや、その扱いに大きな制約があり、実質的に、データセンター等の利用が困難だったことがあります。

この制約は、医療記録が紙文書だった時代の名残でもあったのですが、厚生労働省が 2010 年 2 月 1 日に発行した『「診療録等の保存をおこなう場所について」の一部改正について』通知により、大幅に緩和されることになりました。

通知では、『外部保存を受託する事業者による不正な利用を防止するための措置については、「医療情報システムの安全管理に関するガイドライン」第８章を遵守すること』と記述されています。この「医療情報システムの安全管理に関するガイドライン」は、医療情報を扱う医療機関、医療従事者等向けに書かれたガイドラインなのですが、これは、個人情報保護法の医療等分野における、個人情報の安全管理措置のためのガイドラインでもあります。したがって、医療機関は、個人情報遵守のために、このガイドラインに準じた個人情報の安全管理措置を講じることが求められています。

「医療情報システムの安全管理に関するガイドライン」は、医療関係者が遵守するガイドラインとして記述されていますが、医療等に関連するサービスプロバイダーや、情報処理事業者向け等のガイドラインも発行されています（表 10）。

表 10　医療情報の外部保管に関係するガイドライン

ガイドライン名	発行日	発行者	対象、内容
医療情報システムの安全管理に関するガイドライン	2017/5（5版）	厚生労働省	医療従事者向け
ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン	2010/12（1.1版）	総務省	ASP・SaaS事業者向け
医療情報を受託管理する情報処理事業者向けガイドライン	2012/10（改定版）	経済産業省	情報処理事業者向け

これらのガイドラインの中で、データセンターのサービスへの要件が一番詳細に記述されているのは、2012 年 10 月に改定された「医療情報を受託管理する情報処理事業者向けガイドライン」になりますが、今後大幅な改定の行われた医療情報システムの安全管理に関するガイドラインに合わせた改定が行われると考えられます。以下に「医療情報システムの安全管理に関するガイドライン　第 5 版」におけるデータセンターに関連する記述を紹介します。

> 金融情報、信用情報、通信情報は実態として保存・管理を当該事業者以外の外部事業者に委託しており、合理的に運用されている。金融・信用・通信に関わる情報と医療に関わる情報を一概に同様に扱うことはできないが、一般に実績あるデータセンター等の情報の保存・管理を受託する事業者は慎重で十分な安全対策を講じており、医療機関等が自ら管理することに比べても厳重に管理されていることが多い。

また、データセンターを利用する際に求められる事項についても以下のように紹介しています。

> ③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合
> (略)　法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要がある。そのため、それらの事業者等が、本章の他の項の要求事項、本ガイドラインの他の章で言及されている、責任のあり方、安全管理対策、真正性、見読性、保存性及び C で定める情報管理体制の確保のための全ての要件を満たす必要がある。また、それらのサービス形態によって、経済産業省の定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の要求事項も満たす必要がある。

4.5.3 金融分野の基準・ガイドライン

財団法人 金融情報システムセンター[46]（以下、FISC）は、金融機関等のコンピュータシステムにおける安全対策は第一義的には金融機関等の自己責任に基づいて実施すべきとしながらも、金融機関等のよりどころとなるべき共通の安全対策基準として、「金融機関等コンピュータシステムの安全対策基準」を 1985 年 12 月に制定し、同基準の解説書を 1986 年 3 月に発行しました。

この基準は、1984 年 8 月に全面改訂された「電子計算機システム安全対策基準」を参考に、設備基準、運用基準、技術基準の三つの基準を含んでいます。これらのうち、設備基準はコンピュータセンターの安全対策設備基準と営業店[47]の安全対策設備基準から構成されていました。当初、基準と解説書は、別々に発行されていましたが、2003 年 10 月に発行された第 6 版から「金融機関等コンピュータシステムの安全対策基準・解説書」として 1 冊に纏められました。

FISC は、「金融機関等コンピュータシステムの安全対策基準・解説書」を制定していますが、この基準に基づく検査等を実施していません。しかし、金融庁が公表する金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）において、『検査官は、システムリスク管理態勢に問題点が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、「金融機関等コンピュータシステムの安全対策基準・解説書」（財団法人金融情報システムセンター編）等に基づき確認する。』と記載があることから、金融庁の検査官によって安全対策の実施状況を確認される場合があります。

最新版である第 8 版の追補改訂版(2015 年 6 月)ではクラウドサービスを対象とした安全対策基準の対応付け、セキュリティ脅威の実情に照らした記述内容の見直し、システム障害に対するリスク管理体制に関する追記、東日本大震災を踏まえた安全対策基準の検証等が行われました。特に 2013 年 3 月に発行された追補では、データセンター事業者にとって影響の多い変更点として、非常時の自家発電設備の燃料確保の方法等が挙げられています。その一部を以下に掲載します。

46：現　公益財団法人 金融情報システムセンター（FISC）
47：後に、本部・営業店等と改称。さらに流通・小売店舗等との提携チャネルとして、コンビニ ATM を追加。

設 64 自家発電設備、蓄電池設備を設置すること

6 項　非常時に自家発電設備や蓄電池設備が正しく機能するよう、定期的に点検すること。

- 自家発電設備
  - 燃料容量（備蓄による運転可能時間）
  - 冷却水（不足時の運転可能時間）
- 蓄電池設備

(略)

7 項　自家発電設備の稼働時に必要となる燃料等の確保について、以下の内容を考慮しておくこと。

- 燃料
  - 燃料の補給態勢（燃料供給会社との優先供給契約締結の内容等）
  - 燃料の補給が不可能となった場合の対策（電力使用の抑制、企業間の相互協力等）
- 冷却水
  - ライフラインの途絶等による水不足時の補給対策（給水車などによる補給等）

なお、クラウドサービス等の情報取り扱いの外部委託や、Fintech の活用に向けて、FISC では大幅な安全対策基準の見直しを予定しています。見直しにあたっては、先立って行われた「外部委託に関する有識者検討会」での検討結果を受け、リスクベースアプローチによる管理策の明確化と、外部委託などに対する統制基準の拡充をおこなうことが検討されています。以下に、その内容に関する有識者会議報告書の抜粋を紹介します。

1. 情報システムに会する安全対策の達成目標は、個々の情報システムのリスク統制に応じて、必要十分な内容で決定されるべきである。
2. 情報システムに対する安全対策への経営資源配分は、リスク顕在化後の事後対策と比較秤量したうえで、情報システム予算内での新規開発などの調整のみならず、経営資源全体も視野に入れ企業価値の最大化を目指して、決定されるべきである。
3. 上記原則が順守されたうえで、妥当な意思決定が行われ適切に運営されている限りにおいては安全対策は独自に決定することが可能である。

金融機関が保有する重大な外部性を有する情報システム、および機微情報を有する情報システムにおいては、上記に加えて、その社会的・公共的な観点からこのシステムの外部性や保有情報の機微性を考慮に入れた安全対策の達成目標が設定されるべきである。

銀行分野と並んで高いセキュリティを要求する分野にクレジットカードサービス分野があります。2000 年代インターネットにおけるクレジット決済が普及するなか、クレジット決済に利用する「カード会員データ」を、インターネットの決済をおこなう e コマース等から不正に取

得するといった事件が頻発しました。そういった背景の下、代行決済事業者は団体 Payment Card Industry（PCI）を立ち上げ「Payment Card Industry Data Security Standard（PCI DSS）」を公表しました。PCI-DSS にはデータセキュリティ基準要件とセキュリティ評価手順が定義されています。

割賦販売法の第三十五条の十八に基づいて経済産業大臣が「認定割賦販売協会」に指定している (社)日本クレジット協会は、この PCI DSS をクレジットカード番号等の適切な管理を図るために必要な規則と定めています。このためカード情報を保存、処理、または伝送する企業はこの規則に則りサービスを提供する必要があります。

最新の「PCI DSS 要件とセキュリティ評価手順」はバージョン 3.2 で、2016 年 4 月に公表されています。以下に PCI DSS の記述されている安全管理策の目次を示します。

要件 1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
要件 2: システムパスワードおよび他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない
要件 3: 保存されるカード会員データを保護する
要件 4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
要件 5: すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する。
要件 6: 安全性の高いシステムとアプリケーションを開発し、保守する
要件 7: カード会員データへのアクセスを、業務上必要な範囲内に制限する
要件 8: システムコンポーネントへのアクセスを識別・認証する
要件 9: カード会員データへの物理アクセスを制限する
要件 10: ネットワーク資源およびカード会員データへのすべてのアクセスを追跡および監視する
要件 11: セキュリティシステムおよびプロセスを定期的にテストする
要件 12: 全ての担当者が情報セキュリティに対するポリシーを維持する

PCI DSS は、その名前のとおり「カード会員データ」というデータのセキュリティに注目した安全管理策の基準になりますが、「カード会員データ」を処理する情報システム、この情報システムへの物理的なアクセス制御等についても記述されています。また PCI-DSS では要件だけでなく、その要件を満たしているかを確認するためのテスト手順やガイダンスも規定しています。

４.５.４ 自治体分野の基準・ガイドライン

自治体においても、ホームページの公開や電子申請、電子入札等の電子自治体システムのための情報通信機器の設置場所としてデータセンターの活用が進んでいます。

こうした流れを受け、総務省は 2002 年にデータセンターの利用も含めた IT システムのアウトソーシングプロジェクトの進め方、契約の方法、SLA 等に関する指針を示すことを目的とする「公共 IT におけるアウトソーシングに関するガイドライン」を公表しました。このガイドラインでは IT アウトソーシングに向けて検討すべき内容契約の進め方といった基本的な項目に加えて、利用するサービスの形態選定、システム要件設定そして具体的な SLA の検討等の解説が用意されていて、自治体のみならず一般のエンドユーザーとしても参照可能なドキュメントとなっています。

また、国内の全地方公共団体（都道府県、市町村）間の コミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的として構築された総合行政ネットワーク（Local Government Wide Area Network）（以下、LGWAN）は民間のデータセンターの活用も想定していて、ASP サービスからコロケーションサービス（ファシリティサービスと呼称）まで様々なサービスの利用が可能になっています。ただし、データセンターからこの LGWAN に接続し活用・サービス提供をおこなう場合、データセンター事業者及び利用者は LGWAN-ASP サービス [48]として地方公共団体情報システム機構（以下、J-LIS）の参加資格審査、登録を受ける必要があります。LGWAN-ASP サービスは、ファシリティサービス、通信サービス、ホスティングサービス、ネットワーク層及び基盤アプリケーションサービス、アプリケーション及びコンテンツサービスの５種類のサービスに分けられ、提供するサービスの種類ごとにそれぞれ J-LIS の審査、登録を受ける必要があります。

データセンター事業者の受けるLGWAN-ASPファシリティサービスの登録では以下のような項目についての適合が求められることに加えて、公的基準等の準拠として ISMS 適合性証明制度、若しくは相当の基準を満たし、その認証等を取得することを求めています。

48：LGWAN-“ASP”サービスという名称になっていますが、サービスにはホスティング、コローケーションサービスも含まれている。

（1） 建物及び室は、火災、水、落雷、電界、磁界及び空気汚染の被害を受ける恐れのない場所に設けること。
（2） 設置場所であることの所在を明記しないこと。
（3） 外部及び共用部分に面する窓は、防災、防犯の措置及び外光による影響を受けない措置を講ずること。
（4） 出入口は、不特定多数の人が利用する場所を避けるとともに、入退室の管理をおこなうこと。
（5） 建物及び室は、建築基準法に規定する耐火性能を有すること。
（6） 建物及び室は、水の被害を防止する措置を講ずること。
（7） 建物及び室の内装、什器・備品は、不燃、防炎性能を有する材料を用いるとともに静電気による影響を防止する措置を講ずること。
（8） 建物及び室は、避雷設備、火災報知設備、消火設備、非常照明設備、避難器具、小動物被害防止設備等の建築設備を設置すること。
（9） 設置場所は、一般の事務室、居室とは分離した独立した部屋であること。
（10） 情報漏えい、記録媒体の盗難防止措置を講ずること。
（11） 機器の所要電力を安定的に供給できること。LGWAN に接続するための専用機器（以下「LGWAN 接続ルーター」という。）を設置する場合は、供給電源として、単相 100V の電圧並びに LGWAN 接続ルーターの機器諸元に示す所要電力を安定的に供給できること。
（12） 電源設備は、専用の分電盤又は専用の電源配線によるコンセントを設けること。
（13） 機器の動作環境に配慮し適切な空気調和設備を設置すること。LGWAN-ASP 接続設備を設置する場合は、発熱量仕様約 1,000Kcal/h に対し、LGWAN-ASP 接続設備ラック内温度は 0℃から 40℃、湿度は 0%から 80%の範囲で安定的に保持するとともに結露が発生しない動作環境であること。
（14） 空気調和設備は、防災、防犯及び水漏れ防止の措置を講ずること。
（15） 建物及び室の人の出入り、防災設備及び防犯設備の作動、電源設備及び空気調和設備の稼動状況について適切な監視が可能であること。
（16） 建物及び室は地震被害の恐れのある場所、位置を避けて設置すること。
（17） 建物は、建築基準法に規定する耐震構造とすること 。
（18） 開口部、内装、設備、什器・備品は、落下、転倒及び振動等地震による被害を防止する措置を講ずること。

また、表の要求項目に記載はありませんが、登録申請書類には具体的なスペックの入力を求めている項目があります。例えば「（4）出入口は、不特定多数の人が利用する場所を避けるとともに、入退室の管理をおこなうこと。」の項目では（ア）入退館及び入退室の認証方法、（イ）ゲストの入退館及び入退室の管理方法、（ウ）入退館及び入退室の監視方法　の 3 項目に対してチェックが求められています。なお、LGWAN-ASP ファシリティサービスを提供する事業者を利用したい場合、登録を受けた事業者は J-LIS ホームページ[49]から確認することができます。

49：https://www.j-lis.go.jp/lgwan/asp/servicelist/list/lgwan-asp_fa_servicelist.htm

第５章　セキュリティを実現するシステム

5 章では、データセンター事業者が導入しているセキュリティの例として様々なシステムを統合的に管理する「DCIM (Data Center Infrastructure Management)システム」を中心に、「異常監視システム」「アクセスコントロールシステム」「サーバーラックシステム」「ビルディングオートメーションシステム」といったシステムが組み合わされたシステムを、これらをデータセンターに納入しているメーカー・ベンダーの視点から、仕組みや特徴、そして、昨今の技術トレンドをふまえ紹介します。

5.1 データセンターを支える様々なシステム

今日のデータセンターでは、利用者向けにセキュリティ性、安全性、利便性を、データセンター事業者向けに収益、効率、ブランディングのために、さまざまなシステムを稼動させています。

特に最近では、運用システムの自動化や連携を積極的に進め、事業自体の収益を高めながら、提供するサービスの「レベルと質」を大幅に向上させて、競合他社との差別化を明確にしていくデータセンター事業者が登場しています。また提供されるサービスによっては、今まで安全やセキュリティの尺度として活用していた「丁寧な人的サービス」が、顧客ニーズを先取りした「堅実で簡単なシステム自動化サービス」に置き換わりつつあり、データセンター事業者では「安全性・セキュリティ性の概念変化」を意識せざる得ない環境となっています。

データセンターのセキュリティを実現するシステムの例として、本節でも扱う「異常監視システム」「アクセスコントロールシステム」「サーバーラックシステム」「ビルディングオートメーションシステム」といった複数のシステムがあります。従来はこのシステムを利用してファシリティマネージャによりデータセンターのインフラ設備、建物設備の運用がなされてきました。また、ネットワーク技術者、IT 技術者は別々のシステムにより各々の設備運用を実施してきました。

このように、今日のデータセンターは、その運用におけるセキュリティ、安全性、および効率性のために、さまざまなシステムに依存しています。また、提供するサービスによっては、データセンター要員は、データセンターの物理インフラ（電源、空調、セキュリティシステムなど）だけではなく、そのデータセンター内に収容されている事業者自身、あるいは利用者の情報通信機器・システムを管理する責任を負っています。この物理インフラと情報システムの二つはもともと関連し合っていて、一方が変化すると、もう一方も影響を受けています。

また、運用の観点から言えば、それぞれのインフラの調達、管理、および保守は、別々の部門が行っていることが多いと考えられます。通常は、物理インフラについては施設部門とエンジニアリング部門が責任を負い、情報システムについては情報システム部門が責任を負います。稼動中のデータセンターの環境が日々変化する場合、こうしたシステムの分割管理はデータセンターの運営を困難にしています。

そこで近年では複数のシステム間を統合的に管理するシステムを用い、データセンターの全体像を可視化することで、従来の分割管理によって発生していた問題に対してアプローチがとられています。そして、そのアプローチ可能にしたのが、さまざまなシステムからの情報を集計し、十分な情報に基づいて意思決定できるよう支援するシステムが DCIM (Data Center Infrastructure Management)システムです。これらの関係をまとめると図 22 のようになります。

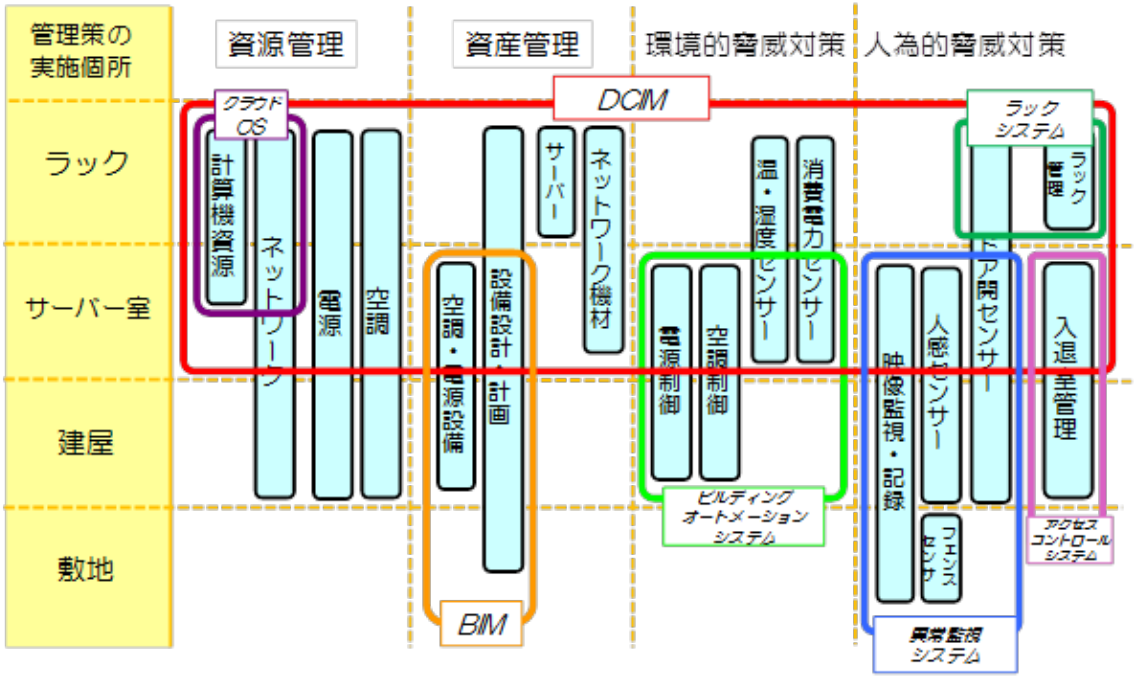


図 22　データセンターを支える様々なシステムの関係図

5.2 DCIM システム

複数のシステム間を統合的に管理するシステムを用い、データセンターの全体像を可視化することで、従来の分割管理によって発生していた問題に対する解決が可能ですが、それを実現するためにはさまざまなシステムからの情報を集計し、十分な情報に基づいて意思決定できるよう支援するシステム、DCIM(Data Center Infrastructure Management)システムが必要です。本節ではこの DCIM を構成するコンポーネントを通じて DCIM システムを概観し、DCIM のカギとなる機能であるダッシュボード機能について解説します。

5.2.1 DCIM システムのコンポーネント

DCIM システムは何十、何百ものハードウェア・ソフトウェアのコンポーネントで構成されます。そうしたコンポーネントを機能に基づいて分類するためのモデルが図 23 です。図 23 では DCIM システムのコンポーネントを Plan-Do-Check-Action のモデルに当てはめ、それぞれのステージで必要となる機能ごとにまとめています。

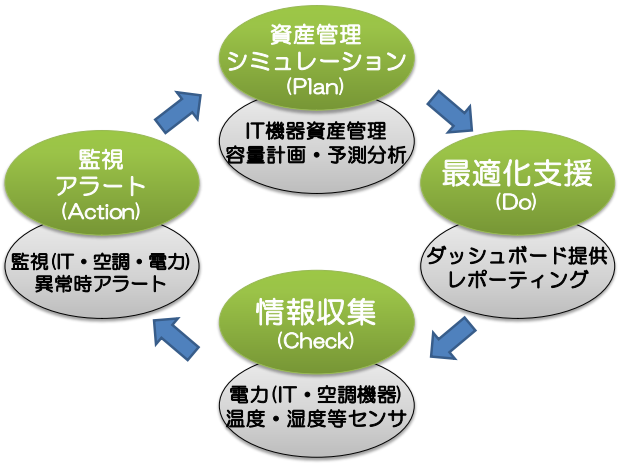


図 23　統合管理システムのコンポーネント

「情報収集」のコンポーネントは、データセンター内の任意の情報に関するリアルタイムなデータの収集や、設備資産に関する資産情報のシステムへの登録支援機能を提供し、以下のような手法によって効率的なデータセンターの状況把握を実現します。

- 様々なセンサーの種類・プロトコルに対応したデータ収集
- 監視対象の柔軟な追加・削除

「監視」「アラート」のコンポーネントは、主要な運用パラメータに関するリアルタイムな時系列情報と、タイムリーな対応に必要となるツールを提供し、以下のような手法によってデータセンターの運用を円滑にします。

- データセンターが計画通りに機能していることを確認する
- 事前に設定された条件をトリガーとして運用要員に異常等を通知する

「資産管理」「シミュレーション」のコンポーネントは、統制された方法でデータセンターを管理・運営するために必要なツールを提供し、以下のような手法によってデータセンターの計画の確度を高めます。

- データセンター内の資産の追跡をおこなう
- 加えられる変更について、その影響をシミュレートし分析する
- 変更を効果的なものにするための計画の支援をおこなう

「最適化支援」のコンポーネントは、様々な形態での情報提供を実現し、以下のような手法によってデータセンターの管理者・運用者のみならず、利用者のデータセンター利活用効率を最適化します。

- データセンター内の環境統制モニタリングの提供をおこなう
- 内部統制報告に利用可能なレポートの自動生成をおこなう
- データセンター利用者の要求に合わせた柔軟なレポート生成をおこなう

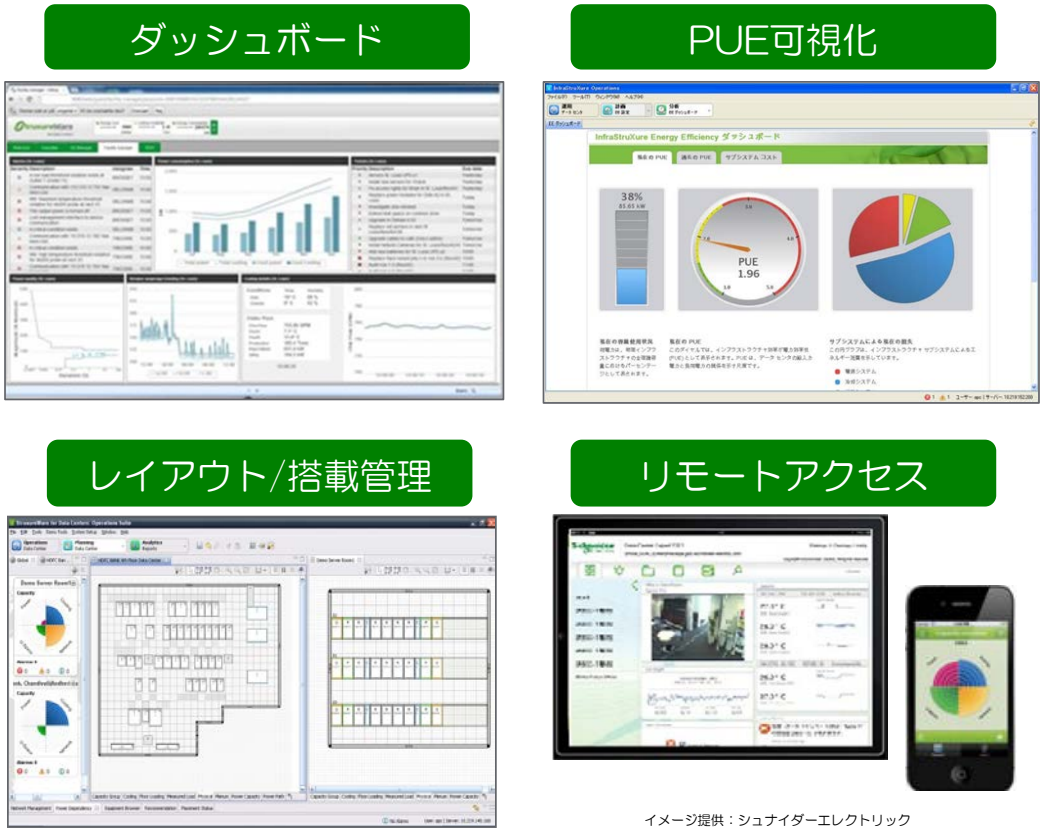
市場には様々な DCIM を銘打った製品が存在していますが、そのコンポーネント構成は様々であり、DCIM システムと呼ばれるものであっても、複数組み合わせることで初めて前述の PDCA サイクルを実現できるような製品もあれば、一つのパッケージで PDCA サイクル全てを実現できるものもあります。

5.2.2 DCIM システムのユーザーインターフェース

ダッシュボードコンポーネントは、データセンターのパフォーマンスに関する重要な情報を統合するための手段となります。その情報は、集計するだけでなく、有意義かつ実用的な形で提示されなければなりません。そのため、ダッシュボードは DCIM を構成するすべてのコンポーネントの情報を一つにまとめることで、データセンターの全体像を確認することができます。運用ダッシュボードに含まれる情報の典型的な例として、次のものがあげられます。

- データセンター内の入退室記録
- 最新の重要な警告
- 特定期間における平均温・湿度、最高・最低の温・湿度
- IT 負荷とデータセンターの総負荷

また、ダッシュボードへのリモートアクセスを可能にすることで 24 時間 365 日の運用をより効果的なものにする、あるいはデータセンターの利用者に対しての適切な情報開示を可能にする機能を備えた製品もあります(図 24)。



イメージ提供：シュナイダーエレクトリック

図 24　運用ダッシュボードの表示画面例

5.3 異常監視システム

本節で紹介する異常監視システムは、温度・湿度といった環境異常、物理的セキュリティ区画への不正なアクセスや、火災や漏水といった異常を検知し、担当者へ通報するシステムの事を示します。ここでは環境異常検知システム、侵入検知システムを構成するセンサーデバイスと、それらを集約して侵入検知時に警報を出すセンサー装置に関して解説致します。

5.3.1 環境異常センサー

サーバー室内環境が適切かどうかを常に監視するセンサーが環境異常センサーです。ここでは、環境異常を検出する為に用いられるいくつかのセンサーを紹介します。

温度・湿度センサー

温度・湿度センサーはサーバー室内の温度・湿度を監視します。特にサーバーラック内部の温度と湿度については、搭載機器の異常に直結する外部要因となるため、管理をおこなうことは少なくありません。搭載機器が吸気するサーバーラック前面エリアを中心に、専用の温度センサーを設置し、温度センサー毎に任意の間隔で取得した温度データを、専用の情報通信機器に記録しているデータセンターもあります(図 25)。また搭載機器の故障を引き起こしやすい高温異常を察知するため、事前に設定した「閾値」を越えた場合、担当者に通報する仕組みを用意しているデータセンター事業者もあります。

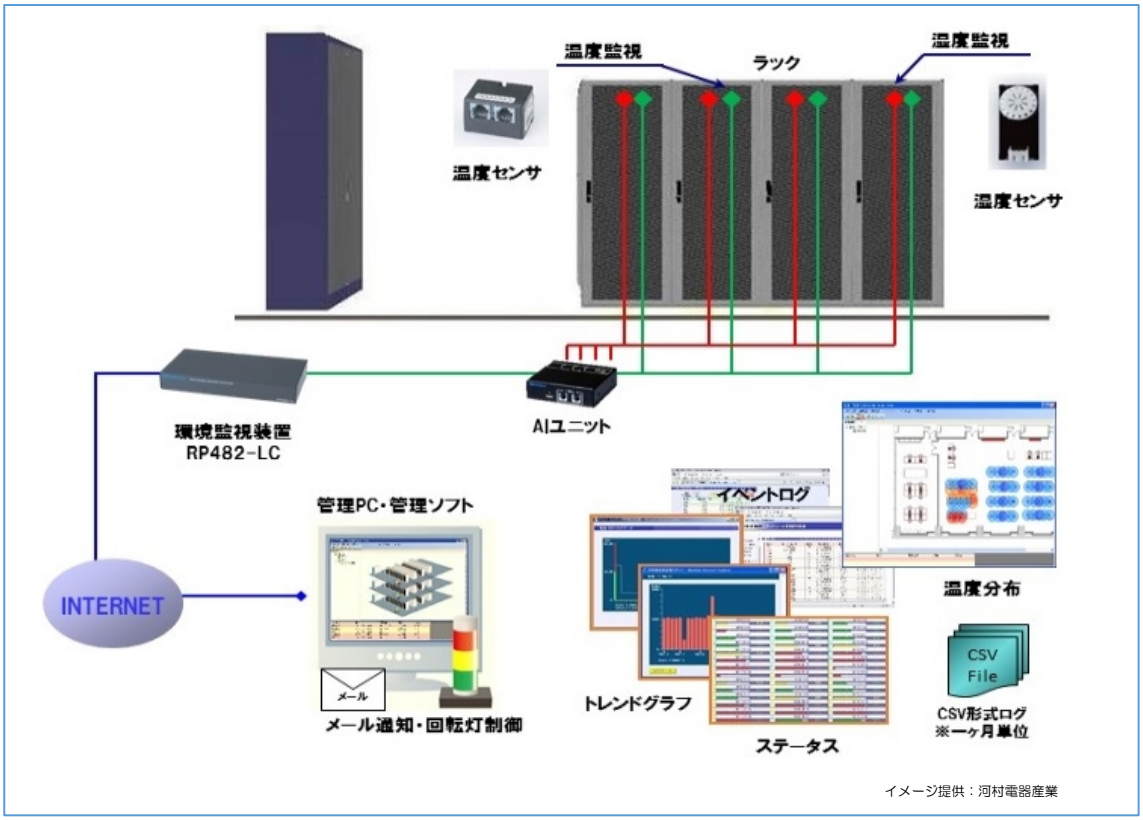


図 25　サーバーラック内温度・湿度監視システムの例

また湿度に関しても、一般的にサーバーラックの搭載機器の最適な湿度数値は 40-55%[50]とされています。この範疇を極端に外してしまうと、多湿による機器への結露現象や乾燥による静電気放電現象での半導体破損が発生し、最終的に搭載機器の故障を引き起こすことになると指摘されています。データセンターでは、空調機で湿度管理を優先して行っている関係上、サーバーラック内部の湿度管理が行われている場合が多くなっています。最近では、サーバーラック列架のコールドアイル部分に湿度センサーを設置し、機器が吸入する空気の湿度を測定しながら、湿度が低下すると加湿器などで湿度調整をしているデータセンター事業者もあります。

電力センサー

電力センサーは情報通信機器や、PDU(Power Distribution Unit)、サーバーラックといった特定の単位の消費電力量を計測し、異常が無いかを監視します。また、送電網から供給される電源を適切な電圧・波形に維持できているかを調べるセンサーを導入しているデータセンターもあります。

漏水センサー

漏水センサーはサーバー室などの床面近くに設置されるセンサーで、サーバー室や重要室の床面に水がたまっていないかを検知します。漏水センサーは、一般に水冷式の空調機を導入しているデータセンターにおいて導入されています。

その他の情報

情報通信機器の故障の原因になるような振動や、サーバー室内の塵埃を検知するセンサーなど、利用者の要求に応じて様々なセンサーが取り付けられています。

5.3.2 侵入異常センサー

侵入異常を検知するセンサーは、マグネットセンサーやガラスセンサーといった「点」の異常を検知する物から、フェンスセンサーのような「線」の異常を検知する物、そして、パッシブセンサーや画像センサーのような「面・空間」の異常を検出する物へと進化してきました。ここでは侵入検知システムに接続される、いくつかの代表的なタイプのセンサーを紹介します。

マグネットセンサー

マグネットセンサーは、ドアやサッシの開閉を磁石とリードスイッチの組み合わせによって検出するセンサーです。非常に安価であり誤報も少ないため様々な場所で用いられますが、サッシに填められたガラス自体が破壊された場合は検知することが出来ないため、下記のガラスセンサーと組み合わせて運用するといった工夫が必要です。

50：米国暖房冷凍空調学会(ASHRAE)のコンピュータールームに関する技術委員会による推奨値

ガラスセンサー

ガラスセンサーはガラスの破壊を検出するセンサーです。ガラスの破壊時に発生する特定の周波数の震動を検知し動作します。

フェンスセンサー

フェンスセンサーにはトラップ方式、同軸ケーブル方式、光ファイバー方式、赤外線ビーム方式といった様々な検出方法を使ったセンサーが存在しています。

トラップ方式は、フェンス上に張り巡らせたワイヤーの張力を端部に設置したセンサーで検知します。この方式の特徴としては、小域での施工コストに優れる、天候の影響を受けにくいといった点が挙げられます。

同軸ケーブル方式は、フェンス上に張り巡らせた同軸ケーブルに接触した時の変形を検知します。この方式の特徴としては、複数同時発生した侵入の検知が可能、侵入地点を特定可能、広域での施工コストに優れているといった点が挙げられます。

光ファイバー方式は、フェンス上に張り巡らせた光ファイバーへかかった圧力を、ファイバー内を走るレーザー光のリング干渉を使って検知します。この方式の特徴としては、最長５ｋｍの広域監視が可能、光検出のため、ワイヤーやケーブルのように雪等が付着し誤動作することがない、広域での施工コストに優れているといった点が挙げられます。

赤外線ビーム方式は、ここまで紹介した方式とは違い、センサー間の空間を赤外線ビームで結び、侵入者がビームを遮ることにより警報を出す仕組みになっています。この方式の特徴としては、最も普及している、施工コストに優れている、侵入者以外の小動物や木枝等による誤報が多いといった特徴があります。

パッシブセンサー

パッシブセンサーは人体等の熱源の発する遠赤外線を複数の区画で検出、その変化パターンによって熱源の移動を検出するセンサーです。パッシブセンサーには検出する空間や変化のパターンに様々なタイプがあり、設置個所における動線等を十分に検討した上で設置するセンサーのタイプを決定する必要があります。

また、センサーによっては画策防止のための様々な工夫が施されているものがあります。

5.3.3 監視カメラ

監視カメラは、侵入者や不正行為の監視・記録を目的に、データセンター内外にカメラを設置して、ライブでのモニタリング及び画像を記録保存するシステムのことを言います。

監視カメラはネットワークタイプとアナログタイプに分けることが出来ますが、近年のデータセンターにおいては、システムの拡張性に優れる等の点からネットワークタイプの画像監視システムが主流になっています。現在は高画質のメガピクセルカメラ（100 万画素以上）が主流で、このタイプを使用すると人の顔の判明がつきやすくなるため、真正性・責任追跡性・信頼性・否認防止の確保がより容易になります。監視カメラはその外装(ハウジング)の形態から大きく三つのタイプに分けることができます。

ＢＯＸ型カメラ

ベーシックなタイプのカメラ。カメラ自体の存在を意識させ、抑止効果を期待したい場合に用いられることがあります。

ドーム型カメラ

ドーム型カメラは BOX 型に並ぶベーシックなタイプのカメラで環境のデザインに溶け込ませ、存在感を意識させず監視したい個所に用いられます。そのシンプルな形状から高い耐衝撃や防塵性を持つモデルもあります。ドーム型のカメラの中には超広角レンズを用いて全周の撮影を可能とするタイプの物もありますが、大きな光学的ひずみを生じるため、ひずみを修正して表示する機能を持ったカメラもあります。

PTZ カメラ

操作 PC から横旋回(Pan)/縦旋回(Tilt)/ズーム(Zoom)操作が可能なカメラ。要員が操作し、不審な被写体を特定して監視するためのカメラとして有効。PTZ カメラは機構が複雑となるため、きょう体や消費電力が大きくなり、コストも高いため、設置個所に制約を受ける場合があります。そのため前述した BOX 型カメラやドーム型カメラと組み合わせて利用されることも多いです。

これらのカメラに加え、環境に合わせた機能を持つカメラがあります。例えば主に屋外で用いられるカメラには防水・防塵の機能に加え、日差し対策や飛来物対策、画策対策を施したハウジング（外装）を持つカメラがあります。また、完全な暗闇(０ルクス)環境下での撮影をしたカメラや、日光等の光源が直接カメラに入った場合や陰になる部分でも、白とびや黒つぶれしない HDR(High Dynamic Range)機能を持つカメラがあり、設備や運用と組み合わせることによって、より効果的に証跡の確保をすることが出来ます。

データセンターのような大規模な建造物における監視カメラシステム構築では、建物の外部・内部においてできるだけ死角を作らないカメラ配置が必要となります。加えて、証跡として残す必要のある画像に関しては、一定以上の画質と完全性を保っての記録を求められるため、十分なストレージ要領の確保、画角にあった解像度をもったカメラの選択、高画質の帯域でも快適にシステム稼働させるためのネットワークの構築、さらには、万が一の障害時の復旧長期化を防ぐための維持・管理プランの策定といった様々な用件が実現されていることを確認する必要があります。

５.３.４ 火災予兆検知システム

データセンター（主にサーバー室）の安全対策を考慮する上で重要なことは、サーバー室で火災が起こった場合に、どのような状況になるのかしっかり理解することにあります。ここでは、サーバー室で発生する火災の性状について説明します。

図 26（左）は、一般のオフィスで火災が発生した場合に、どのように煙が広がっていくかを示したものです。写真では、煙は燃焼の熱による上昇気流に乗り天井面に到達した後に、層を形成しながら水平方向に広がっていくことがわかります。したがって、天井面に消防法で定められた前述

の煙感知器を設置することで、有効に火災を検知することが出来ます。一方で、データセンターのサーバー室のように、室内で強制的な循環空調が行われている場合は、図 26（右）のように発生した煙は強力な空調気流によって天井面に層をつくることができず、拡散し希釈されながら室内全体に充満します。

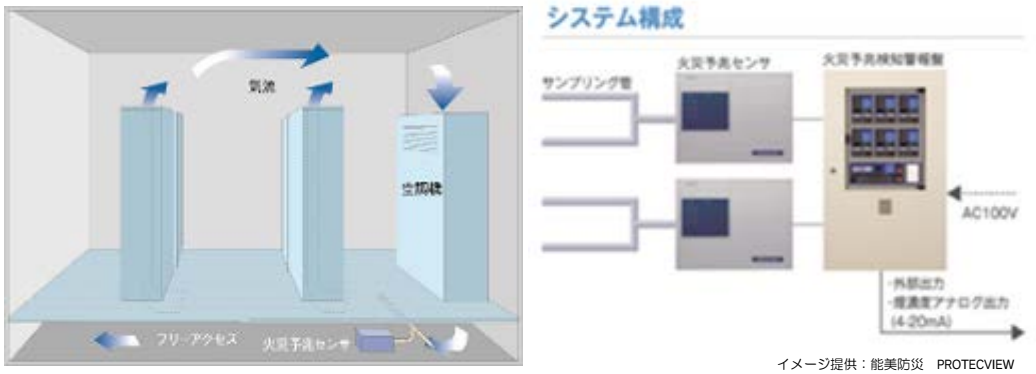
このような火災では、消防法で定められる煙感知器が作動した時点では、既に室内全体に非常に高い濃度の煙や有毒ガスが充満しています。この時点では、高濃度の煙によって視界が遮られ有毒ガスによる危険にもさらされるため、人が室内に入って対応することはほぼ不可能であり、初期消火をおこなうには危険を伴う状態となります。

イメージ提供：能美防災

図 26　一般的なオフィス（左）とサーバー室（右）での煙の広がり方の違い

そして、サーバー室の火災について注意しなければならないのは、室内全体に非常に高い濃度の煙が充満した状態で検知しても、原状回復までに莫大な時間とコストがかかるということです。したがって、安全対策を考える上では、火災の予兆を検知するシステムについて検討することが重要となります。このような要求に応えシステムとして、「火災予兆検知システム」があります。

「火災予兆検知システム」は、監視区画を１点で監視するスポット型のセンサーとは異なり、監視区画の空気を多数の吸引孔を設けたサンプリング配管を通じて、常時区画全体の平均濃度を監視します。サーバー室などにおける空調設備による気流と設置例とシステム構成の一例を図 27 に示します。



イメージ提供：能美防災　PROTECVIEW

図 27　火災予兆システムの設置方法（左）とシステム構成（右）

火災予兆センサーは、超高感度から低感度まで広いレンジで検出可能です。超高感度のレンジでは、消防法で定められた煙感知器に比べ数千倍の検知感度を持っています。これにより、循環気流にて希釈され薄まった煙を早期に検出することができます。また、火災予兆センサーの煙を検知する検出部にはレーザーダイオードを使用し、煙粒子による散乱光の総出力量を検出する「総散乱光受光方式」（粒径による制限を受けない）を採用しているため、燻焼によって生じる煙（白煙）から有炎燃焼によって生じる微粒子の煙（黒煙）まで、幅広い粒子径の煙を高感度で検出することができます。火災予兆検知システムの警報盤には、監視区画の環境濃度がリアルタイムでバーグラフ表示されると共に、デジタル数字でも表示されるため、現在の監視区画の状況を容易に監視することができます。

近年データセンター事業者は、火災を予兆段階から早期に検知し被害を最小限に抑えることで、事業を継続的に維持できると考え、また、社会的責任を果たすことも含め、事業継続計画（BCP）の中に早期火災検出対策を導入し始めています。

一方で、火災予兆検知システムのセンサーによる検知では、検出された区画しか判明せず、発煙箇所の特定をすることは困難です。そのため「火災予兆の個所を特定するための手順を明確にしておく」、「火災予兆発生時の初期対応についての運用フローを明確にしておく」という運用方針と組み合わせて火災予兆検知システムを導入することが BCP 上重要となります[51]。近年では、前者の方針に対応できるように「ポータブル火災予兆センサー(図 28)」という製品が開発されています。この製品は火災予兆センサー発報後、発煙箇所を捜索するための補助ツールです。現地に駆け付けたときには煙濃度が極めて薄いことが想定され発煙箇所の早期特定をサポートします。

図 28　ポータブル火災予兆センサー外観

51：コラム⑨ 運用におけるＢＣＰ的観点による手順構築 参照

5.4 アクセスコントロールシステム

データセンターにはその性格上、入館、入室に対して非常に厳しい管理を施すと同時に、データセンターの利用者に対し十分な利便性を確保するといった、相反する要求が課されています。アクセスコントロールシステムは、その相反する条件を実現するセキュリティ上、最も重要ともいえるシステムです。本節ではそのアクセスコントロールシステムに求められる機能と、その動向について紹介します。なお、サーバーラック内へのアクセスコントロールは、利用者の専有区画のセキュリティ境界として非常に重要な役割を担っているため、「サーバーラックシステム」として次の節において個別の項目として扱っています。

5.4.1 ゾーニングとセキュリティゲート

セキュリティゲートを活用してリスクを低減するためには、セキュリティを検討する際にゾーニングが正しく実現されていることが必要になります。ゾーニングで厳密にセキュリティ区画構成が管理できることで、初めてアクセス権を与えられた人のみがセキュリティ区画に入る状態の実現が出来ます。セキュリティゲートはこのゾーニングの一部を構成する物ですので、ゲートの受け持たない部分からの人の侵入までは防げません。すなわち、いくら高価なゲートを導入しても、ゲートと同等のセキュリティ境界を持って全体をゾーニングしなければ、セキュリティゲート以外のところからの侵入を招くだけであるという点に留意する必要があります。ゲートの種類は大きく分けて、腰高までのデザインの“ハーフハイト仕様”、背の高いデザインの“フルハイト仕様”に分類されます（表 11）。背の高いフルハイト仕様のゲートは、主に無人管理下にて運用されますが、腰高のゲートは乗越えや潜り抜けが出来てしまうため、有人管理下（主に受付や警備員のサポート）で運用することが望ましいと言えます。

表 11　ゲートの種類と適した設置場所

ゲート種類			適した設置場所
ハーフハイト仕様	 トライポットバリア	 フラッパーゲート	セキュリティレベルが比較的低い場所。不特定多数の人が利用する場所。
フルハイト仕様	 ターンスタイルゲート	 インターロックゲート（サークルゲート）	データセンターのようなセキュリティレベルが比較的高い場所。特定の人しか利用しない場所。無人警備を必要とする場所。

一例として、セキュリティ区画別に適したタイプのゲートを配置するとのようになります。図からも分かるように、ゲートと一言に言っても様々なタイプの物が存在していて、使用場所や目的に応じて選択肢が変わります。データセンター全体のセキュリティプランニングと整合のとれたゲートの選択が必要となります。

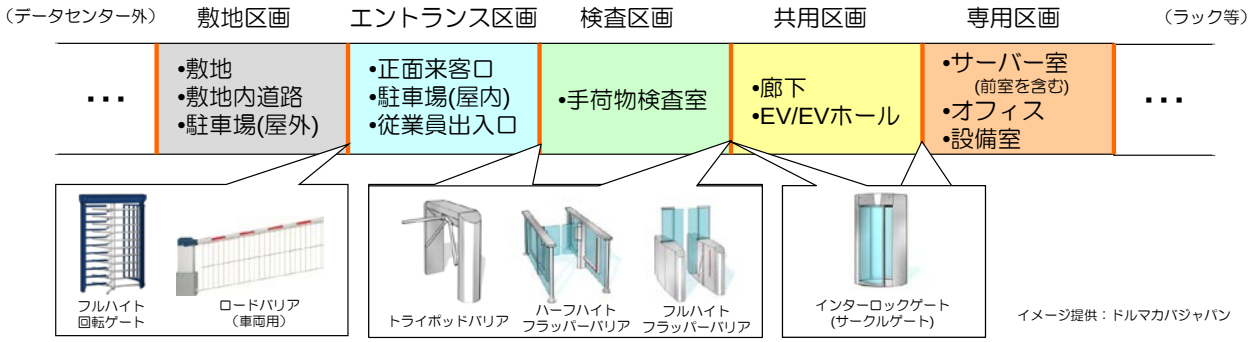


図 29　セキュリティゲートの配置例

5.4.2 人の動きの記録と制御

入退管理システムでは、基本的な機能としてだれが（WHO）、いつ（WHEN）、どこに（WHERE）アクセスしたかを認識し、セキュリティゲートや施解錠機構に伝達し、証跡として記録する機能を持っています。これらの機能を用いることで下記のような機能を実現することが出来ます。

インターロック

サーバー室の前室等で、前室内にいる人間を確定し共連れを防止するため、入室後、入り口側出口側の両方の扉が施錠された状態にならないと、出口側の解錠操作が出来なくなる機能。

アンチパスバック

正確な入退室の管理や記録取得のため、サーバー室等の入室・退室で本人認証を行わずに入退室すると、次回入退室を拒否される機能。

TPMOR（Two Person Minimum Occupancy Rule）

最初の入室者と最後の退室者は２人同時でないと入室・退室が出来ない機能。一人での在室を防止する為の機能。

エスコートルール

ビジターや臨時の入館者に対しての記録を残すため、（データセンター要員の）誰が（利用者、データセンター出入り業者等の外部者の）誰をエスコートしたかを記録する機能。

グローバルアンチパスバック

一つのセキュリティ区画だけではなく、複数のセキュリティ区画を跨ぐ場合の制限を与える機能。例えば、データセンターに入館しないと中のサーバー室等の区画に入室出来ない、あるいは、中のサーバー室で正常に退室処理をしないとデータセンターから退館出来なくなる機能があります。

時間指定 / ワンタイムパス

日付と時間を指定して本人認証後のアクセス権限を付与、無効にする機能。方式としては、システム側で一部の入室権限について日付時間を指定して有効にする、あるいは、あらかじめ利用可能な時間帯を設定したトークン(ワンタイムパス)を配付するといった方式があります。

緊急モード

緊急時に入室権限を変更する機能。緊急時には全ての人に権限を付与するパニックオープンの考え方と、逆に全ての人の権限を停止するパニッククローズの二つの考え方があります。

５.４.３ 本人認証

本人認証システムの目的は、入退管理システムの骨格をなすだれが（WHO）、いつ（WHEN）、どこに（WHERE）に入退室できるか？の“誰”を識別し認証することにあります。本人認証では、主張された身元（アクセス権限者であるかどうか）の検証を行いますが、この検証をおこなうためには被認証者の確認情報が必要となります。本人認証システムで用いられる被認証者確認情報は、一般に以下の三つがあります。

1. 記憶を用いた本人認証　　（暗証番号による認証など）
2. 所持品を用いた本人認証　　（カードによる認証など）
3. 特性を用いた本人認証　　（指紋認証など）

これらの被認証者情報を複数組み合わせた本人認証は、２要素認証、または、多要素認証と呼ばれ、技術的な観点から、一般的に本人認証に関する高い強度がある(≒他者になりすましされにくい)と認識されています。以下の節ではこれらの本人認証について紹介します。

（1）記憶を用いた本人認証（暗証番号による認証など）

被認証者の記憶による本人認証では、確認情報として、被認証者のみが記憶している情報を使い本人認証を行ないます。一般によく用いられている記憶情報の例としては、暗証番号を用いた本人認証がこれに当たります。暗証番号を被認証者確認情報として用いる場合、本人認証システムの設計では、暗証番号は身元を主張する被認証者のみが知っていることが前提になっていることを留意する必要があります。また、被認証者の記憶による本人認証では、暗証番号等の漏えいを本人が気付かず、被害などにあって初めて気が付く、場合によっては、気が付かないまま不正に利用されるといったことも考えられます。

（2）所持品を用いた本人認証（カードによる認証など）

「所持品による本人認証」では、被認証者確認情報として被認証者が所持する媒体を利用します。この媒体の例として IC カードなどが挙げられますが、広い意味では、家の鍵、通帳とハンコ、クレジットカード、パスポート、運転免許書なども「所持による本人認証」の道具と考えることもできます。

「所持品による本人認証」においては重要なポイントがふたつあります。ひとつは、「所持品による本人認証」に利用する所持物が、複製（偽造）されにくいこと、もうひとつは所持物の発行、失効、再発行のプロセスが確立されていることです。後者については特に盗難、紛失に対応した失効プロセスが重要です。一例として、24 時間体制の受付窓口の整備等は「所持品による本人認証」にとっては重要な意味を持つと言えます。

「所持品による本人認証」の例として、磁気ストライプカードを用いた本人認証があります。磁気ストライプカードには、低コストで導入が容易であるというメリットがありますが、磁気記録情報を不正に読み出して複製を容易に作成できてしまう課題があり、より複製困難な IC カードの登場・低価格化もあり、現在ではあまり用いられなくなっています。

IC カードを用いた「所持品による本人認証」では特に、暗号技術を用いた IC カードを暗号技術的トークン（Cryptographic Token）と呼ぶことがあります。こうした暗号技術を用いる本人認証は、ネットワーク上での通信を前提にして設計されているため、遠隔での認証が可能になるといった特徴があります。暗号技術的トークンでは、IC チップに暗号で使用される「鍵」が格納され、その「鍵」を使って IC トークン内部において演算をすることで、トークン、ないし、利用者の本人認証を行ないます。このようなトークンでは、「複製（偽造）」の脅威に対抗するため本人認証に利用する「鍵」を保護する仕組みが盛り込まれています。

（3）特性を用いた本人認証（指紋認証など）

特性認証は、利用者確認情報として、利用者の特性に基づくデータ（主に生体情報が用いられる）により利用者を本人認証する方法です。代表的なものとして、利用者の特性としての指紋、音声、虹彩、顔の形などを識別することにより本人認証をおこなうものがあります。表 12 に主な特性認証の種別、用いる生体情報、特徴を示します。

生体認証では、暗証番号などの記憶に基づく本人認証における「忘れる」、「他者に知られる」といった問題や、カードなどの所持に基づく本人認証における「紛失」、「盗難」、「置き忘れ」の問題を回避できるとされています。一方で、生体情報はアナログな性質を持つため、他者を利用者と誤認する危険性を排除できない、利用者であるのに利用者でないと認識してしまうといった問題もはらんでいます。

表 12　主要な生体認証の種類とその特徴

生体情報	特徴
静脈	手、指等の血管パターンを特徴をコード化して本人認証する。指紋を用いた場合に比べて偽装が困難なため、データセンターにおいて幅広く普及している。 血圧や体温などの影響を受けやすい点が課題となる。
指紋	指紋隆線の特徴点等を用いた本人認証、比較的低コストの入力装置が多い。指紋を転写して偽造できる脆弱性が指摘されている他、不鮮明指紋の場合対応できない場合もある。
虹彩	虹彩の模様を特徴コード化して本人認証する方式。認証精度は最も高い部類であるが、操作性やコストが課題となる。
顔	顔部品の特徴点、部品配置、輪郭、立体形状等を用いて本人認証する方式である。生体情報に一般的なカメラを用いることができるため入力が簡便な一方で、光条件等の耐環境性が課題となる。

５.４.４ その他の機能

その他にアクセスコントロールシステムに付帯する機能として、以下のような機能があります。これらの項目の多くは一般的な物であり、近年では他のシステムを複合化させることにより、より高度な機能を、利用者の負担を少なく、かつ安価に実現できるよう着実に発展を続けています。

自動バックアップ・リストア

通常の運用では有りませんが、システム設定内容、データベース、履歴を自動でバックアップする機能も非常に重要です。障害発生時においてもデータベースを簡単にリストアできる事で、素早い復旧・証跡の確保が可能になります。

外部連携

データのインポート機能、エクスポート機能、様々なソフトウェアインターフェースによるデータベース更新機能。大企業の人事異動時等にデータ更新を素早く簡単におこなうことができます。

レポート作成

入退室記録を多彩なフィルタ、問い合わせの組み合わせによって抽出し、的確なレポートを素早く作成する機能（システムに用意されるテンプレートに則ったレポートだけでなく、データセンターの監査対応等のケースにおいては、外部からデータベースに接続してカスタムレポートを作成する必要がある場合もある）。入退管理システムにおいて最も重要なのがこのレポート機能とも言えます。

5.5 サーバーラックシステム

サーバーラックは「最後の境界」であり、表面的には大きな変化は見られないものの、その実は構造的にも性能的にも弛まぬ進化が見られます。また、年々データセンターにおけるセキュリティのニーズがレベルアップして来ており、より一層この最後の境界を進化させるには、物理的な対策だけでは限界が見えてきているのも事実です。この章では、サーバーラックへの要求の歴史的な変化を踏まえつつ、これらニーズを高度なセキュリティレベルまで引き上げるひとつの手法として、システム化との連動で両立させる事案を解説していきます。

5.5.1 サーバーラックの機能向上とセキュリティの変遷

2011 年 3 月の東日本大震災以降、BCP の観点から、社内の基幹システムをデータセンターに再構築する利用者が増加し、それに呼応するように 2012 年ぐらいからデータセンターの建設ラッシュが本格化しました。その際、今までには余り無かった大規模センターを計画されたため、データセンターの運用に「システム化」というテーマを取り上げ、急増するお客様や各種作業の対応に、効率よく対処していくスキームの検討が進められることになりました。その手始めが、最後の境界となっていたサーバーラック扉の開閉管理の自動化です。

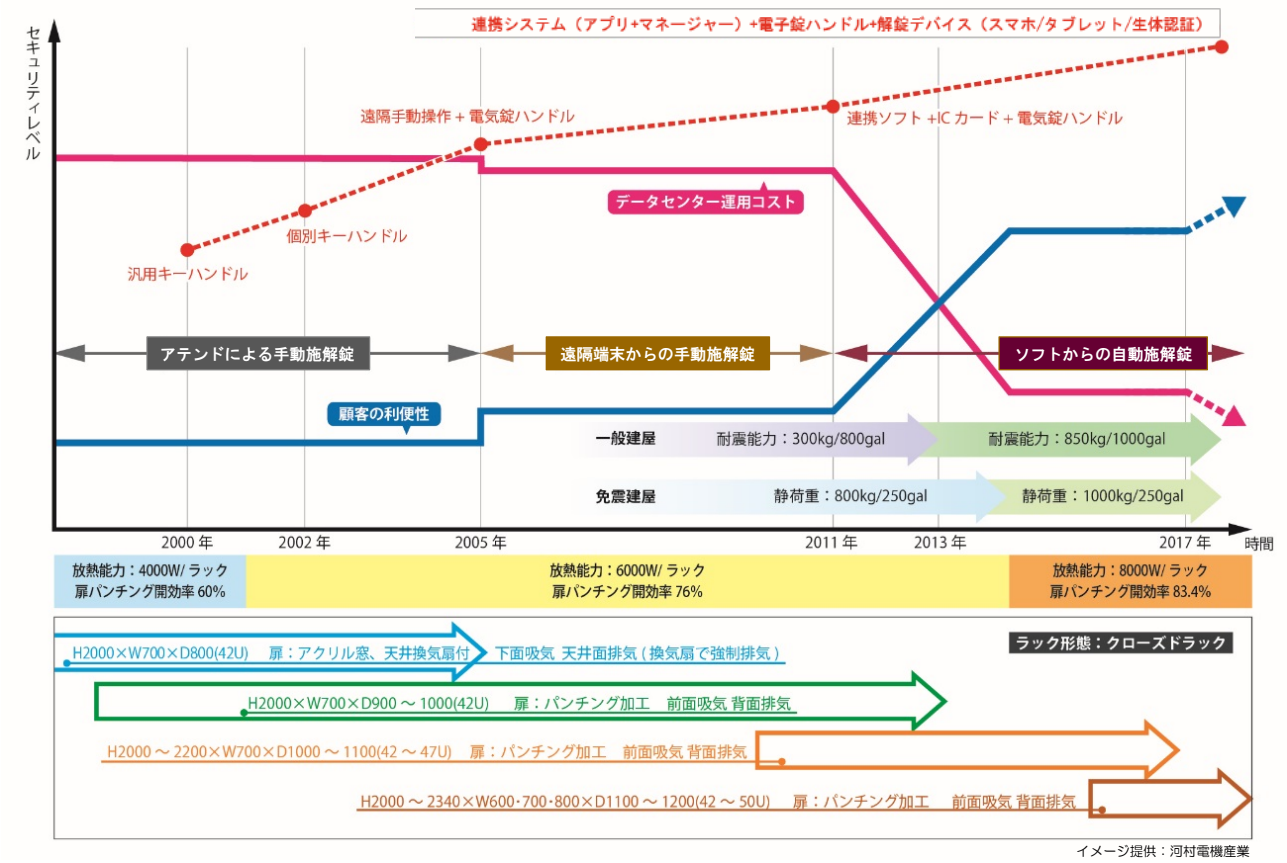


図 30　サーバーラックの構造と性能の変遷

それまでのデータセンターで利用記録として用いていたのは、入館する際に発行する IC カードのタイムスタンプのデータで、そのログを流用してお客様の作業時間帯の記録として代用していました。ところが、新設の大規模センターでは、入館時におこなうセキュリティチェック項目が増え、

入りロからの移動距離が延びたことで、人によるアテンド等の対応が難しくなり、その部分の作業内容を見直す必然性が出てきました。また、セキュリティだけでなく運用管理の側面からもセンター内での実際の作業時間帯を克明に知りたいというニーズが高まったことから、サーバーラック扉のシステム化が進んでいきました。具体的には、サーバーラック扉を開閉するハンドルに電気錠を装着して、サーバーラック扉の開錠時間及び施錠時間を装置側やソフト側で自動的に収集するといった仕組みが用いられています。このようなシステムを用いることにより、来訪されたお客様の入館時刻及び退館時刻と、実際に作業した時間帯が明確に記録に残すことが可能になりました。また、ユーザービリティの面においてはサーバーラック扉を解錠するタイミングについても、電話して遠隔からオペレータが解錠操作する仕組みよりも、入館の際に手渡される IC カードを利用してお客様自身が解錠する方法が好まれるようになり、その IC カードにサーバーラック扉を解錠する権限を付与する仕組みが普及してきました。

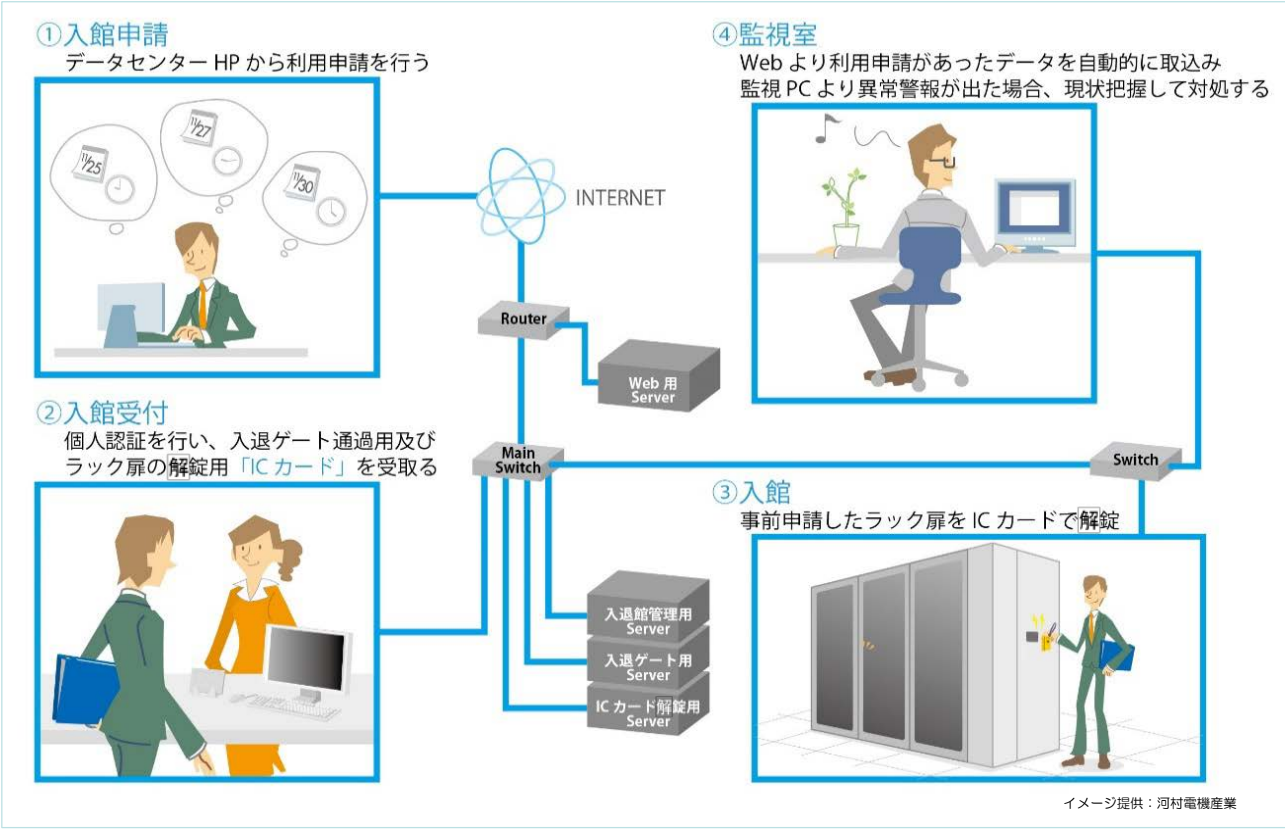


図 31　IC カードを利用したシステム化の事例

5.5.2　サーバーラックにおけるシステム自動化

データセンターにおける運用業務はお客様のアテンド、サーバーラック内のサーバーメンテナンス、サーバーラック状態の監視といった数多くの業務があります。

データセンターの入館や退館、サーバールームへの入室などは、既に様々な認証方法を用いたシステムの自動化が構築されていますが、最後の境界としてのサーバーラック扉の解錠は、物理キーに頼っている事業者がまだ大部分を占めています。

近年では、高いセキュリティを持ったサーバーラックの自動化システムを構築して運用しているデータセンターが増えて来ていて、今後もこの分野での技術革新が続くと思われます。この章ではサーバーラックの自動化システムのメリットおよび今後の展望について解説していきます。

お客様へのアテンド業務では、データセンターへの入館処理、サーバーラック扉の解錠と施錠、作業後の退館処理といった業務があります。それを属人化された状態ではなく、システムとして運用していくことで、セキュリティの向上や煩雑な作業量の低減で、大きなメリットがあります。ここでは IC カードを利用し、入退館ゲートやサーバーラック扉を 1 枚の IC カードで解錠できるシステムを採用された事例を紹介します。

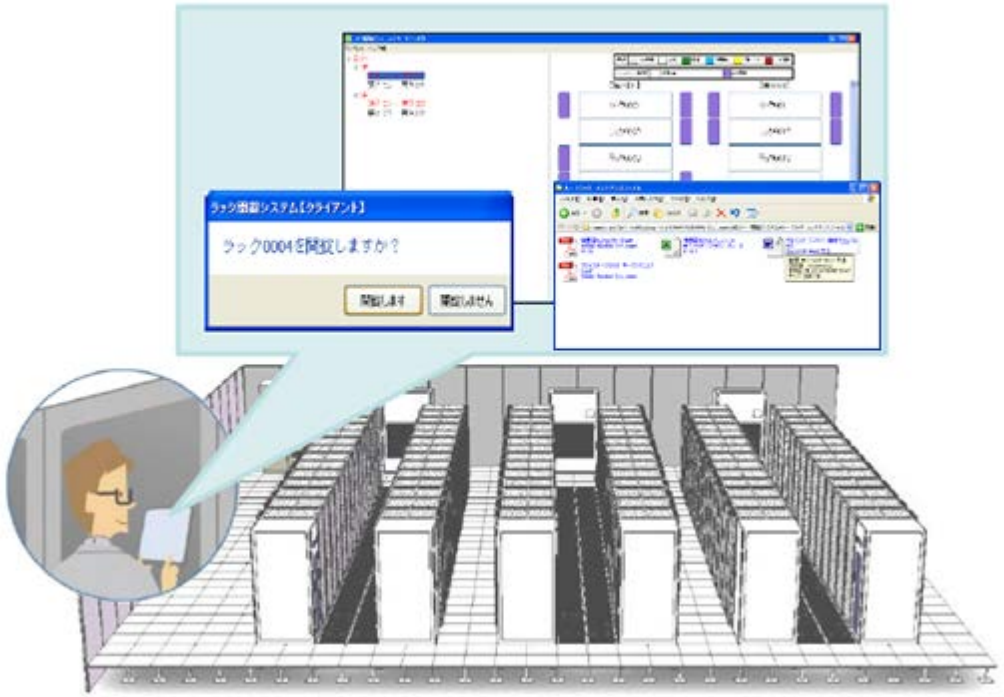
サーバーラックのセキュリティでは、入館手続きを完了しなければサーバーラックを解錠できない、退館処理をしてしまうと持っていたサーバーラックの解錠権限が消失して再利用ができなくなる、 退館時にサーバーラック扉が施錠されているかを遠隔から確認できる、といった機能が求められます。また作業量の低減という観点からは、システム化することで入退館した時間やサーバーラックを解錠・施錠した時間がシステム上のログとして記録されることで、利用者のアクセス履歴として報告書の作成、専用ソフトウェアからリアルタイムでの利用状況の把握が可能になります。これにより、実施する作業の優先順位が判り易くなり、効率良く対応できる体制が整えられます。

イメージ提供：河村電機産業

図 32　IC カードによるサーバーラックのシステム自動化の画面例

また、サーバーメンテナンス業務においては、利用者との契約に応じて、作業スケジュールの管理、実メンテナンス作業時の作業記録の保存が可能になります。つまり、ラック扉の解錠記録とともに、作業内容・結果の記録を取得が可能になります。

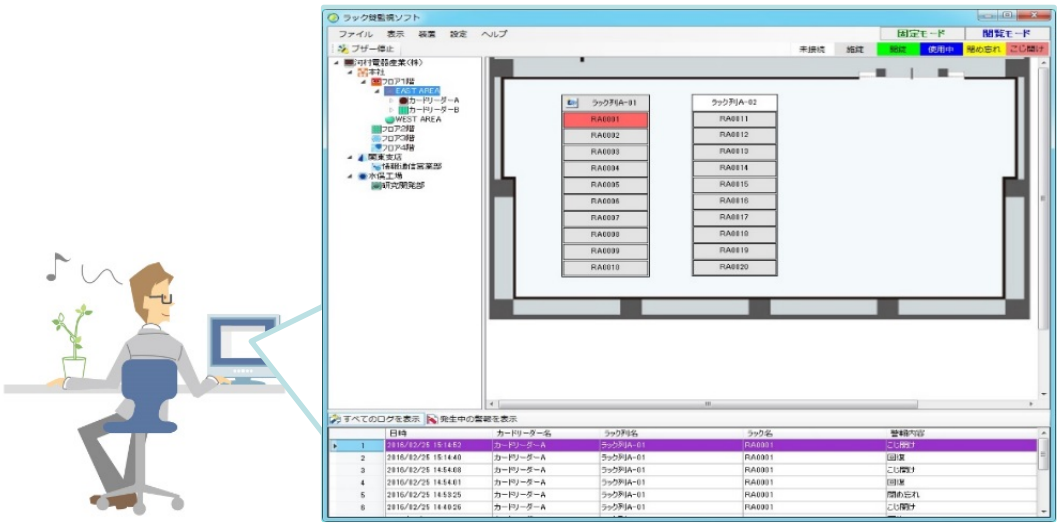
こういった作業の際には、サーバーラック列架の並びに沿って、順に横移動して行く事になりますが IC カードだけの運用では、いちいちカードリーダーに IC カードを当てに行く作業が発生するため、作業の効率化は望めません。そこでこのメンテナンス業務においては、IC カードで解錠するだけではなく、タブレット端末を用いて、サーバーラック解錠とメンテナンス作業を同時にこなす事で、作業性の向上が図れるようなシステムを利用している事例もあり、従来の紙媒体での記録と比べて、劇的な作業効率の改善を果たしています。



イメージ提供：河村電機産業

図 33　タブレット端末を使用したメンテナンス管理画面の例

サーバーラックのラック扉の状態監視はデータセンターにおける重要な業務です。ラック扉がこじ開けや閉め忘れ状態になっていれば即座に対応しなければなりませんし、緊急時に遠隔でサーバーラックを解錠させるような場合もあります。そこでデータセンターのサーバーラック監視に特化した監視ソフトウェアも登場しています。そのような監視ソフトウェアではデータセンターではサーバーラックを列毎に配置しているため、監視画面を実際のサーバーラック列に合わせたレイアウトにできるようにしていて、直感的な視界での監視ができるように工夫されています。



イメージ提供：河村電機産業

図 34　サーバーラックの状態監視画面の例

このような高度なサーバーラックシステムは新設のデータセンターに導入されている事例が殆どです。しかし、近年では 2000 年代に建設された既存のデータセンターを、改修する事業者も増

えており、その改修のタイミングに合わせて、ここまで紹介したようなサーバーラックシステムを低コストで導入する事例も増えています。そういった場合、これまでは一般的にサーバーラックシステムを導入するには、電気錠を導入済みのサーバーラックに対してのシステムの導入が前提となっていましたが、最近では使用されている物理錠仕様のサーバーラックに、後付けの電気錠を加工して取り付けることにより、低コストでサーバーラックシステムを実現している事例も登場しています。

図 35　既設サーバーラック扉の電気錠化の事例

5.5.3　サーバーラックシステムの今後

現在データセンターの業務を支援するシステムは「アテンド業務」「サーバーラック内のメンテナンス業務」「サーバーラックの状態監視」が別々のシステムで管理されていることが多いです。これはそれぞれの業務で担当者、要求される作業内容が異なり、また、各システムで要求されているデータの中身が違うためです。しかし上記の三つの業務を、統合的に運用することは運用コストの最適化の面では大きなメリットになると考えられます。一方で、このような重要なデータを単一のシステムで管理することは業務の単一障害点ともなりうるため、システムのデータベースを多重化するなど、信頼性を上げるようなシステム構築が求められています。

また、IC カードを利用したサーバーラックシステムに対して、さらに利便性を上げ、セキュリティを強化するために、入退管理システムで使われているような生体認証（指紋、虹彩、顔、静脈）を利用したシステムに移行していくという将来も予想されます。

一方で、データセンターに置かれているサーバーラックは、１区画で数十～百ラックという単位であり、サーバーラック一つ一つに生体認証装置を設置させるのは非現実的となってしまいます。そこで、スマートフォンなどを利用したラック解錠のシステム化が検討されています。例えば、業務や館内での連絡用に利用されるスマートフォンに搭載されている指紋や顔による認証機能を使いサーバーラック扉の解錠等の機能が提供されていく可能性が考えられます。

5.6 ビルディングオートメーションシステム

5.6.1 ビルディングオートメーションシステムの機能

ビルディングオートメーション(BA)システムは中央監視システムとも呼ばれ、以下のような建築設備の監視・計測および操作・制御を行います。

- 施設内の空調・衛生・電気・照明設備、防災設備、セキュリティ設備など、建築設備の一元的な状態監視、警報監視、運転管理（スケジュール）
- 設備の自動制御
- 設備間の連携制御（火災連動やセキュリティ連動など）
- 室内環境・エネルギー使用量・運転データの計測・記録など

ビルディングオートメーションシステムの一般的な機能一覧を示します。

表 13: ビルディングオートメーションシステムの一般的な機能

機能	項目		機能概要
監視	発停・設定操作		機器の運転/停止、温度設定、モード切替
	警報監視		故障機器シンボルの点滅、ブザー鳴動
	状態監視		機器の運転状態(ON/OFF)の監視
	（アナログ）計測値		温度センサ等計測値の監視
	積算計測値		電力量・熱量等メータ積算値の監視
	負荷リスト		ポイント状態/現在値等のリスト表示と、表示機器の一括発停・設定
	警報リスト		現在発生中の警報をリスト表示する
	計測値上下限監視		事前に設定した上下限範囲から外れたら警報発報
	運転時間		機器の運転時間、投入回数を記録
	連続運転時間監視		指定機器の連続運転時間を監視
	警報移報		警報発生時に接点信号やメールにより外部へ出力
	システム死活監視		各サブシステムなど関連システムの動作確認を定期的に行う
制御	共通	カレンダ管理	平日、休日、祝祭日、季節開始日、特殊日等の設定
		スケジュール制御	日や季節の属性に応じた発停・設定運転パターン指定・機器のグルーピング設定と、それらに基づいた制御の実施
		連動制御（イベント制御）	機器の状態変化や警報発報を契機に、関連機器の起動・停止を実施
	空調	間欠運転制御	間欠的な空調機の起動/停止による省エネルギー運転の実施
	電気	停電時制御	停電発生時に各種監視・制御を抑止し復旧時に通常運用に戻す
		電力デマンド監視制御	電力デマンドの監視・制御（機器停止）
		力率改善制御	受電無効電力コンデンサの監視・制御により力率を改善する
	防災	火災処理	火災発生時に空調を停止し、各種監視・制御を抑止する。復旧時に通常運用に戻す
システム管理	メッセージ履歴		警報/操作設定等を記録し、検索により表示
	アカウント管理		監視ユーザの登録・管理
	認証		監視画面を開く・設備操作を行う際のユーザ認証
データ管理	トレンド表示		指定ポイント（複数）の値・状態を指定時間間隔でグラフ表示する
	データ出力		トレンドデータをCSV形式ファイルとして保存する
	帳票		日月年報の表示・蓄積・出力
	帳票印刷		日月年報の自動印字

各機能は基本機能とオプションに分類されます。建物の用途や規模、建築設備の種類や仕様、そして連携させて動作させるシステムの有無などによって、オプションを選択しカスタマイズを施して導入されます。

5.6.2 ビルディングオートメーションシステムを構成する要素

ビルディングオートメーションシステムの一般的な構成を図 36 に示します。

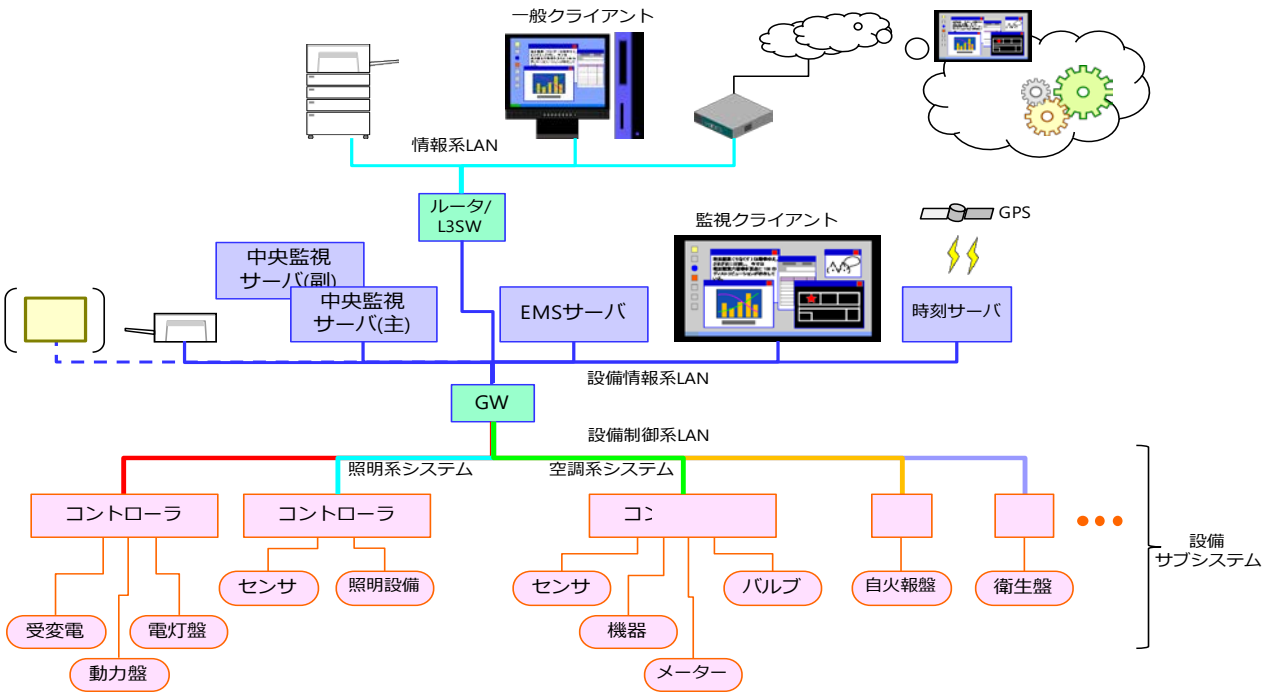


図 36　ビルディングオートメーションシステムの構成

施設内の環境を常時適切に管理するため、ビルディングオートメーションシステムにおいては可用性の担保が最重要視されます。そのため過去の中央監視システムは、設備分野毎に特化した専用の OS・通信規格を用い、外部システムと隔離させることで閉じた環境を形成していました。また、外部システムとの連携は、接点によるものか、手動での対応に限られていました。しかし近年、監視制御業務の一元化のため、各サブシステムの情報を統合的に扱い連携させることや、操作・表示インターフェースの共通化が求められるようになり、機器制御レイヤーについても国際規格・デファクト規格対応など相互運用性を重視したオープン化の流れが顕著になってきています。

さらに、経営情報開示の一環や、環境基準への適合を確認するためのエネルギー消費量の報告等の理由により、経営層など運用担当者以外による施設内の環境情報へのアクセスの容易化・日常化が求められるようにもなってきています。このような要求から、WEB 系システムをベースとし、PC から WEB ブラウザにより中央監視サーバーにアクセスするアプリケーションを用いることにより管理の自由度を高めたシステムへと変化してきています。

このようにこれまで独立したシステムとして、外部とは隔離された環境で動作させることが一般的であったビルディングオートメーションシステムも、何らかの形で外部情報システムとの接点を持つ場合を無視できなくなっています。

ビルディングオートメーションシステムの各コンポーネントについて説明します。

中央監視（BA）サーバー

各サブシステムと通信し、情報の収集と蓄積、提供（表示、検索）操作指令の受領と実行警報の管理等を行います。

マンマシンインターフェースとして、キーボード・マウスやディスプレイ等の入出力装置を備えるものがよく見られる仕様でしたが、先に述べた事情により、クライアントプログラムや WEB ブラウザによりサーバーにアクセスし監視操作をおこなう処理系も一般的になりつつあります。

ビルディングオートメーションシステムを守る機構として、トラブル時に無監視状態としないために、複数サーバーによる冗長化構成をとる場合があります。またシステムへアクセスするために多要素認証（例：IC カード+パスワード+生体認証）を採用する例も増加しつつあります。

EMS (Energy Management System)

エネルギーおよび環境管理のための情報を収集・監視し、帳票の形で提供したり、デマンド制御を実施したりするシステムです。ビルディングオートメーションサーバーと一体となっている場合や、図 36 のシステムのように別途システムとして実装される場合があります。

コントローラー（各サブシステム）

空調、照明、衛生などの各種建築設備の詳細な監視・制御や、アクチュエータに対する制御メッセージの信号化やセンサーからの監視信号の計算機可読化などをおこなう装置。UI や DB の役割を担う中央監視サーバーと連携し、抽象的なオペレーションを各装置へブレークダウンしていきます。また、アクセスコントロールや防災など、他の施設内システムからの警報を直接受けて、自らの管理下にある装置の制御をおこなう場合もあります。

タイムサーバー

ビルディングオートメーションシステムに接続される各システムに時刻情報を供給する装置です。インターネット上にある NTP サーバーを参照することでも同等の機能は得られますが、インターネットへの常時直接接続を避ける場合には、図にあるように GPS や JJY[52] を時刻ソースとした専用のタイムサーバーをシステムに組み込みます。

プリンター

帳票や画面ダンプ等を出力します。サーバーに直接接続されることは少なくなり、ネットワーク接続による複合機の利用に移行しています。

52： 何れも無線による時刻情報配信の仕組み。GPS(Global Positioning System)は測位のための技術として知られているが、測位のために必要な高精度の時刻情報も衛星から配信していて、これを時刻情報源として用いることができる。JJY は日本標準時を長波により送出する無線局の名称で(独)情報通信研究機構が運用している。

ゲートウェイ（GW）

各サブシステムを統括するコントローラーと、中央監視サーバー等各種サーバーとを接続します。接続にあたっては、

- 単なるスイッチングハブとして働く
- 各コントローラーは別々のネットワークに属するものとして分離させて接続する
- プロトコル変換をおこなう
- プロトコル変換に加えてある程度のデータ加工・蓄積をおこなう

など、システム構成に応じ機能が割り当てられるため、様々な実装があります。

L3 スイッチ (ルーター)

要求性能やセキュリティポリシーが異なる二つのネットワーク、設備情報系 LAN と情報系 LAN とを繋ぐネットワーク機器です。L3SW の場合、多数の機器を接続できます。また、アクセス制限を施すことも可能になっています。

ファイアウォール(ルーター)

遠隔監視やクラウド環境の利用などインターネットへの接続が必要な場合に利用するネットワーク機器です。アドレスやポートに応じた動作を設定するアクセス制限や、拠点間で安全な通信をおこなう VPN 接続などを行います。

UPS（無停電電源装置）

この他、停電時にビルディングオートメーションシステムを構成するサーバー機器やネットワーク機器に対して一定時間電力を供給し、シャットダウン制御をおこなうローカルの UPS が設置されます。ローカルの UPS がシャットダウン制御をおこなうインターフェースとしては、ビルディングオートメーションシステムではシリアル接続が一般的ですが、SNMP(Simple Network Management Protocol)を用いたネットワーク接続による実装もあります。

5.6.3 ビルディングオートメーションシステムの活用

ビルディングオートメーションシステムは、最も基本的な機能として設備機器を監視し、状態を管理者に伝え、操作のインターフェースとなり、制御をおこなう、という役割を果たしてきました。そこでは、警報イベント発生や操作に対する反応の遅延を小さくし、かつ応答を確実に返すことが求められてきました。

しかし近年は単なる建築設備の運転制御にとどまらず、室内環境とエネルギー性能使用状況を把握し最適化を図る、すなわち BEMS に相当するアプリケーションが重視される流れとなっています。このような機能のサポートのためには、ビルディングオートメーションシステムが管理する情報の蓄積・提供とともに、機能の公開による設備システム相互の連携等が求められるようになり、結果としてビルディングオートメーションシステムはその守備範囲を広げつつあります。

他システムとの連携…アプリケーションの視点から

ビルディングオートメーションシステムと施設内の他システムとの連携は以前から行われてきています。例えば火災時の設備停止や電気錠の緊急解放などのアプリケーションが、接点入力/出力でのハードウェアのワイヤリングにより古くから実装され、現在もその枠組みは活用されています。

一方で、BACnet や SOAP(Service Oriented Architecture Protocol)など通信プロトコルやデータ形式の共通化を進めることにより、中央監視サーバーと設備サブシステムとの連携を中心にソフトウェアによる柔軟な相互運用を実現している場合もよく見られるようになってきています。この枠組みを応用することにより、例えば会議室の予約管理システムと連動した照明・空調制御など、施設内の業務に関係するシステムとの連携も一般的に実装されるものとなっています。

ここから、データセンターを支えるシステムとの連携を考えてみます。

〇アクセスコントロールとの連携

複数のアクセスコントロールによる入場状況を一種の位置認証として捉えることにより、たとえば照明や監視カメラを必要な場所で集中的に作動させる制御を行い、利用可能な施設機能の制限や、消費エネルギーや記録リソース使用量の最適化をおこなうといった応用が考えられます。

〇DCIM との連携

DCIM の管理対象はデータセンター内の環境情報や情報通信機器、および周辺の機器・設備に関する情報であることから、施設の監視・制御をおこなうビルディングオートメーションシステムと共有することが有用な情報が多くあります。中央監視サーバーにおいて外部からシステム機能を利用可能な API を提供することにより、DCIM のダッシュボードから直接ビルディングオートメーションシステムの情報を参照することが可能になります。

〇マルチサイト可視化

BIM が提供する設計情報へのオーバーレイをおこなうことで、より詳細な環境シミュレーションが可能となると期待されています。例えばサーバーラック・機器の物理的配置と稼働状況をパラメータとして環境のリアルタイムシミュレーションと現状の環境モニタリングとの比較を実施することにより、現状の 3 次元的な視覚化やファンアレイ制御に結び付けるなどの応用がなされています。

また、複数サイトにおける構成や状態を BIM 情報により 3 次元視覚化することにより、設備保全管理（CMMS[53]）、資産管理（EAM[54]）、経営資源計画（ERP[55]）への適用をおこなうことも考えられます。

〇AI クラスタ(GPU クラスタ)対応：

AI をはじめとした解析用計算資源である GPU クラスタの利用者へのニーズに応え得る、機動的な物理機器の配置・運用という例題を考えてみます。仮想化環境を駆使して需要に応じた論理的かつ動的な情報通信機器のリソース配置をおこなう運用をベースに、空調制御を満足のいく範囲でシ

53： Computerized Maintenance Management System
54： Enterprise Asset Management
55： Enterprise Resource Planning

ンクロさせるというシナリオが描けます。できる限り既存のサービスインフラを用い、工事も少なくという要望に対し、ファンアレイ制御をきめ細かくおこなうなどの手段により対応をおこなうことが考えられます。

しかしGPUの発熱量は莫大であることから、配置計画やサーバーラック間での排気の衝突干渉への対策など、制御以前の計画段階での考慮と、空気の流れを知るためのより詳細なモニタリングが重要になります。以上が満たされて初めて制御に関する検討が意味を持つことになるため、未だ課題が多いアプリケーションであると言えます。

ビルディングオートメーションへのインテリジェンス導入と時系列データ

複雑化・多様化する建物内の機能・情報へ、

- 統合的な視点で監視制御
- 専門的視点で監視制御（エネルギー、経済、メンテナンス）

という複数の立場からアクセスしつつ、全体として良好に機能させたい、という要求を満たすために、これまで「手足」として働き、データを記憶してきたビルディングオートメーションシステムに、「判断する頭を据える」検討もなされ始めています。

少数パラメータを一つのアクションに結び付ける素直な条件判断であれば、既にハードウェアロジックやソフトウェアによるIF…THEN的条件分岐により実現されてきています。しかし電力、温熱環境、風量等の変化を取得可能なデータより予測し、配置運用を計画するなどのアプリケーションは、より高次の知的機能になります。これらを実現するためには、建物・設備の構成やモニタリングデータ、さらにはサーバーの利用状況をもとに、統計解析や機械学習をはじめとする手法により予測や計画をおこなう、知的な制御手法への展開が求められます。

ビルディングオートメーションシステムのアプリケーションとして、今起こっていることを特定時点(時間断面)での情報に基づいて判断しアクションを起こすだけでなく、将来の「予測」やそれに基づいた「計画」にも対応しようとする場合、時系列的なデータの扱いが分析的データ利用フェーズとして重要になります。このように施設を支えるシステム相互での時系列的データ利用に着目した体系として、データ交換のプロトコル(SOAP)を規定するとともにデータ提供・利用環境をモデル化したIEEE1888が挙げられます。

おわりに

データセンターセキュリティガイドブック 2017 年版を最後までお読みいただき、ありがとうございました。

6 年前、東日本大震災の影響も冷めやらぬ中で、様々乱立するセキュリティに関する基準をどのように俯瞰するか、という観点から議論が始まり、様々な紆余曲折を経てこのガイドブックのコンセプトが確立されました。そのコンセプトは、データセンターの利用者および事業者にデータセンターの適切なセキュリティの為の「考え方」と「共通言語」を示すことでした。

老子曰く、「人に授けるに魚を以ってするは、漁を以ってするに如かず」。未知の脅威に対応する適切なセキュリティを実現する為には、外部から与えられた基準をもって取り組むのではなく、その基準のつくられる背景を踏まえ、自身の頭と手を使って適切なセキュリティとは何かを考える必要があります。そしてその為にはステークホルダー間で考え方を共有する為の「共通言語」は不可欠なものです。

2013 年の本ドキュメントの第一版公開後、読者の方から「このガイドブックにおける「考え方」はミッションクリティカルな建物全般にも当てはめることが出来るものである」というご意見を頂戴しました。このご意見の通り、本ガイドブックでご紹介した基本的な考え方は物理、論理、建物、運用、システム等、幅広い分野のセキュリティにあてはめることが出来るものです。読者の皆様には本ガイドブックを知識として身につけるだけでなく、自身の頭と手を使って適切なセキュリティを考える際、手引きとしてご活用いただけますと幸いです。

読者の方々もそれぞれのお立場からセキュリティについて考えたこと、感じたことがあるかと思います。今後の本ガイドブックの充実の為にも、そういったご意見を是非日本データセンター協会 info@jdcc.or.jp までお寄せください。

最後に、本書は著者一覧に掲載させていただいた方々のみならず、様々な企業・団体・個人の方々からご助力をいただき作成させていただいております。皆様に心より感謝いたします。

日本データセンター協会
セキュリティワーキンググループ　リーダー

索引

付録.A セキュリティ区画-脅威-管理策-基準対応表

区画	セキュリティレベル	管理策の実施場所	脅威	管理策	基準における言及		
					ISMS(ISO/IEC 27002:2006)	FISC 安全対策基準(第8版)	JEITA ITR-1001D
敷地区画	レベル1	門扉(正門、裏門)	侵入(乗り越え)	**画像監視システム(Oルクス対応、動体検知)**			Ⅱ-2(監視)
				施錠可能かつ強固・十分な高さを持つ門扉	9.1.1(d) [建物・敷地の障壁設置]		Ⅱ-10[侵入防止]
				侵入検知システム(パッシブセンサー)		設備5-3[侵入防止(装置)]	Ⅱ-2(監視)
				防犯灯		設備5-4[照明]	Ⅱ-10[侵入防止]
				カメラ付きインターフォン			Ⅱ-2(監視)
				立哨警備	9.1.1(c) [建物・敷地の入場管理]	設備16-2[防犯]	
			侵入(破壊)	**画像監視システム(Oルクス対応、動体検知)**			Ⅱ-2(監視)
				施錠可能かつ強固・十分な高さを持つ門扉	9.1.1(d) [建物・敷地の障壁設置]		Ⅱ-10[侵入防止]
				侵入検知システム(パッシブセンサー)		設備5-3[侵入防止(装置)]	Ⅱ-2[監視]
				防犯灯		設備5-4[照明]	Ⅱ-10[侵入防止]
				カメラ付きインターフォン			Ⅱ-2[監視]
				立哨警備	9.1.1(c) [建物・敷地の入場管理]	設備16-2[防犯]	
			車両事故(接触[対物])	**画像監視システム(Oルクス対応、動体検知)**	9.1.1(d) [建物・敷地の障壁設置]		Ⅱ-10[侵入防止]
				施錠可能かつ強固・十分な高さを持つ門扉			Ⅱ-2[監視]
		駐車区画(敷地内)	不審車両	**画像監視システム(Oルクス対応、動体検知)**			Ⅱ-2[監視]
				搭乗者受付			Ⅱ-2[監視]
				車両受付ゲート(ナンバー識別、RFID、IC)	データセンター独自の価値基準に基づいた管理策		
				巡回警備	9.1.2(a) [入退記録]		Ⅱ-11[入退管理]
		外周フェンス	侵入(乗り越え)	**画像監視システム(Oルクス対応、動体検知)**	9.1.1(d) [建物・敷地の障壁設置]	設備5-2[侵入防止(塀・柵)]	Ⅱ-10[侵入防止]
				フェンス(忍び返し含む、強度のあるもの)		設備5-3[侵入防止(装置)]	Ⅱ-2[監視]
				防犯システム(パッシブセンサ)		設備5-3[侵入防止(装置)]	Ⅱ-2[監視]
				防犯システム(フェンスセンサー)		設備5-4[照明]	Ⅱ-10[侵入防止]
				防犯灯			Ⅱ-2[監視]
				巡回警備			Ⅱ-2[監視]
			侵入(破壊)	**画像監視システム(Oルクス対応、動体検知)**	9.1.1(d) [建物・敷地の障壁設置]	設備5-2[侵入防止(塀・柵)]	Ⅱ-10[侵入防止]
				フェンス(強度のあるもの)		設備5-3[侵入防止(装置)]	Ⅱ-2[監視]
				防犯システム(パッシブセンサ)		設備5-3[侵入防止(装置)]	Ⅱ-2[監視]
				防犯システム(フェンスセンサー)		設備5-4[照明]	Ⅱ-10[侵入防止]
				防犯灯			Ⅱ-2[監視]
				巡回警備			Ⅱ-2[監視]
エントランス区画	レベル2	正面来客口	不審者の侵入(訪問内容確認含む)	**来館者受付(事前入館申請含む)**	9.1.1(c) [建物・敷地の入場管理]	設備16-1[出入管理]	Ⅱ-11[入退管理]
				画像監視システム	9.1.1(f) [扉・窓の侵入検知]	設備16-2[防犯]	Ⅱ-2[監視]
				立哨警備	9.1.1(c) [建物・敷地の入場管理]	設備16-1[出入管理]	Ⅱ-11[入退管理]
				カメラ付きインターフォン	9.1.1(c) [建物・敷地の入場管理]	設備16-2[防犯]	
			危険物の持ち込み	画像監視システム(置き去り、持ち込み検知)		設備16-2[防犯]	Ⅱ-2[監視]
				立哨警備			Ⅱ-2[監視]
		機器搬入・搬出口	不審者侵入・危険物の持ち込み	画像監視システム	9.1.1(f) [扉・窓の侵入検知]	設備16-2[防犯]	Ⅱ-2[監視]
				立会い	9.1.2(a) [訪問者監督]		
			搬入物品の盗難	画像監視システム		設備16-2[防犯]	Ⅱ-2[監視]
				立会い	9.1.2(a) [訪問者監督]		
				強固かつ施錠可能なシャッター等の開口部設備	9.1.6(c)[荷受場の外部扉]	設備19[扉]	Ⅱ-10[侵入防止]
		従業員出入口	共連れ	入退管理システム(共連れ検知)		設備16-1[出入管理]	Ⅱ-11[入退管理]
				画像監視システム		設備16-1[出入管理]	Ⅱ-2[監視]、Ⅱ-11[入退管理]
				カメラ付きインターフォン		設備16-1[出入管理]	Ⅱ-11[入退管理]
				立哨警備		設備16-1[出入管理]	Ⅱ-2[監視]、Ⅱ-11[入退管理]
			不審者の侵入	入退管理システム		設備16-2[防犯]	Ⅱ-11[入退管理]
				画像監視システム		設備16-2[防犯]	Ⅱ-2[監視]
				カメラ付きインターフォン		設備16-2[防犯]	Ⅱ-11[入退管理]
				立哨警備		設備16-2[防犯]	Ⅱ-2[監視]、Ⅱ-11[入退管理]
		建屋窓・外壁	(破壊による)侵入	画像監視システム(Oルクス対応、動体検知)	9.1.1(f) [扉・窓の侵入検知]		Ⅱ-2[監視]
				防犯システム(ガラスセンサー)	9.1.1(f) [扉・窓の侵入検知]	設備15[開口部防犯]	Ⅱ-2[監視]
				巡回警備			Ⅱ-2[監視]
検査区画	レベル3	手荷物検査室	不正侵入	**フラッパーゲート**	9.1.2(b) [アクセス管理・記録]		Ⅱ-11[入退管理]
				画像監視システム	9.1.1(f) [扉・窓の侵入検知]		Ⅱ-2[監視]
				立哨警備			Ⅱ-2[監視]
			不審物持ち込み	**持込み検査(金属探知、X線透視)**	(9.2.7(a) [装置・情報の持出禁止])	設備16-2[防犯]	Ⅱ-2[監視]
				立哨警備			Ⅱ-2[監視]
共用区画	レベル4	廊下・EV・EVホール	不正侵入	画像監視システム	9.1.2(b) [アクセス管理]		Ⅱ-11[入退管理]
				入退管理システム(ICカード・生体認証)	9.1.2(b) [アクセス記録]		Ⅱ-2[監視]
			共連れ	**ローターゲート**	9.1.2(b) [アクセス管理]		Ⅱ-11[入退管理]
				入退管理システム(共連れ検知)	9.1.2(b) [アクセス管理]		Ⅱ-11[入退管理]
				画像監視システム	9.1.2(b) [アクセス記録]		Ⅱ-2[監視]
				立哨警備			Ⅱ-2[監視]
専用区画	レベル5a	オフィス	不正侵入	画像監視システム	9.1.2(b) [アクセス管理]		Ⅱ-11[入退管理]
				入退管理システム(ICカード・生体認証)	9.1.2(b) [アクセス記録]		Ⅱ-2[監視]
	レベル5b	サーバー室(前室含む)	不正侵入	**画像監視システム**	9.1.2(b) [アクセス管理]	設備45-1[出入管理]	Ⅳ-14[入退管理]
				入退管理システム(ICカード・生体認証)	9.1.2(b) [アクセス記録]	設備45-1[出入管理],2[防犯]	(Ⅱ-2[監視])
				フリーアクセス床の特殊ボルトによる固定	データセンター独自の価値基準に基づいた管理策		
			不正滞留	**画像監視システム**	9.2.1(a)[不必要な接触の最小化]	(運用61[作業管理])	
				入退管理システム(在室カウント)	9.2.1(a)[不必要な接触の最小化]	(運用61[作業管理])	(Ⅱ-2[監視])
			共連れ	**画像監視システム**	9.1.2(b) [アクセス管理]	設備27-1[入室者チェック]	Ⅳ-14[入退管理]
				入退管理システム(前室での共連れ検知)	9.1.2(b) [アクセス記録]	設備45-1[出入管理]	(Ⅱ-2[監視])
			危険物持ち込み	**画像監視システム**	9.2.1(d)[潜在的な脅威の抑止]		Ⅲ-22[電磁ノイズ源の持込禁止]
				水、火気、電磁ノイズ源等の持ち込み禁止ルール	9.2.1(d)[潜在的な脅威の抑止]		Ⅲ-22[電磁ノイズ源の持込禁止]
			火災	火災予兆検知	9.2.1(d)[潜在的な脅威の抑止]	設備37[火災報知]	Ⅲ-17[火災報知]
			情報の不正持ち出し	**画像監視システム**	9.2.7(a) [装置・情報の持出禁止]		
				記録媒体の持ち込み禁止ルール	9.2.7(a) [装置・情報の持出禁止]		
	レベル5c	設備室	不正操作(破壊)	画像監視システム	9.1.1(f) [扉・窓の侵入検知]	設備55[侵入防止(施錠)]	Ⅳ-14,Ⅴ-10[施錠]
				入退管理システム(ICカード・生体認証)	データセンター独自の価値基準に基づいた管理策		
			火災	火災検知システム	9.2.1(d)[潜在的な脅威の抑止]	設備57[火災報知]	Ⅳ-6[火災報知]
重要区画	レベル6a	ラック	不正操作(破壊・改ざん)	**画像監視システム**	9.1.2(b) [アクセス管理]	(運用61[作業管理])	Ⅱ-17[ラック]
				ラック扉管理(ICカード・生体認証)	9.1.2(b) [アクセス管理]	(運用61[作業管理])	Ⅱ-17[ラック]
				ラック	9.1.2(b) [アクセス記録]	(運用61[作業管理])	(Ⅱ-2[監視])
	レベル6b	設備室(NW、電気、空調室監視室等)	不正操作(破壊)	画像監視システム	9.1.1(f) [扉・窓の侵入検知]	設備55[侵入防止(施錠)]	Ⅳ-14,Ⅴ-10[施錠]
				入退管理システム(ICカード・生体認証)	データセンター独自の価値基準に基づいた管理策		
			火災	火災検知システム	9.2.1(d)[潜在的な脅威の抑止]	設備57[火災報知]	Ⅳ-6[火災報知]

付録.B データセンターセキュリティ関連ドキュメント一覧

No.	名前	カテゴリ	発行元	発行	参照ページ	参考URL
	基準・ガイドライン					
1	ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements	マネジメントシステム	International Organization for Standardization	2013.9		https://www.iso.org/standard/54534.html
2	JIS Q 27001:2014 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム – 要求事	マネジメントシステム	日本工業標準調査会	2014.3		http://www.jisc.go.jp/index.html
3	ISO/IEC 27002:2013 Information technology –Security techniques – Code of practice for information security management	マネジメントシステム	International Organization for Standardization	2013.9		https://www.iso.org/standard/54533.html
4	JIS Q 27002:2014 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステムの実践の	マネジメントシステム	日本工業標準調査会	2014.3		http://www.jisc.go.jp/index.html
5	ISO/IEC 27017:2015– Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services	マネジメントシステム	International Organization for Standardization	2015.12		https://www.iso.org/standard/43757.html
6	JIS Q 27017:JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範	マネジメントシステム	日本工業標準調査会	2016.12		http://www.jisc.go.jp/index.html
7	ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項(JIP-ISMS517-1.0)	マネジメントシステム	日本情報経済社会推進協会(JIPDEC)	2016.8		https://isms.jp/isms-cls/isms-cls-publish.html
8	ISO/IEC 20000-1:2011 Information technology – Service management –Part 1: Specification	マネジメントシステム	International Organization for Standardization	2011.2		https://www.iso.org/standard/43757.html
9	JIS Q 20000-:2013 情報技術 – サービスマネジメント – □第1部:仕様	マネジメントシステム	日本工業標準調査会	2013.11		http://www.jisc.go.jp/index.html
10	ISO/IEC 20000-2:2012 Information technology – Service management –Part 2: Code of practi	マネジメントシステム	International Organization for Standardization	2012.2		https://www.iso.org/standard/51987.html
11	JIS Q 20000-2:2013 情報技術 – サービスマネジメント – □第2部:実践のための規範	マネジメントシステム	日本工業標準調査会	2013.11		http://www.jisc.go.jp/index.html
12	ISO 22301:2012 Societal security – Business continuity management systems – Requirements	マネジメントシステム	International Organization for Standardization	2012.5		https://www.iso.org/standard/50038.html
13	JIS Q 22301:2013 社会セキュリティ–事業継続マネジメントシステム–要求事項	マネジメントシステム	日本工業標準調査会	2013.10		http://www.jisc.go.jp/index.html
14	ISO 9001:2015 Quality management systems -- Requirements	マネジメントシステム	International Organization for Standardization	2015.9		https://www.iso.org/standard/62085.html
15	JIS Q 9001:2015 品質管理システム – 要求事項	マネジメントシステム	日本工業標準調査会	2008.12		http://www.jisc.go.jp/index.html
16	JIS Q 15001:2006 個人情報保護マネジメントシステム – 要求事項	マネジメントシステム	日本工業標準調査会	2006.5		http://www.jisc.go.jp/index.html
17	顧客から預かる情報の取り扱いについて(解説)	マネジメントシステム	日本情報経済社会推進協会(JIPDEC)	2014.1		http://privacymark.jp/reference/pdf/guideline_kaisetsu_140120.pdf
18	ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors	マネジメントシステム	International Organization for Standardization	2014.8		https://www.iso.org/standard/61498.html
19	IT-1002A 情報システムの設備環境基準	データセンター	電子情報技術産業協会(JEITA)	2011.4		http://it.jeita.or.jp/document/setsubi/ITR1001-1002/1002.htm
20	ITR-1001D 情報システムの設備ガイド	データセンター	電子情報技術産業協会(JEITA)	2015.5		http://www.jeita.or.jp/japanese/standard/book/ITR-1001D_J
21	JQA情報システム及び関連設備の運用基準 第3版	データセンター	日本品質保証機構(JQA)	2011.4		http://www.jqa.jp/service_list/infosecu/service/info/data.html
22	ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers	データセンター	Telecommunications Industry Association	2012.8		http://tiaonline.org/node/773
23	ANSI/TIA-942-A-1 Telecommunications Infrastructure Standard for Data Centers : Addendum 1 – Cabling Guidelines for Data Center Fabrics	データセンター	Telecommunications Industry Association	2013.3		http://tiaonline.org/node/773
24	ANSI/BICSI 002-2014, Data Center Design and Implementation Best Practices	データセンター	Building Industry Consulting Service International	2014		https://www.bicsi.org/book_details.aspx?Book=BICSI-002-CM-14-v5
25	G1-031Phisical Protection of Computer Servers	データセンター	Royal Canadian Mounted Police	2008.3		http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-031-eng.htm
26	GO-ITS 25.18 Physical Security Requirements for Data Centers v.1.1	データセンター	Government of Ontario	2012.11		https://dr6j45jk9xcmk.cloudfront.net/documents/1863/go-its-25-18-data-centre-physical-security.pdf
27	Tier Standard: Topology	階層系	Uptime Institute	2012.1		http://www.uptimeinstitute.com/publications
28	Tier Standard: Operational Sustainability	階層系	Uptime Institute	2012.1		http://www.uptimeinstitute.com/publications
31	ASP・SaaSにおける情報セキュリティ対策ガイドライン	クラウド	総務省 情報通信政策局 情報セキュリティ対策室	2008.1		http://www.mhlw.go.jp/shingi/2008/07/dl/s0730-18l.pdf
32	クラウドサービス利用のための情報セキュリティマネジメントガイドライン(2014年版)	クラウド	経済産業省 商務情報政策局 情報セキュリティ政策室	2014.3		http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html
33	クラウドサービス提供における情報セキュリティ対策ガイドライン	クラウド	総務省 情報通信政策局 情報セキュリティ対策室	2014.4		http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html
34	クラウドサービスの安全・信頼性に関する情報開示指針	クラウド	総務省 情報流通行政局 情報流通振興課	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
35	ASP・SaaSの安全・信頼性に係る情報開示指針(第2版)	クラウド	総務省 情報流通行政局 情報流通振興課	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
36	ASP・SaaS(特定個人情報取扱いサービス)の安全・信頼性に係る情報開示指針	クラウド	総務省 情報流通行政局 情報流通振興課	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
37	ASP・SaaS(医療情報取扱いサービス)の安全・信頼性に係る情報開示指針	クラウド	総務省 情報流通行政局 情報流通振興課	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
38	IaaS・PaaSの安全・信頼性に係る情報開示指針(第2版)	クラウド	総務省 情報流通行政局 情報流通振興課	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
39	データセンターの安全・信頼性に係る情報開示指針(第3版)	データセンター	総務省 情報流通行政局	2017.3		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
40	クラウド情報セキュリティ管理基準(平成28年版)	クラウド	日本セキュリティ監査協会(JASA)	2016		http://jcispa.jasa.jp/cloud_security/criterion_of_control/
41	Security Guidance for Critical Areas of Focus in Cloud Computing v.3.0	クラウド	Cloud Security Alliance	2011.11		https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/
42	クラウドコンピューティングのためのセキュリティガイダンス v.3.0	クラウド	Cloud Security Alliance	2013.5		http://www.cloudsecurityalliance.jp/guidance.html
43	Cloud Controls Matrix v.3.0.1	クラウド	Cloud Security Alliance	2016.6		https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
44	医療情報システムの安全管理に関するガイドライン 第5版	医療	厚生労働省 医政局研究開発振興課 医療技術情報推進室	2017.5		http://www.mhlw.go.jp/stf/shingi/0000026088.html
45	医療情報を受託管理する情報処理事業者向けガイドライン 第2版	医療	経済産業省 商務情報政策局 情報経済課	2012.10		http://www.meti.go.jp/press/2012/10/20121015003/20121015003.html
46	ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第1.1版	医療	総務省 情報流通行政局 情報流通振興課	2010.12		http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_01000009.html
47	政府機関の情報セキュリティ対策のための統一基準群(平成28年度版)	政府	内閣サイバーセキュリティセンター(NISC)	2016.5		http://www.nisc.go.jp/active/general/kijun28.html
48	金融機関等コンピュータシステムの安全対策基準・解説書(第8版)	金融	金融情報システムセンター(FISC)	2011.3		http://www.fisc.or.jp/publication/disp_target_detail.php?pid=225
49	金融機関等コンピュータシステムの安全対策基準・解説書(第8版追補)	金融	金融情報システムセンター(FISC)	2013.3		https://www.fisc.or.jp/publication/disp_target_detail.php?pid=266
50	金融機関等コンピュータシステムの安全対策基準・解説書(第8版追補改訂)	金融	金融情報システムセンター(FISC)	2015.6		https://www.fisc.or.jp/publication/disp_target_detail.php?pid=316
51	PCI DSS(Payment Card Industry Data Security Standard)v.3.2	信販	Payment Card Industry Security Standards Council	2016.4		https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
52	LGWAN-ASPサービス接続／変更／解除申込書様式	自治体	地方公共団体情報システム機構(J-LIS)	--		https://www.j-lis.go.jp/lgwan/asp/application/cms_15763941.html
53	組織における内部不正防止ガイドライン(第4版)	その他	情報処理推進機構(IPA)	2017.1		http://www.ipa.go.jp/security/fy24/reports/insider/index.html
	ホワイトペーパー等					
a	データセンター利用ガイド	データセンター	ASP・SaaS・クラウドコンソーシアム(ASPIC)	2010.10		http://www.aspicjapan.org/business/datacenter/pdf/datacenter_vol1.pdf
b	データセンター事業者連携ガイド	データセンター	ASP・SaaS・クラウドコンソーシアム(ASPIC)	2012.12		http://www.aspicjapan.org/information/guideline/pdf/guide.pdf
c	クラウドセキュリティガイドライン活用ガイドブック	クラウド	経済産業省 商務情報政策局 情報セキュリティ政策室	2014.3		http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html
d	FIPS PUB31 "Guidelines for Automatic Data Processing Phisical Security and Risk Management" (データ処理における物理セキュリティ及びリスクマネジメント)	政府(海外)	National Bureau of Standards (現:National Institute of Standarts and Technology	1974.1		http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA406247
e	NIST SP800-30 rev.1 "Risk Management Guide for Information Technology Systems" (ITシステムの為のリスクマネジメントガイド)	政府(海外)	National Institute of Standarts and Technology (IPA訳)	2012.9		https://www.ipa.go.jp/security/publications/nist/
f	NIST SP800-53 rev.2 "Security and Privacy Controls and Assessment Procedures for Frderal Information Systems and Organizations (連邦政府情報システムにおける推奨セキュリティ/プライバシー管理策)"	政府(海外)	National Institute of Standarts and Technology (IPA訳)	2008.6		https://www.ipa.go.jp/security/publications/nist/
g	NIST SP800-53 rev.4 "Security and Privacy Controls and Assessment Procedures for Frderal Information Systems and Organizations"	政府(海外)	National Institute of Standarts and Technology	2010.5		http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
h	NIST SP800-116 "A Recommendation for the Use of PIV Credentials in Phisical Access Control Systems"	政府(海外)	National Institute of Standarts and Technology	2008.11		http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf
i	Cloud Computing: Benefits, risks and recommendations for information security (クラウドコンピューティング:情報セキュリティに関わる利点、リスクおよび推奨事項)	クラウド	European Network and Information Security Agency (IPA訳)	2001.11		http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
j	Cloud Computing: Information Assurance Framework (情報セキュリティ確保のためのフレームワーク)	クラウド	European Network and Information Security Agency (IPA訳)	2001.11		http://www.ipa.go.jp/security/publications/enisa/index.html
k	監査基準委員会報告第18号『委託業務にかかる統制リスクの評価』	調査報告書	日本公認会計士協会	2003.1		http://www.hp.jicpa.or.jp/specialized_field/pdf/00534-001629.pdf
l	Statement on Standards for Attestation Engagements (SSAE) No. 16 "Reporting on Controls at a Service Organization"	調査報告書	米公認会計士協会	2011.6		http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx
m	組織内部者の不正行為によるインシデント調査	調査報告書	独立行政法人 情報処理推進機構	2012.7		http://www.ipa.go.jp/security/fy23/reports/insider/index.html
n	Accredited Tier Designer Technical Paper Series: Engine-Generator Ratings	階層系	Uptime Institute	2010.6		http://www.uptimeinstitute.com/publications
o	Accredited Tier Designer Technical Paper Series: Makeup Water	階層系	Uptime Institute	2010.6		http://www.uptimeinstitute.com/publications
p	Accredited Tier Designer Technical Paper Series: Continuous Cooling	階層系	Uptime Institute	2010.6		http://www.uptimeinstitute.com/publications
q	Natural Disaster Risk Profiles for Data Centers	階層系	Uptime Institute	2010.6		http://www.uptimeinstitute.com/publications
	JDCCドキュメント類					
A	JDCC FS-001 データセンター ファシリティ スタンダード Ver.2.3		NPO 日本データセンター協会	2017.1		http://www.jdcc.or.jp/news/article.php?nid=c81e728d9d4c2f636f067f89cc14862c&sid=126
B	JDCC ES-001 PUE計測・計算方法に関するガイドライン Ver.2.7		NPO 日本データセンター協会	2015.5		http://www.jdcc.or.jp/news/article.php?nid=c81e728d9d4c2f636f067f89cc14862c&sid=111
C	データセンターネットワークリファレンスガイド 第2版		NPO 日本データセンター協会	2010.10		http://www.jdcc.or.jp/news/article.php?nid=c81e728d9d4c2f636f067f89cc14862c&sid=98

付録.C データセンターセキュリティ関連団体一覧

団体名	URL	登場頁	備考
特定非営利活動法人　ASP・SaaS・IoTクラウドコンソーシアム	www.aspicjapan.org		「データセンター情報開示制度」の運用等
特定非営利活動法人　日本セキュリティ監査協会	www.jasa.jp		「情報セキュリティ監査制度」の運用等
特定非営利活動法人　日本ネットワークセキュリティ協会	www.jnsa.org/		「情報セキュリティインシデントに関する調査報告書」の発行等
一般社団法人　JPCERTコーディネーションセンター	www.jpcert.or.jp		サイバーセキュリティに関する情報共有等をおこなう
一般社団法人　情報サービス産業協会	www.jisa.or.jp		情報サービス産業分野における業界団体
一般社団法人　日本クラウドセキュリティアライアンス	www.cloudsecurityalliance.jp		クラウドに関連する幅広いセキュリティに関する情報共有をおこな
一般財団法人　日本規格協会	www.isa.or.jp		各種JIS規格の原案作成・発行・出版等
一般財団法人　日本情報経済社会推進協会	www.jipdec.or.jp		ISMS適合性評価制度の運用等
一般社団法人　電子情報技術産業協会	www.jeita.or.jp		「IT-1002A 情報システムの設備環境基準」の発行等
公益財団法人　金融情報システムセンター	www.fisc.or.jp		「金融機関等コンピュータシステムの安全対策基準」の発行等
公益社団法人　防犯設備協会	www.ssaj.or.jp		防犯設備士・総合防犯設備士の認定等
BICSI(Building Industry Consulting Service International) 日本支部	www.bicsi-japan.org		情報配線の設計・施工にかかわる資格の認定等
個人情報保護委員会	www.ppc.go.jp		個人情報の保護と利活用を監督する行政委員会
内閣官房　サイバーセキュリティセンター	www.nisc.go.jp		国内のサイバーセキュリティ政策における中核組織
地方公共団体情報システム機構	www.j-lis.go.jp		地方公共団体に対して情報システムに関する支援をおこなう
経済産業省　商務情報政策局　情報政策課　情報セキュリティ政策室	www.meti.go.jp		経済産業省における情報セキュリティ政策を主管する
総務省　情報流通行政局　情報流通振興課　情報セキュリティ対策室	www.soumu.go.jp		総務省における情報セキュリティ政策を主管する
独立行政法人　情報処理推進機構	www.ipa.go.jp		各種調査報告、米国NISTの資料の邦訳等を公開

執筆者一覧

データセンターセキュリティガイドブック　2017 年版　改定メンバー

はじめに・第 1 章・おわりに

○松本　泰	セコム 株式会社
水戸　和	セコム 株式会社

第 2 章

○水戸　和	セコム 株式会社
安達　大樹	株式会社 IDC フロンティア
田中　雄作	Colt テクノロジーサービス 株式会社
山口　知	Colt テクノロジーサービス 株式会社

第 3 章

○奈良輪　康弘	株式会社 アット東京
村井　裕治	株式会社 アット東京
永田　友	キヤノン IT ソリューションズ 株式会社
鈴木　智久	日本電気 株式会社
小泉　充	株式会社 野村総合研究所
竹内　誠	富士ソフト 株式会社
野澤　俊二	富士ソフト 株式会社
高　元伸	ヤフー 株式会社

第 4 章

○高　元伸	ヤフー 株式会社
安達　大樹	株式会社 IDC フロンティア
玉井　睦	セコム 株式会社
水戸　和	セコム 株式会社

第 5 章

○星島　恵三	NTT ファシリティーズ 株式会社
児玉　憲志	河村電器産業 株式会社
多賀　優	清水建設 株式会社
廣瀬　啓一	清水建設 株式会社
金澤　学	能美防災　株式会社

レビュアー

染谷　博行	アズビル 株式会社
松原　利幸	大成建設 株式会社
綾野　孝義	NSSLC サービス　株式会社
根津　義雄	SCSK　株式会社
谷本　逸哉	株式会社コーアツ
山崎　訓由	新日鉄住金ソリューションズ 株式会社
大槻　英彰	株式会社 野村総合研究所
清水　健	株式会社 野村総合研究所
川崎　康弘	富士通 株式会社
斉藤　丈洋	三菱総研 DCS 株式会社
加藤　雅彦	NPO 日本セキュリティ監査協会　/ 長崎県立大学

データセンターセキュリティガイドブック　2015 年版　執筆・改定メンバー

（2013・2017 年版メンバー除く）

姉崎　淳	株式会社 アット東京
長野　真樹	株式会社 アット東京
長舟　利雄	株式会社 大林組
掛谷　美里	伊藤忠テクノソリューションズ 株式会社
三浦　耕太郎	伊藤忠テクノソリューションズ 株式会社
金　澤根	ソフトバンク 株式会社
後藤　武志	NEC ネッツエスアイ 株式会社
上野　天徳	一般財団法人 日本品質保証機構
清水　一郎	一般財団法人 日本品質保証機構
大湯　正啓	日比谷総合設備 株式会社

データセンターセキュリティガイドブック　2013 年版　執筆・改定メンバー

（2015・2017 年版メンバー除く）

宮地　英和	河村電器産業 株式会社
有本　一	シュナイダーエレクトリック 株式会社
鈴木　良信	シュナイダーエレクトリック 株式会社
トニー　クラークス	シュナイダーエレクトリック 株式会社
亀村　昭寛	住友電気工業 株式会社
田口　雄二	住友電気工業 株式会社
月足　新	住友電気工業 株式会社
今村　武英	住友電気工業 株式会社
森口　雅弘	住友電気工業 株式会社

藤川　春久	セコムトラストシステムズ 株式会社
毛利　信雄	セコムトラストシステムズ 株式会社
深田　航	セコムトラストシステムズ 株式会社
植田　聡	日本カバ 株式会社（現　ドルマカバジャパン株式会社）
西山　利明	日本カバ 株式会社（現　ドルマカバジャパン株式会社）
小川　三奈津	日本カバ 株式会社（現　ドルマカバジャパン株式会社）
鈴木　彰人	日本カバ 株式会社（現　ドルマカバジャパン株式会社）
宮山　直喜	一般財団法人 日本品質保証機構
吉方　敬	能美防災 株式会社
住谷　健	ビデオテクニカ 株式会社
池田　利弘	フューチャーファシリティーズ 株式会社
佐藤　隆明	NEC ネッツエスアイ 株式会社
土谷　尚	NEC ネッツエスアイ 株式会社

本ガイドブックのライセンスについて

データセンター セキュリティ ガイドブック

2017 年 10 月発行

特定非営利活動法人日本データセンター協会

Japan Data Center Council （略称：JDCC）

http://www.jdcc.or.jp

JDCC
日本データセンター協会
Japan Data Center Council