特集論文

データセンター向け セキュリティソリューション

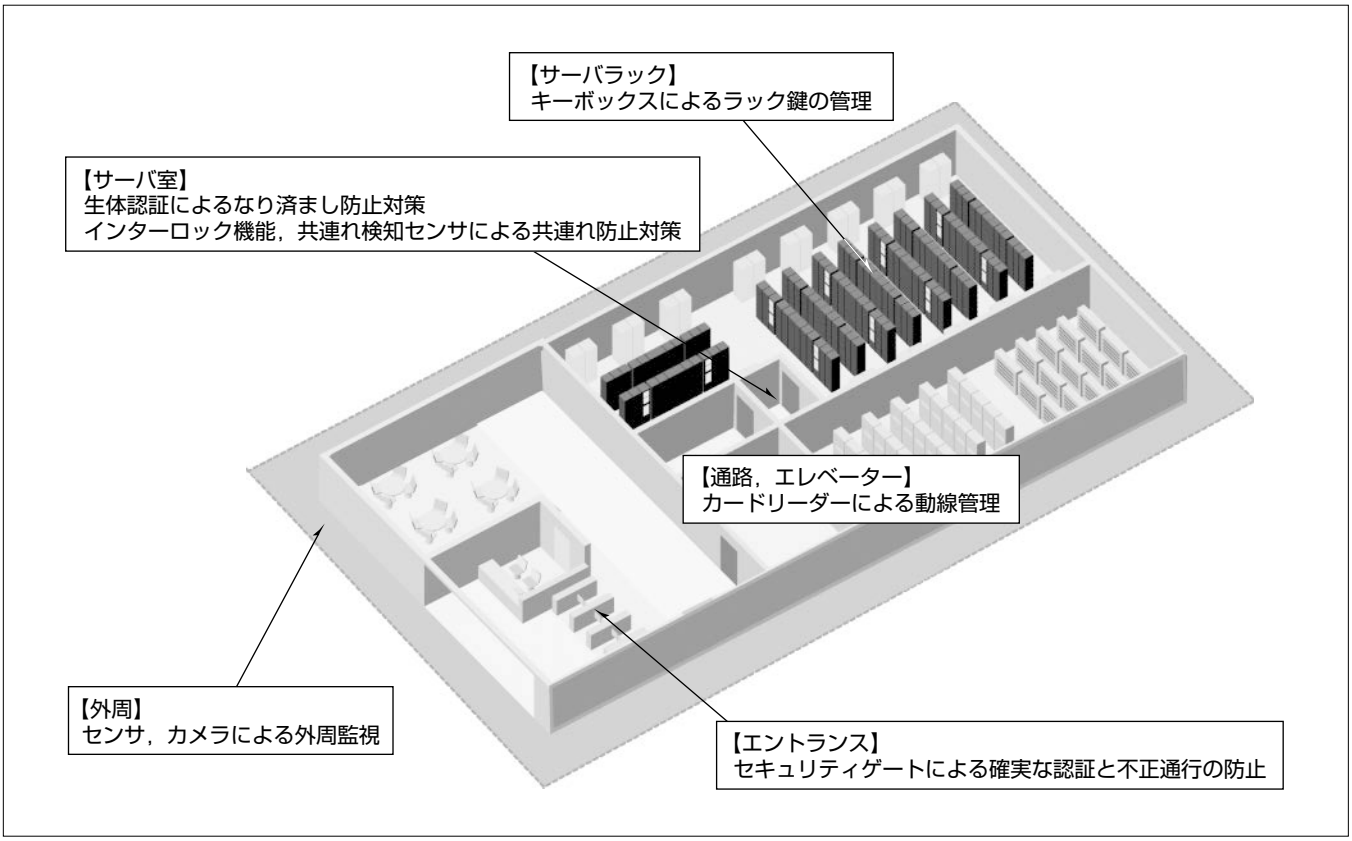
大庭寿康*
井上智善*

Security Solution for Data Center

Toshiyasu Oba, Tomoyoshi Inoue

要　旨

“クラウド”という言葉が一般的に認知され，本格的なクラウド時代の到来に加え，2011年3月に発生した東日本大震災とこれに伴う計画停電の影響によって，BCP(事業継続計画)の観点から，災害に強いファシリティと安定した電力供給能力を持つデータセンターの需要が高まっている。2010年には日本データセンター協会が“データセンターファシリティスタンダード[(1)]”を策定した。三菱電機は，この中で規定される最高レベル“ティア4”を満たすセキュリティを三菱トータルセキュリティソリューション“DIGUARD(ディガード)”で提供する。データセンターを守るためには，正常ルートで立ち入る者の認証を行う“アクセス管理”と，フェンス乗り越えなどによる不正ルートからの侵入を監視する“外周監視”が必要となる。外周監視では，設置環境や警戒レベルに応じたセンサの選定が重要となる。建物内のアクセス管理では，エントランスでのセキュリティゲートによる一人一人の確実な認証と不正通行の防止が必要となる。最重要エリアとなるサーバ室へのアクセスには，万人不同な生体情報を使った生体認証によるなり済ましの防止対策を行う。さらに，インターロック機能と共連れ検知センサの組合せによる，共連れ防止対策を行うことで，悪意を持った不正な侵入をも防止する，非常に高いレベルのセキュリティを提供することが可能である。サーバラックについては，キーボックスを利用することで，セキュリティと運用負荷の軽減を同時に解決することが可能であり，DIGUARDによって“外周”から“サーバラック”にいたるまでの全てのセキュリティをサポートする。



データセンター向けセキュリティソリューション

三菱のトータルセキュリティソリューションDIGUARDでは，敷地の外周から建物，サーバ室，サーバラックにいたるまで，データセンターで求められる高いレベルのセキュリティを丸ごと提供することで，安全・安心なデータセンター作りをサポートする。

*トータルセキュリティー事業推進部

1. まえがき

クラウド時代の到来によるサーバの集中化に加えて，2011年3月に発生した東日本大震災によってBCP（事業継続計画）の観点から，データセンターの需要が高まってきている。

データセンターのセキュリティはこれまで事業者が独自の基準で行っていたが，2010年10月に日本データセンター協会によってデータセンターで必要な設備の基準として“データセンターファシリティスタンダード（以下“JDCC FS”という。）”が策定され，立地条件，建物本体，電源設備，空調設備，通信設備と並び，セキュリティについても“ティア1”～“ティア4”の基準が示されることになった。“ティア”とは“Tier”であり“階層”の意味を持つ。JDCC FSでは階層ごとに満たすべき基準を規定することで，データセンターの設備がどの階層にあたるかを指し示し，データセンター事業者，利用者，建築・設備の設計者，運用保守に携わる人等，データセンターにかかわる様々な人に広く利用されることを目的としている。

本稿ではJDCC FSで規定される“外周監視”と“アクセス管理”のそれぞれに対して，最高レベル“ティア4”を満たすセキュリティソリューションについて述べる。

2. 外周監視

“ティア4”では建物内のカメラによる監視に加えて，敷地外周部での人又はカメラ，センサによる監視が必要であると規定している。昨今増加している郊外型の大型データセンターは広大な敷地を持っているため，その全てを人によって監視することはコスト面からも難しく，カメラ，センサによる外周監視システムの導入が有効である。

2.1 外周監視のセンサ

敷地外周部の監視，いわゆる外周監視をする上で重要なのはセンサの選定である。選定の誤りによって誤報の多発や，失報の発生といった事象が発生し，本来の目的を達成できないこととなる。センサの選定はセンサの特徴を踏まえて警戒するレベルや設置環境を十分に考慮して行う必要がある。外周監視のセンサとして使用されている代表的なセンサを次に示す。

(1) 赤外線センサ（線警戒（面警戒））

赤外線ビームの遮断によって侵入を検知する線警戒のセンサ（多段化による面警戒も可）である。

(2) 光ファイバセンサ（面警戒）

フェンスに取り付けた光ファイバの振動や検知線張力で生じる光の歪みによって侵入を検知する面警戒のセンサである。

(3) 電波式センサ（空間警戒）

2本のセンサケーブル間に形成される微弱な電界の変動によって侵入を検知する空間警戒のセンサ（**図1**）である。

2.2 センサの選定

センサにはそれぞれ特徴があり，検知性能でいえば，“線警戒”→“面警戒”→“空間警戒”の順に侵入を検知する能力が高くなり，すり抜けが困難となる。また，設置環境も重要なポイントになるため，**表1**に示すセンサの特徴を踏まえて選定する。

3. アクセス管理

“ティア4”のアクセス管理としては“敷地”“建物”“サーバ室”“ラック（サーバラック）”の4つのエリアに対してアクセス管理を規定している。データセンターという特性を踏まえると，“敷地”については工場や，オフィスビルのそれと大きな違いはないため，今回は“建物”“サーバ室”“ラック”のアクセス管理について述べる。

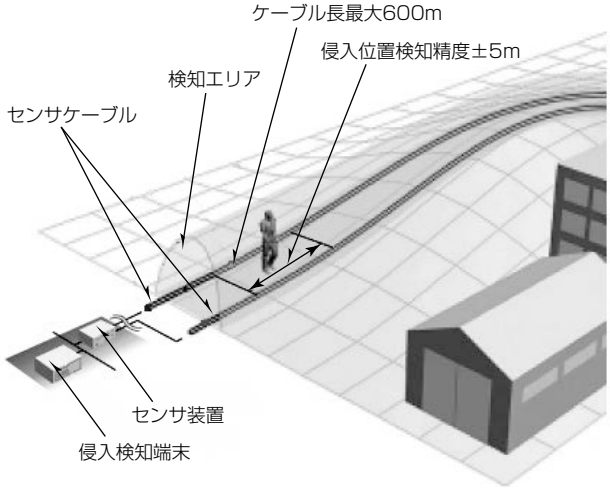


図1．電波式センサ“MELWATCH”のイメージ

表1．センサの主な特徴

方式	赤外線センサ	光ファイバセンサ	電波式センサ
検知性能	・植栽，小動物，飛来物等による誤報あり ・赤外線ビームのすり抜けによる失報の可能性あり	・フェンス面への接触が必要 ・テンション式，断線式，振動式の選択が可能	・植栽，小動物等による誤報は少ない ・空間警戒のためすり抜けによる失報なし
検知位置精度	・数m幅も可能だがセンサ数増大，通常50m幅以上	・10m幅以上で任意に設定が可能	・±5mの精度（10m幅）で侵入位置の検出可能
耐環境性	・豪雨，濃霧，着雪でビーム減衰，地盤沈下での光軸ずれ障害あり	・豪雨，濃霧，着雪，雷害の影響を受けにくい	・豪雨，濃霧，着雪の影響を受けにくい ・監視ラインの屈曲や地形の傾斜に対応可能
設置環境	・ポール，壁面等への設置が可能	・フェンスへの設置が可能	・地面への転がし敷設，埋設も可能
保守性	・投受光部の清掃や光軸調整が必要	・目視点検程度だけ	・センサケーブルはメンテナンスフリー

3.1 “建物”のアクセス管理

(1) エントランス

建物内で最初に出てくるアクセス管理の境界が，エントランスである。ここでの目的は，一人一人の確実な認証と，不正通行を防ぐことであり，セキュリティゲートの導入が有効である。データセンターでは，通常のオフィスに比べ，より確実な認証と不正通行を防ぐため，物理的に乗り越えを防止できるようなタイプが多く導入されている(**図2**)。

(2) 通路扉，エレベーター

サーバは利用者が用意し，場所，回線，電源等の設備を提供するコロケーションサービスを行うデータセンターでは様々な企業が出入するため，利用者が自社サーバの設置フロア，エリア以外に立ち入ることができないよう，利用者の動線を制限することが必要となる。フロアの制限はエレベーターのかご内にカードリーダーを設置し，共用フロア以外は行き先階のボタンを無効にしておく。利用者はカード認証をすることで許可されたフロアのボタンが有効となり，そのフロアへの立入りが可能となる。

3.2 “サーバ室”のアクセス管理

“ティア4”では“サーバ室”への入室には，カード認証だけでなく，テンキー(暗証番号)又は生体認証による，なり済まし防止対策，さらに，共連れ防止対策が必要であると規定している。

図2．セキュリティゲート

3.2.1 なり済まし防止対策

カードだけの認証では，紛失，盗難及び，譲渡によって不正にカードを入手した人物が正規所有者になり済まして入室ができてしまう。この対策としてテンキー又は生体認証の導入が考えられるが，テンキーによる対策は紛失，盗難によるなり済ましを防ぐことはできても，(故意の)譲渡によるなり済ましは暗証番号も同時に漏えいする可能性が高いため，防ぐことができない。このため，確実になり済ましを防止するには生体認証の導入が必要となる。

3.2.2 共連れ防止対策

共連れを防ぐためには，確実な一人通行をさせる仕組みが必要となる。今回はインターロック機能と共連れ検知センサの組合せによる共連れ防止対策について述べる。

(1) インターロック機能

入退室管理におけるインターロック機能とは，1つの部屋で，同時に2か所以上の扉を開扉させないようにする機能である。共連れ防止対策では，サーバ室の入り口に前室を作り，サーバ室側の扉が開扉しているときは反対側の扉が開扉されないようにすることで，後から来た人物が前室に入ることを防ぐ。しかし，これだけでは前室内にはじめから2人の人物がいた場合に，共連れが可能になってしまう。これを防ぐために，必要となるものが共連れ検知センサである。

(2) 共連れ検知センサ

共連れ検知センサは，2組のステレオ画像計測によって得られる情報(人物の高さ・面積等)をもとに検知エリア内の人数を高精度に判定する。前室の大きさを検知エリアに合わせることで，前室内の人数を判定し，2人以上を検知した場合は，サーバ室側の認証操作を禁止することで，サーバ室に一人ずつしか入ることができないようにする。

図3にインターロック機能と共連れ検知センサの利用イメージ，**図4**に共連れ検知センサの外観を示す。

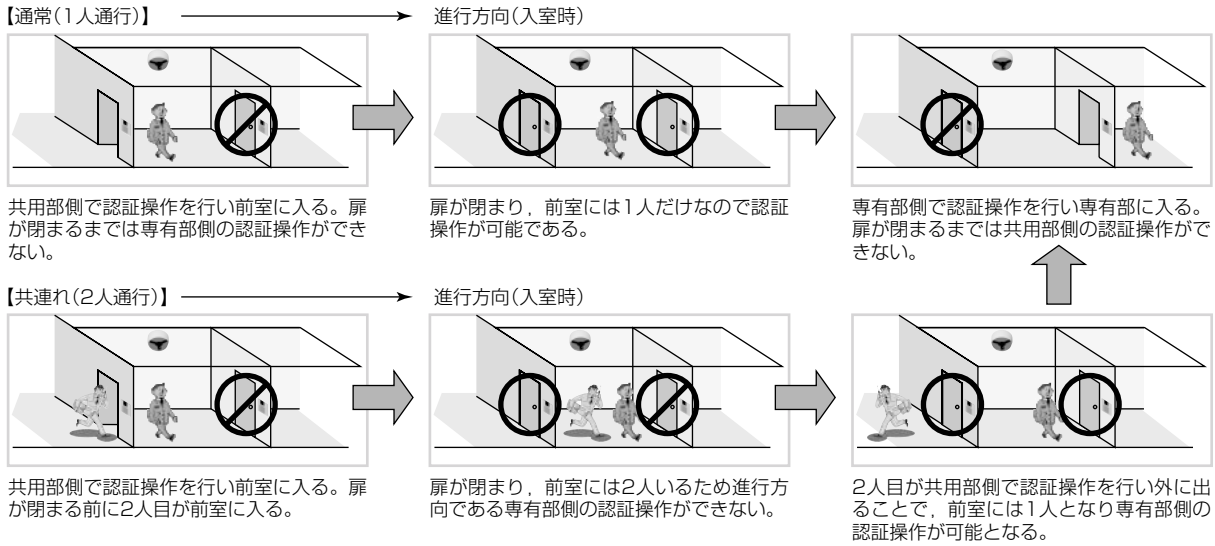


図3．インターロック機能と共連れ検知センサの利用イメージ

図4．共連れ検知センサ

図5．キーボックス

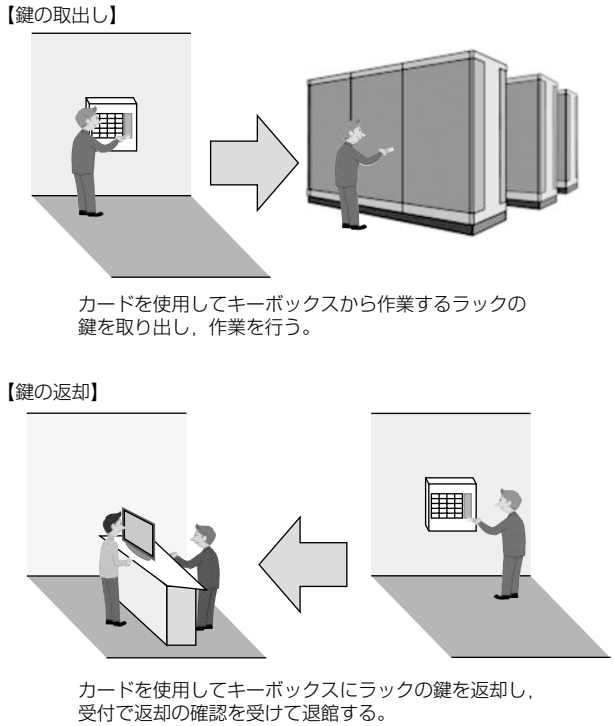


図6．キーボックスの運用イメージ

3.3 “ラック”のアクセス管理

“ティア4”では“ラック”のアクセス管理として鍵又は，カード認証・生体認証の使用を規定している。鍵による管理が最も一般的であるが，鍵の管理を人が行う場合は，貸出し，返却，及び履歴の記入等，管理業務による運用負荷が高くなり，誤った鍵を貸し出すなどのミスも懸念される。一方，ラックの開閉にカード認証・生体認証を使用することで運用負荷は軽減できるが，ラック自体に認証装置が必要となるため初期導入時やラック増設時のコストが非常に高額となる。この問題を同時に解決する方法が，キーボックスによる鍵の管理である。

カードリーダーを内蔵したキーボックス(**図5**)によってラックの鍵を管理することで，利用者自身で鍵の取り出し，返却を行うことが可能となる。利用者が取り出せる鍵はあらかじめ設定しておくため，誤って別の鍵を使われる心配もなくなり，扉の通行履歴と同様に誰が，いつ鍵を取り出し，返却したのかは履歴としてシステムに自動で蓄積される。また，鍵の返却状況はセンター装置で確認が可能なため，受付にセンター装置を設置することで，退館時に鍵の返却を確認することが可能となる。

図6にキーボックスの運用イメージを示す。

4. む す び

データセンターに求められるセキュリティについて，“JDCC FS”で規定する最高レベル“ティア4”を満足する具体的なセキュリティソリューションを一部運用も交えて述べた。DIGUARDでは今回述べたソリューション以外にも，セキュリティロッカーや，昨今特に重要なテーマとなっている省エネルギーに関連したソリューションとして，入退室管理システムと照明システムを連携させ，無駄なく，快適に照明を制御することが可能なソリューションなど，様々なラインアップを揃(そろ)えている。

郊外型データセンターの増加や，コンテナ型のデータセンターの登場等，データセンターの需要が高まるとともに，その形態も変化してきているが，今後もDIGUARDの様々なラインアップから最適なソリューションを提供していく。

参 考 文 献

(1) データセンターファシリティスタンダードの概要，日本データセンター協会（2010）