データセンターの物理的脅威の監視手法

ホワイトペーパー102

改訂 3

クリスチャン・コーワン
クリス・ガスキンス

> 要約

従来の方法によるデータセンター環境の監視は、もはや十分なものではありません。空調の需要に拍車をかけるブレードサーバーなどのテクノロジーが開発され、データセキュリティーにさらに高度な要件を求めるサーベンスオクスリー法などの法令が定められている現在、データセンターの物理環境は、さらに厳密に監視する必要に迫られています。UPS システム、コンピュータールームの空調設備、消火システムといった物理機器を監視するための、十分な理解を得たプロトコルが存在する一方で、見落とされることが少なくないある種の分散監視ポイントも存在します。本書では、ダウンタイムの低減を目的として、この種の脅威を詳述し、監視装置へのアプローチを提案するとともに、収集データの活用におけるベストプラクティスを提示します。

目次

セクションをクリックすると、
そのセクションに直接移動します。

APC　Schneider Electric 発行のホワイトペーパーライブラリーに、Schneider Electric Data Center Science Center 執筆による APC のホワイトペーパーが加わりました。同ホワイトペーパーの内容に関するお問い合わせは、DCSC@Schneider-Electric.com までお願いいたします。

Schneider Electric

はじめに

こんにちのデータセンター環境の一般的な監視方法は、中央に集中化されたメインフレームの時代にさかのぼります。当時は、温度計を持ってあちこち計測して歩いたり、部屋の環境に対する IT 部門のスタッフの「勘」に頼ったり、というケースもありました。しかしデータセンターは、パワーと空調の需要に拍車をかける分散処理やサーバーのテクノロジーとともに進化し続けているため、その環境をさらに厳密に監視する必要があります。

電力密度と動的な電力変動の向上は、IT 環境の監視方法に変化を強いる二大要因です。ブレードサーバーの登場により、電力密度は大幅に高まり、周辺環境の電力および空調の変化の型は劇的な変化を遂げました。電力管理技術の発展により、サーバーや通信機器の性能が飛躍的に向上し、計算負荷に基づいて消費電力（すなわち熱の放散）を変化させることが可能になりました。この点については、ホワイトペーパー43「*データセンタとサーバールームの動的な電力変動*」で詳述します。

関連リソース
ホワイトペーパー43
データセンタとサーバールームの動的な電力変動

無停電電源装置（UPS）、コンピュータールーム空調装置（CRAC）、消火システムなどの物理機器に高度な監視機能やアラート機能を備えることは一般的ではありますが、物理環境のその他の面は、見落とされることが少なくありません。機器を監視するだけでは十分とは言えません。周辺環境を全体的にとらえ、不審者の侵入や脅威を積極的に監視する必要があります。そうした脅威には、サーバーの換気口の過熱、漏水、データセンターへの無許可の人為アクセス、あるいはデータセンター内のスタッフによる不適切な行為も含まれます。

リモート ネットワーク ロケーション（支社や支部、ネットワーククローゼット、各地の販売拠点など）では、人を物理的にその場に配置して温度や湿度などの条件を確認させるのは現実的ではないし、信頼性も低くなるため、自動監視システムの需要がさらに高まっています。無人のネットワーク拠点が導入されたことにより、IT 管理者は信頼性の高いシステムを確保して、ネットワークの最新状態を把握する必要に迫られています。

最新の技術を用いれば、監視システムを、データセンターの特定の環境およびセキュリティ要件を満たすように仔細に設定することができます。つまり、各ラックは、独自の要件を持つ小さな「データセンター」とみなされ、複数のデータ収集点を対象とする監視戦略が確立されます。

本書では、分散監視戦略によって軽減できる物理的脅威について説明し、データセンター内にセンサーを設置するためのガイドラインとベストプラクティスを提供します。また、データセンターの設計ツールを使用して、こうした分散監視システムの仕様およびデザインプロセスを単純化する方法についても述べます。

分散した物理的脅威とは

本書では、分散した物理的脅威という部類の脅威への対処について述べます。重要なのは、この種の脅威からデータセンターを守るには綿密かつ専門的な設計が必要だということです。この種の脅威を特定するには、データセンターに対するさまざまな脅威の特徴を簡単に把握しておくことが役立ちます。

データセンターの脅威には、ソフトウェアおよびネットワーキング（**デジタルの**脅威）の領域にあるものと、データセンターの物理サポートインフラストラクチャー（**物理的な**脅威）の領域にあるもの、という 2 つの大分類があります。

関連リソース
ホワイトペーパー101
ネットワークセキュリティの基礎

デジタルの脅威

デジタルの脅威とは、セキュリティまたはデータのフローに対する偶発的または悪意のある攻撃（ハッカー、ウイルス、ネットワークボトルネック、その他）のことです。デジタルの脅威は業界やメディアでも注目を浴びており、防御策としてほとんどのデータセンターでは、堅牢性の高い、積極的に保守がなされたシステム（ファイアウォール、ウイルスチェッカーなど）を備えています。デジタルの脅威への対応策については、ホワイトペーパー 101「*ネットワークセキュリティの基礎*」で確認します。本書の主題は、デジタルの脅威ではありません。

物理的脅威

IT 機器に対する物理的脅威には、電力や空調の問題、人為ミスや悪意、火災、水漏れ、大気質などがあります。これらの脅威のうち、電力に関するものと空調および火災に関するものは、電力、空調、および消火に関する各装置の内蔵機能によって定期的に監視されます。たとえば、UPS システムは電力品質、負荷、およびバッテリー状態を監視します。PDU は回路の負荷を監視します。空調装置は吸込み、および吹出しの温度とフィルターの状態を監視します。消火システムは（建築基準で必須とされるもの）は、煙と熱が発生していないかどうかを監視します。こうした監視は、情報を集約・記録・解釈・表示するソフトウェアシステムによって自動化された、十分な理解を得たプロトコルに従って行われます。このように、機器に組み込まれシステム化された機能によって監視される脅威は、それを監視・解釈するシステムが技術的に優れていれば、ユーザーの専門知識や計画を立てる手間を特に必要とせずに、効果的に管理することができます。*こうした自動監視の対象となる物理的脅威は、総合的な管理システムの重要な要素ではありますが、本書の主題ではありません。*

しかし、データセンターにおけるある種の物理的脅威（しかも深刻なレベルのもの）は、事前に設計された組み込みの監視ソリューションを提供してはくれません。たとえば、湿度が低下するという脅威は、データセンター内のどの場所でも起こりえるため、湿度センサーの数と配置はこの脅威を管理するうえでの重要ポイントです。そうした脅威は、**データセンターのあらゆる場所、部屋のレイアウトや機器の配置に特有のさまざまな場所に分布している可能性があります。**本書で取り上げるそうした分散した物理的脅威は、一般に次のようなカテゴリーに類されます。

- IT 機器に対する大気質の脅威（温度、湿度）
- 漏水
- 人の存在または異常な行為
- 人員に対する大気質の脅威（外来の空気中物質）
- データセンターの危険要因による発煙および火災[1]

図 1 はデジタルの脅威と物理的脅威の違いを、さらに物理的脅威についてはシステム化された機器ベースの電力／空調監視における脅威と監視センサーのタイプ、場所、および数を判断するために、評価、決定、計画を要する（本書の主題である）分散した脅威に分けて、その違いを説明しています。効果的な監視戦略のデザインに関する知識や専門技術の欠如から事態を等閑視する危険を招くおそれがあるのは、後者のタイプの物理的脅威です。

[1] 室内では最小限の煙・火災検知対策を講じることが建築基準の要件となっていますが、これは特定の法令または安全規格によって規定されるものであり、本書の主題ではありません。本書は、建築基準の要件からは離れて、データセンターの危険に特有の補助的な煙検知を取り上げます。

図 1

データセンターの脅威

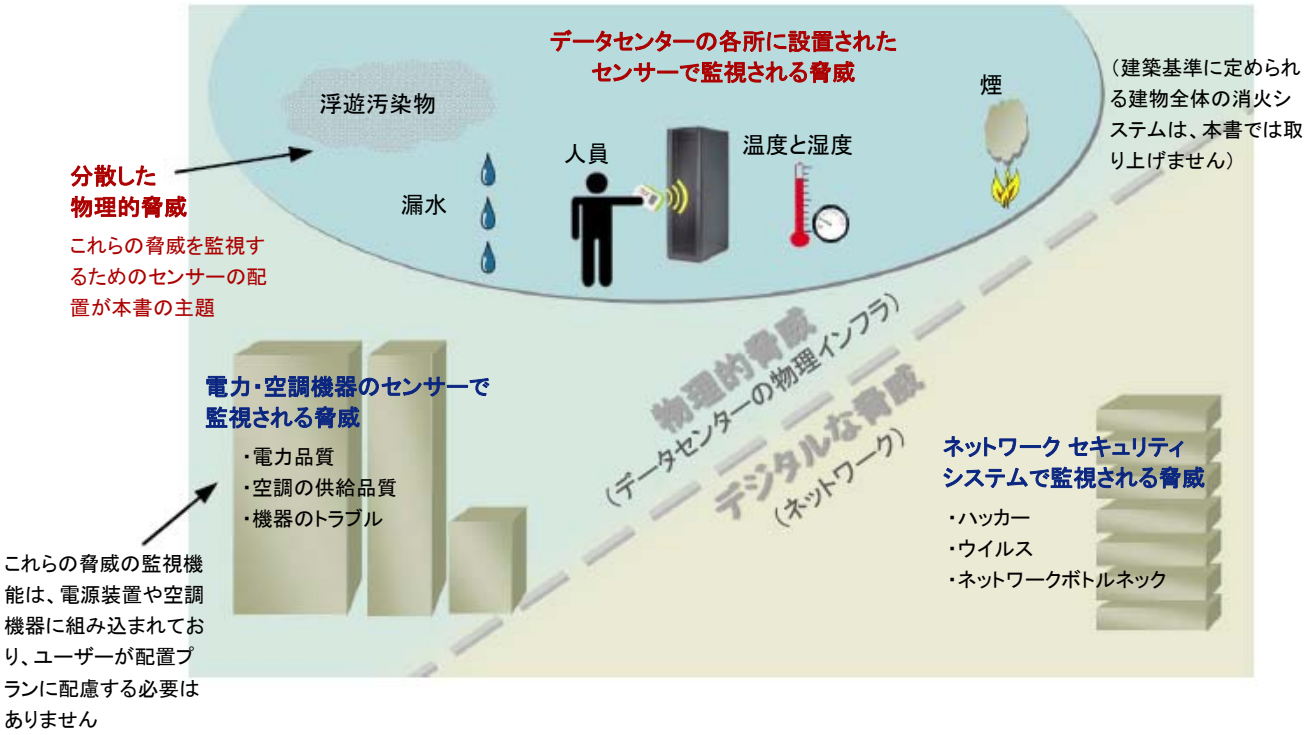


表 1 は、分散した物理的脅威、そのデータセンターに対する影響、およびその監視に使用するセンサーのタイプをまとめたものです。

表 1

分散した物理的脅威

脅威	定義	データセンターへの影響	センサーのタイプ
温度	部屋、ラック、および機器の温度	仕様値を超える温度による機器の故障や寿命の短縮、または急激な温度変化、あるいはその両方	温度センサー
湿度	部屋およびラックの特定の温度における相対湿度	低湿度での静電気蓄積による機器の故障 高湿度での結露の発生	湿度センサー
液体の漏れ	水または液冷媒の漏れ	液体による床面、配線、および機器への損傷 CRAC のトラブルの兆候	ロープ式の漏水センサー スポット式の漏水センサー
人為ミスと人の出入り	人員による意図しない不正行為 無許可または強制による（あるいはその両方）、悪意を伴うデータセンターへの入室	機器の損傷、およびデータの損失 機器の中断 機器の盗難、および損壊	デジタル ビデオ カメラ モーションセンサー ドアスイッチ ガラス破壊センサー 振動センサー
煙／火炎	電気または物質から生じた火災	機器の故障 資産やデータの損失	補助煙センサー
危険な浮遊汚染物	大気中の化学物質（バッテリーの水素、粉塵などの粒子）	人員にとって危険な状況または UPS の信頼性の欠如（あるいはその両方）と、水素の放出による故障 静電気の増加による機器の故障や、粉塵の蓄積によるフィルター/ファンの詰まり	化学／水素センサー 粉塵センサー

センサーの配置

さまざまなタイプのセンサーを使用することで、上記のような脅威がもたらすトラブルを早期に警戒することができます。センサーの細かいタイプと数は、予算、脅威のリスク、および違反行為のビジネスコストによって異なりますが、ほとんどのデータセンターにとって有用な必要最小限のセットがあります。**表 2** に、この推奨される基本的なセンサーのセットのガイドラインを示します。

表 2

基本的なセンサーのガイドライン

センサーのタイプ	場所	一般的なベストプラクティス	コメント	該当する業界のガイドライン	例
温度センサー	ラック	各ITラックの前面ドアの上部、中央部、および下部。ラック内の装置の吸気口温度を監視する。	ネットワーククローゼットやその他のオープンラック環境では、温度監視は機器の吸気口にできるだけ近い位置で行うこと。	ASHRAE ガイドライン[2]	
湿度センサー	ラック列	コールドアイルごとに1本。ラック列中央にあるラックの前面に設置する。	CRACユニットに湿度の測定値が示されるため、CRACの出力に近すぎる場合はラック列ベースの湿度センサーを調整する必要がある。	ASHRAE ガイドライン	
ロープ式の漏水センサー スポット式の漏水センサー	部屋	各CRACシステム周辺、空調分配ユニット周辺、およびフリーアクセスフロアの下、その他のあらゆる水漏れ源（配管など）にロープ式漏水センサーを配置する。	ドレンパンの液体のあふれを監視するためのスポット漏水センサー。小さ目の部屋やクローゼット、その他あらゆる低位置のスポットを監視する。	業界基準なし	
デジタルビデオ カメラ	部屋およびラック列	入出ポイントをカバーし、すべてのホットアイル／コールドアイルが見渡せるデータセンターのレイアウトに従って効果的に配置。必要な視界全体を確実にカバーする。	通常アクセスと無許可または定時過ぎのアクセスを、ビデオ監視ソフトにより監視・記録する。	業界基準なし	
ルームスイッチ	部屋	すべての入口のドアに電子スイッチを配置し、部屋への出入りについて追跡記録を残す。また、部屋への出入りを特定の時刻／人員のみに制限する。	ルームスイッチは設備に統合されることが望ましく、これは通信インターフェイスを介して実現できる。	HIPAA 法およびサーベンスオクスリー法[3]	

表 2 に示した必須のセンサーのほかに、個別の部屋の構成、脅威のレベル、および可用性の要件に基づいて任意に検討してよいものがあります。
表 3 に、ベストプラクティスのガイドラインとともにその他のセンサーを一覧で示します。

[2] ASHRAE TC9.9 Mission Critical Facilities, *Thermal Guidelines for Data Processing Environments*, 2004.

[3] CSO Fiona Williams, Deloitte & Touche セキュリティーサービスは次のように述べています。「物理的なセキュリティはサーベンスオクスリー法の要件に該当する。物理的なセキュリティは、一般的なコンピューター制御に欠かせないだけでなく、情報セキュリティープログラムの重要な要素でもある。これは、経営陣に対して内部の制御手段が有効に機能しているかどうかを評価・確認するよう求める第 302 条および第 404 条に該当する。http://www.csoonline.com/read/100103/counsel.html（2010 年 5 月にアクセス）

表 3

状況に応じて追加するセンサーのガイドライン

センサーのタイプ	場所	一般的なベストプラクティス	コメント	該当する業界のガイドライン	例
補助煙センサー	ラック	非常に重要なエリアまたは専用の煙センサーがない環境において、ラック単位で「超高感度煙検出器」(VESD)を設置する。[4]	予算の都合によりラック単位で補助煙検出器を設置できない場合は、各CRACの吸気口にVESDを設置して一定レベルの早期警戒機能を確保する。	業界基準なし	
化学／水素センサー	部屋	データセンターにVRLAバッテリーが配置されている場合、湿式電池とは異なり通常の使用では水素が放出されないため、室内に水素センサーを設置する必要はない。	独立したバッテリー室にある湿式電池は、特別な規則の要件を満たしている必要がある。	Draft IEEE / ASHRAE ガイド[5]	
モーションセンサー	部屋およびラック列	デジタルカメラを設置する予算がない場合に使用する、ただしデジタルカメラの設置がベスト(**表 2** を参照)。	モーションセンサーは、人の動きを監視するビデオカメラの代用として、比較的低コストで導入できる。	業界基準なし	
ラックスイッチ	ラック	人の出入りが多いデータセンターでは、前面および背面のドアに電子スイッチを設置し、アクセスの追跡記録を残すとともに、特定時刻の特定人員による重要機器へのアクセスを制限する。	ラックスイッチは設備に統合されることが望ましく、これは通信インターフェイスを介して実現できる。	HIPAA 法およびサーベンスオクスリー法	
振動センサー	ラック	人の出入りが多いデータセンターでは、各ラックに振動センサーを設置し、重要な機器の無許可の設置や撤去を監視する。	各ラックの振動センサーは、誰かがラックを動かしたことを検知するのにも利用できる。	業界基準なし	
ガラス破壊センサー	部屋	すべてのデータセンターの窓にガラス破壊センサーを備える(廊下や部屋の内外)。	ビデオ監視カメラと組み合わせて使用するのがベスト。	業界基準なし	

[4] 建築基準を満たす火災検知システムが配備されているという想定。

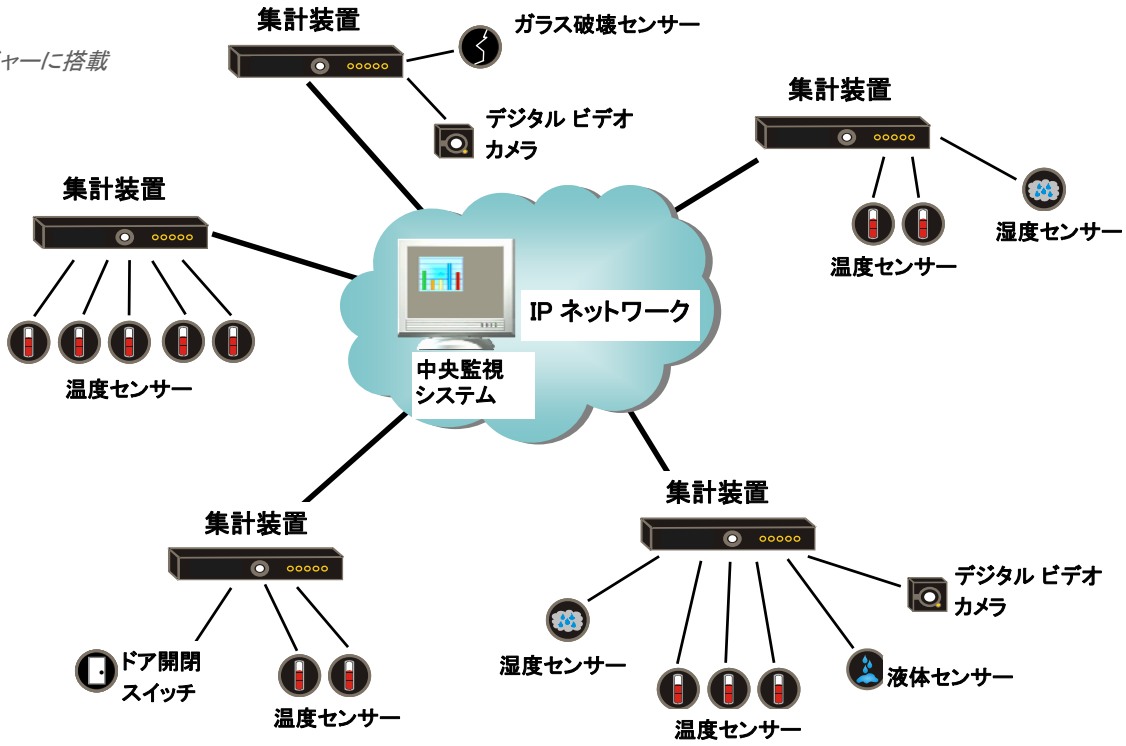
[5] IEEE/ASHRAE の「*Guide for the Ventilation and Thermal Management of Stationary Battery Installations*」(2006 年後期に票決の草稿)

センサーデータの集計

センサーを選択し、配置したら、次のステップは、各センサーで検出されたデータの集計と分析です。センサーのデータをすべて中央の収集ポイントに送るよりも、データセンターの各所に集計ポイントを分散し、各集計ポイントにアラートと通知の機能を用意するほうがよいでしょう。こうすれば、1 カ所のポイントの障害が中央集計ポイントに影響を及ぼすリスクを排除できるだけでなく、遠隔地のサーバールームや通信事業用クローゼットの監視にも対応できます。[6] 各集計装置は、IP ネットワークを介して中央監視システムと通信します（**図 2**）。

図 2

ラックのエンクロージャーに搭載された集計装置



各センサーは、通常は、個別に IP ネットワークに接続してはいません。集計装置がセンサーデータを解釈し、アラートを中央システムへ、または直接通知リストへ（あるいは両方の方法で）送信します（次項を参照）。こうした分散監視のアーキテクチャーは、必要なネットワークのドロップ数を劇的に減少させ、システム全体のコストと管理の負担を低減します。集計装置は、通常はデータセンター内の物理エリアに配置され、センサーの配線の複雑化を避けるために、限定されたエリアのセンサーを対象として集計を行います。

「インテリジェントな」アクション

センサーからは生データが得られますが、そのデータを解釈して、アラート、通知、修正といったアクションにつなげることも、同じくらい重要です。監視戦略が高度化し、監視の行き届いたデータセンター内でセンサーの数が増すにつれて、膨大化し得るデータを「インテリジェント」に処理することが重要になります。センサーのデータを収集・分析して適切なアクションを起こすためには、前項で説明した「集計装置」を利用するのが最も効果的で効率的な方法です。

[6] アラートおよび通知機能を備えた複数の集計装置がセンサーをサポートするというこのアーキテクチャーは、「エッジでの分散インテリジェンス」とも呼ばれます。

重要なのは、データの選別、関連付け、および評価を行い、異常なイベントが発生した場合でも最善のアクションを決定するということです。効果的なアクションとは、適切な人に、適切な方法で、適切な情報をもって警告することです。アクションは、以下の 3 つの方法で実行されます。

- 特定の機器、ラック、またはデータセンター全体の脅威となり得る異常な状態に対して**警告(アラート)**する
- 特定のアラートや閾値に基づく自動的な**アクション**
- 改善、最適化、および障害/故障の測定を促すための**分析とレポート**

アラート

アラートの設定時には3つの項目を指定します。***アラームのしきい値***(どの程度の値に達したらアラームを発生させるか)、***アラートの方法***(誰に対してどのようにアラートを送るか)、および***エスカレーション***(特定の種類のアラームを解決するために、異なるレベルのエスカレーションを必要とする)

アラームのしきい値 - それぞれのセンサーについて、稼動状態の許容値を定義し、その値を超えたときにアラームが発せられるようにしきい値を設定します。各センサーに複数のしきい値を設定して、注意、警告、重大、故障といったいろいろなレベルのアラートを発することのできる柔軟性ある監視システムが理想的です。単独のしきい値に加え、しきい値超過が一定時間継続した場合や、値の増加率、減少率など、複数のアラーム発生条件を設けておく必要があります。温度については、一時点の温度よりも温度の変化率を基準にしてアラートを発するほうが、障害をより早期に発見できます。

しきい値を最大限に活用するには、慎重に設定する必要があります。しきい値にはさまざまな種類があり、事態の深刻さに応じて異なるアラートが発生します。たとえば、湿度がしきい値を超えた場合は IT 管理者にE メールが送信されるだけなのに対し、煙センサーの場合は自動的に消防署に呼び出しがかかります。同様に、各レベルのしきい値で、それぞれ異なる経路のエスカレーションができます。たとえば、誰かが無許可でラックにアクセスした場合は IT 管理者に通知されるだけなのに対し、ラックに無理やり侵入した場合は IT 部門の責任者に通知されるという具合です。

まず、グローバルに適用されるしきい値の初期値を設定しておき、IT 機器の仕様やセンサーの設置場所、機器の設置場所に応じて調整する必要があります(たとえば、サーバーの電源近くに設置したセンサーは、サーバーの吸気口近くに設置したセンサーよりも高い値でアラームが発するように設定します)。**表 4**[7] は ASHRAE TC9.9 に基づく温度と湿度の推奨閾値を示しています。これらのしきい値に加えて温度の変化を監視することも重要です。5 分間で温度変化が 5.6°C 以上ある場合は、CRAC に障害が発生している可能性があります。

表 4

温度・湿度センサーの推奨閾値

センサー	高閾値	低閾値
温度	25°C	20°C
湿度	相対湿度55%	相対湿度40%

[7] *最も厳密に管理されるクラス 1 環境のための ASHRAE TC9.9 勧告。重大任務を遂行するデータセンターに最適です。*

アラートの方法 ― アラートを伝えるには、E メール、SMS テキストメッセージ、SNMP トラップ、HTTP サーバーへの投稿など、いろいろあります。重要なのは、意図した受信者に適量の情報を確実に送信できるように、アラートシステムに柔軟性を持たせ、カスタマイズ可能な状態にしておくことです。アラートの通知には、ユーザーが定義したセンサーの名前と場所、アラームの日時などの情報を含めるようにします。

アラートのエスカレーション ― 緊急の対処を必要とするアラートもあります。インテリジェントな監視システムでは、指定時間内に問題が解決できない場合、アラームの権限レベルが高まるように設定できなければなりません。アラートのエスカレーションによって、些細なことが大きな問題になる前に、タイミングよく問題に対処できるようになります。

役立つアラートと、あまり役立たないアラートの例を以下に示します。

Temperature sensor #48 is over threshold（温度センサー48 がしきい値を超過）― センサー48 がどこに設置されているかわからないため、あまり役に立ちません。

Web server X is in danger of overheating（Web サーバー X が過熱で危険な状態）―サーバーが特定されているため、比較的役に立ちます。

Door sensor has been activated（ドアのセンサーが作動中）―ドアが特定されていないため、あまり役に立ちません。

Door X at location Y has been opened, and a picture of the person opening the door was captured（場所 Y のドア X が開いており、ドアを開いた人物の映像が記録されている）―ドアの名前と場所が特定され、現場の写真があるため、非常に役に立ちます。

データに基づくアクション

センサーからのデータの収集は第一歩にすぎません。データセンターの管理者が手動の対応のみに頼っていては、収集したデータを最大限に活用することはできません。ユーザーが設定したアラートとしきい値に基づいて、自動的にアクションを実行するシステムが利用できます。そうした「インテリジェントな」自動システムを導入するには、以下のことを検討する必要があります。

アラートのアクション―アラートの深刻度に応じて、どのような自動アクションが必要か。自動アクションには、担当者への通知や、修正措置（ドライ接点を作動させてファンやポンプのオン／オフを自動的に切り替えるなど）があります。

センサーデータのリアルタイム表示―センサー状態の「スナップショット」を表示する機能は必須です。ただし、各センサーの「トレンド」をリアルタイムで表示できれば、状況をより正確に把握できます。こうしたトレンドを解釈することによって、管理者は幅広い問題を見つけ出し、複数のセンサーのデータを相互に関連付けることができます。

アラートシステムは、しきい値の超過を通知する以上の機能が求められます。たとえば、一部の監視システムでは、管理者がアラートに追加情報を含めることができます。追加できるのは、ビデオ、音声、グラフ、地図などです。こうした高度なアラートシステムがあれば、データのコンテキスト情報もアラートに含めることができるため、管理者はより正確な情報に基づいて意思決定ができるようになります。場合によっては、多すぎる情報から有用な情報のみを抽出する必要があります。たとえば、人の出入りが激しいデータセンターで、人の動きがあるたびにアラートが発生するようでは仕事の妨げになります。また、セキュリティのために特定の情報をブロック（マスク）する場合もあります。たとえば、キーボードを写しているビデオでは、パスワードを入力する場面はブロックされます。
「インテリジェントな」解釈とアクションの例を以下に挙げます。

- 温度がしきい値に達したら、自動的にファンや CRAC をオンにする
- リアルタイムのビデオ監視によって人の顔を判別し、電子式ドアを装えたラックへのアクセスをリモートで与える
- リモートのデータセンターで水漏れが検知された場合、自動的に排水ポンプを作動させる
- 通常の稼働時間外にデータセンター内で人の動きが検知された場合、自動的にビデオに撮影し、警備員に通知する
- 終業後にガラスの破損が検知された場合、警備員に通知して警報を鳴らす
- ドアスイッチによってラックのドアが 30 分以上開いている(ドアが正しく閉じられていない)ことが判明した場合、ドアを確認するように管理者に警告する

分析とレポート

インテリジェントな監視システムでは、センサーデータの短期間のトレンドだけでなく、長期間にわたる履歴データも扱うことができます。最善の監視システムでは、週単位、月単位、さらには年単位のセンサーデータにアクセスし、それをグラフやレポートの形で出力する機能を備えています。グラフには、同一レポートに複数のタイプのセンサーが表示され、比較と分析ができるようになっています。レポートには、指定した時間帯における各種センサーの最高値、最低値、および平均値が示されます。

センサーの長期間の履歴情報は、さまざまな方法で活用できます。たとえば、長期データを分析することによって、データセンターのキャパシティが一杯になった原因は物理的なスペースではなく不十分な空調システムにある、といったことがわかります。データセンターの機器が増え続ける中で、こうした情報を、将来のトレンドの分析に利用したり、データセンターがキャパシティに達する時期の予測に役立てたりすることができます。長期間のトレンド分析をラックレベルで利用することで、各ラックに配置された各メーカーの機器を比較し、より放熱が多い機器はどれか、より稼動時の放熱が少ない機器はどれかを判別できます。こうした情報は、将来の機器の購入にも影響します。

監視システムが捕捉したセンサーのデータは、業界標準の形式でエクスポートして、カスタムのレポートや分析ソフトだけでなく、より汎用性の高いレポートにも活用できます。

設計方法

脅威監視システムの仕様と設計は複雑に見えますが、APC の InfraStruXure Designer をはじめとするデータセンター設計ツールを利用すれば、作業を自動化することができます。こうした設計ツールでは、ユーザー指定項目の簡単なリストを入力するだけで、センサーと集計装置が適切な数だけ自動的に配置されます。
生成された要約レポートには、推奨されるセンサーのパーツリストと設置手順が記されます。こうしたデータセンター用の設計ツールでは、ベストプラクティスと業界標準に基づいたアルゴリズムや既成のルールを用いて、密度、部屋のレイアウト、部屋へのアクセスに関するポリシー、ユーザーごとの監視条件などに応じた特定の構成を推奨します。

たとえば、以下のようなユーザー指定項目は、データセンターのトラフィックとアクセスのレベルに応じて、脅威の監視システムの設計に影響を及ぼします。

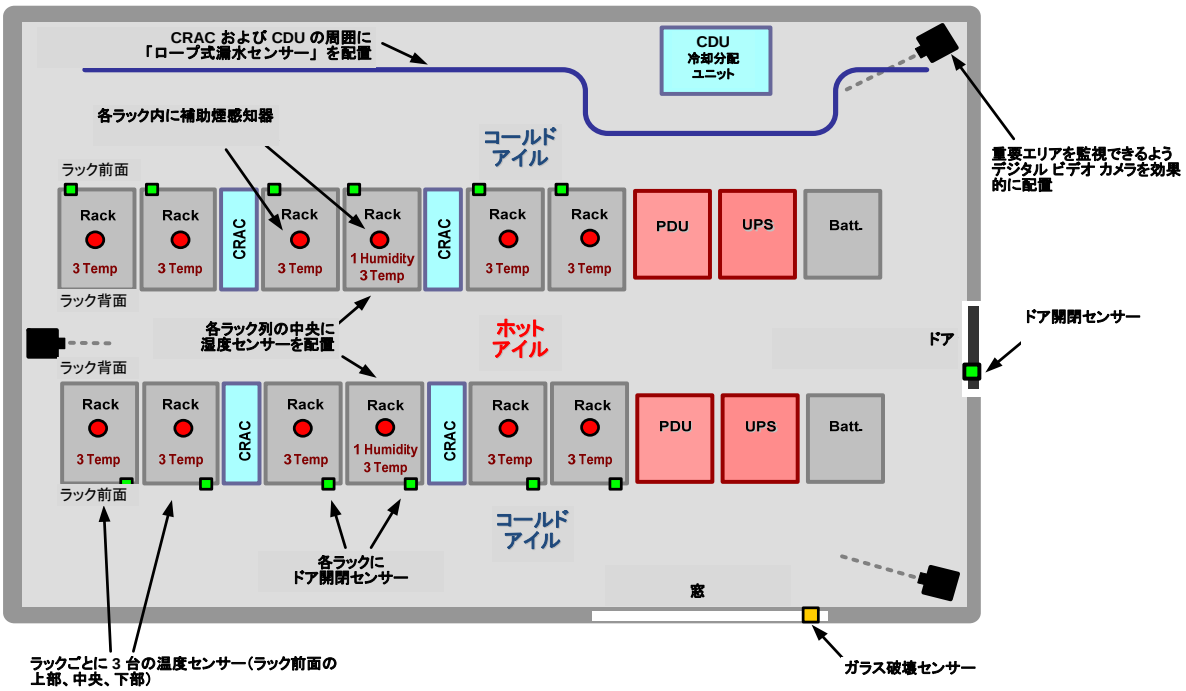
- **多いトラフィック／アクセス**－さまざまな用件や職務の人が多数アクセスするデータセンターの場合、各ラックにラックスイッチを配備し、必要な人にのみラックへのアクセスを許可します。
- **少ないトラフィック／アクセス**－データセンターの役割に責任を持つ少数の特定の人だけがアクセスするデータセンターの場合は、各ラックへのアクセスを制御するためのラックスイッチではなく、他の人が部屋へ入るのを制限するためのルーム ドア スイッチを備えれば十分です。

センサーのレイアウト例

図 3 にデータセンターのレイアウト例を示します。監視装置は、本書に示したベストプラクティスに基づいて配置されます。

図 3

センサーのレイアウト例



結論

総合的なセキュリティ戦略においては、分散した物理的脅威への対策を講じることがたいへん重要です。センサー機器の配置と用法には、評価、判断、および設計が必要となりますが、ベストプラクティスと設計ツールを利用すれば、効果的なセンサーの配備に役立ちます。

適切なタイプのセンサーを、適切な場所に適切な数だけ設置することに加え、収集したデータの管理、ログイン、トレンド分析、インテリジェントなアラート通知、修正措置の自動化などのための、ソフトウェアシステムも用意しておく必要があります。

分散した物理的脅威に対処するテクニックを理解することによって、IT 管理者は、データセンター全体のセキュリティにおける危険な隙間を埋めて、データセンターの絶えず変化するインフラや可用性の目標値に見合った物理的セキュリティを維持することが可能になります。

謝辞

本書のオリジナルコンテンツを執筆した**クリスチャン・コーワン**と**クリス・ガスキンス**に深く感謝します。

参考資料

アイコンをクリックすると、直接リソースに移動します。

データセンタとサーバールームの動的な電力変動
ホワイトペーパー43

ネットワークセキュリティの基礎
ホワイトペーパー101

ホワイトペーパー一覧
whitepapers.apc.com

APC TradeOff Tools™一覧
tools.apc.com

お問い合わせ

このホワイトペーパーの内容についてのご意見やご感想、お問い合わせ先:

Data Center Science Center
DCSC@Schneider-Electric.com

製品やサービスに関する具体的なお問い合わせ先:

シュナイダーエレクトリック株式会社までお問い合わせください
TEL:03-5931-7500 FAX: 03-3455-2030 Email:jinfo@schneider-electric.com

© 2012 Schneider Electric. All rights reserved.