ホワイトペーパー

インテリジェントな監視による周辺保護

さまざまな業界で将来性に優れたセキュリティソリューションを確保するためのセンサーオプション、アプリケーション、および重要な考慮事項に関する考察

7月 2021

AXIS COMMUNICATIONS

目次

1 まとめ

フェンスは、多くの場合、サイト保護の「外層」の基本的な構成要素として使用され、人物と動物に対する障壁、遮蔽物、または抑止力として機能することができます。物理的な障壁は侵入を遅らせたり妨害したりすることしかできないため、他の機能を組み込むことでフェンスの効果を高めることができます。

フェンスと併用して、さまざまなタイプの検知器が使用されます。ケーブルベースの検知器はフェンスに沿って配置でき、レーダー (マイクロ波) センサー、赤外線バリア、またはレーザーを戦略的な場所に配置することができます。

すべてのタイプの検知器は、動物、揺れる植物や樹木、悪天候などによって誤報を引き起こす可能性があります。マイクロ波センサーを使用する際の周波数の干渉や、設置環境の物理的な制限など、他の制約要因も存在する可能性があります。

カメラは、広範な領域や複数の場所を監視したい場合に明確な利点を提供します。最新のネットワークビデオソリューションでは、カメラ内でのコンピューター処理と人工知能が組み合わされています。テクノロジーの固有の拡張性、有効性、および抑止力は、ビデオカメラが費用対効果に優れたセキュリティシステムの構成要素となる可能性を示します。

カメラと動体検知ソフトウェアは周辺保護の範囲と機能を拡張しましたが、これらのソリューションは、悪天候下では検知できないため、これにより制限される可能性があります。サーマルカメラは、適切にキャリブレートし、ビデオ分析機能と組み合わせることで、照明条件の影響を受けず、また、厳しい天候の影響をほとんど受けずに、効果的な監視を提供します。

ビデオ分析は時間とともに大幅に進化し、ホームセキュリティ市場向けのカメラでも一般的になっています。分析機能は、対象のアクティビティを含む映像のみを記録することにより、ストレージ要件を削減できます。大部分の録画映像をカメラ自体で処理することで、カメラからは関連映像だけがストリーミングされるため、ネットワークの負荷が大幅に削減されます。これは、管理室でのシナリオに明確な利点をもたらします。

他のセキュリティ対策と同様、周辺保護ソリューションの評価は適切かつ相応である必要があります。通例どおり、脅威は第一に考慮する必要があります。

セキュリティに関しては、ITや運用などの他部門からの見解や意見を含める集中型のアプローチが、急速にベストプラクティスになりつつあります。これには、エンジニアリングに対応する人々を、可能な限り早い段階で含める必要性が含まれます。

インシデントの防止を目的として設計されたセキュリティソリューションの投資収益率 (ROI) を明確にすることは、非常に困難です。これは主に、コストに対して測定する見込み収入 (収益) がないためです。疑わしい行動や侵入について担当者に警告するだけでなく、自動応答をトリガーできるソリューショなどでは、より具体的なROIを示すことが可能です。

2 はじめに

従来、電子周辺保護ソリューションは、警備の厳重な政府や商業施設、または非常に裕福な人の保護として使用されていました。テクノロジーの進歩、市場の競争の激化、それによるコスト削減により、より多くの人が比較的高度なソリューションを利用できるようになりました。

では、最新の周辺保護ソリューションは何で構成されているのでしょうか？どのようなテクノロジーが使用されていて、どのように安心と真の保護を提供できるのでしょうか？

このホワイトペーパーでは、現在利用可能なセンサーベースの境界保護ソリューションの選択肢を検証するとともに、ソリューションの背後にあるテクノロジーに関する洞察についてまとめています。

3 周辺保護ソリューション

3.1 物理的なソリューション

物理的なソリューションは、区画化によるサイト保護の「外層」の基本的な構成要素となることが多く、通常、溶接パネルまたはコンクリートパネルにワイヤーまたは溶接網を施した境界フェンスが使用されます。境界フェンスは多くの目的を果たしますが、主な目的の1つは、侵入の遅延や防止を図る物理的な障壁を作ることです。フェンスは抑止力としての役割を果たし、動物の侵入を防止します。よじ登り防止装置、指定車両アクセスルート、横断防止装置、フェンススクリーンなどの機能を組み込み、境界フェンスの効果を高めることもできます。

ただし、物理的な障壁は侵入を遅らせることしかできません。したがって、境界には、検証可能なリアルタイムアラート、位置データ、ターゲットの追跡、およびインシデント発生後の調査を目的とした証拠とデータのパッケージ化機能を提供できる、自動侵入検知テクノロジーも装備されている必要があります。

3.2 物理的な境界における侵入検知

境界の外側には、さまざまなタイプのケーブル「検知器」が使用されることが多くあります。こういったケーブルベースの検知器は通常、地面に埋められるか、フェンスに取り付けられます。直線である必要はなく、フェンスに沿って配置できます。また、コーナー周辺や**死角**もカバーできます。一部のサプライヤーは、自動検知ソリューションを備えたフェンスを提供しています。

その他の検知ソリューションと同様、ケーブルベースの検知器は「誤検知」と呼ばれる誤報を引き起こすことがあります。誤検知の一般的な原因には、動物、揺れる植物や樹木、悪天候などがあります。ケーブルベースのソリューションは、映像監視と組み合わせた場合に最善の機能を発揮します。ビデオは、侵入を検証するだけでなく、アラームの原因を確認するためにも使用できます。ケーブルベースのソリューションは、侵入自体のアラートしか提供できません。侵入者の数や、対応の準備に必要なその他の詳細に関する情報を提供することはできません。

3.3 その他の侵入検知センサー

レーダー (マイクロ波) センサー、赤外線バリア、レーザーなどのその他の侵入検知器は、敷地周辺の戦略的な場所に配置できます。ここでも、設置ルールに正確に従わなかった場合、誤検知や、距離と高さに関する検知機能の制限などの問題によって、これらのテクノロジーが制約を受ける可能性があります。

周辺保護におけるレーダーの使用は、他の電子機器を使用する環境では特に問題になる可能性があります。レーダーと電子機器は同じ周波数とスペクトルで動作する可能性があり、周波数を慎重に選択する、または出力を下げることで干渉を抑えられる場合がありますが、この場合、装置の有効範囲も阻害されます。

4 ビデオベースのソリューション

4.1 ビデオカメラのアプリケーション

過去に使用されていたスタンドアロン型のCCTVテクノロジーは、現在の高度なネットワークカメラソリューションとはあまり似ていません。最新のネットワークソリューションは、カメラ内でのコンピューター処理と人工知能を組み合わせることができます。ただし、この水準のテクノロジーが利用できるようになったのはごく最近で、まだ初期段階にあります。

カメラは、広範な領域や複数の場所を監視したい場合に明確な利点を提供します。テクノロジーの固有の拡張性、有効性、および抑止力は、ビデオカメラが費用対効果に優れたセキュリティシステムの構成要素となる可能性を示します。

地域の法律によっては、カメラテクノロジーを使用して物理的な境界線を越えて監視することで、監視バッファを追加し、オペレーターが応答する時間にゆとりを持たせられる可能性があります。ビデオ分析を活用したソリューションでは、設定ルールに従ってアラームをトリガーできます。たとえば、人がフェンスから50メートル以内に近づくとアラームが鳴り、同じ人が徘徊し続ける、または10メートル以内のゾーンに入るとより大きな音でアラームが鳴るというように設定が可能です。

4.2 サーマル映像監視ソリューション

ビデオ監視カメラと動体検知ソフトウェアを組み合わせることで、単純な検知から複雑な侵入分析へと、周辺保護ソリューションの範囲と機能が拡張されました。ただし、悪天候下では検知できないため、ビデオの有効性が大幅に制限されることがあります。

サーマルカメラテクノロジーの利用可能性の高まりにより、周辺監視での使用が注目されるようになりました。サーマル (またはサーモグラフィ) カメラは、適切にキャリブレートし、ビデオ分析機能と組み合わせることで、照明条件の影響を受けず、また、厳しい天候の影響をほとんど受けずに、効果的な監視を提供することができます。サーマルテクノロジーを使用するセンサーは、一般的な可視光カメラと比較して優れたコントラストを提供し、侵入検知機能が大幅に向上されるため、周辺保護に有益です。

サーマルセンサーは、車両や人物などの物体から放射される赤外線を使用して画像を生成します。十分な処理能力を備えた最新のサーマルカメラは、ビデオ分析機能と組み合わせると、さまざまなタイプの侵入ターゲットを区別し、あらかじめ設定された条件リストに基づいてオペレーターに警告することができます。このリストには、人物または車両の進行方向や速度が含まれる場合があります。これは、従来のカメラでも可能ですが、可視光を使用する必要があります。可視光カメラについては、次の項で説明します。

4.3 可視光カメラ

すべての標準的な可視光監視カメラは、画像の生成に自然光または追加照明のいずれかを必要とします。映像監視をサポートするための照明は、それ自体で専門分野であり、この重要な課題については別のドキュメントに掲載されています。ただし、標準のカメラには可視光が必要であるという、当たり前ながら重要なポイントを繰り返す必要があります。光はあらゆる環境で問題となる可能性があり、光の質が変化すると明確な影響があります。特にソリューションを指定する人々によって、必ずしも考慮または把握されないのが、天候の影響です。

サーマルカメラには利点がありますが、これは、サーマルカメラが可視光カメラの直接的な代替品であるべき、または代替品になり得るという意味では決してありません。これらの2つのテクノロジーは、同じソリューションに統合された場合に最善の機能を発揮します。従来のカメラは、サーマルカメラのように長距離にわたり物体を検知することはできません。しかし、サーマルカメラは、可視光カメラのように現場検証に使用可能な詳細部分を提供することはできません。多くの場合、この2つのテクノロジーは組み合わされ、サーマルカメラは検知によるアラームを、可視光カメラは証拠とターゲットの追跡という現場検証目的に関する利点を提供します。

4.4 ビデオコンテンツ分析機能

ネットワーク映像監視は、セキュリティ運用にかつてない基準をもたらしました。効果的な権限の階層は、理論的には無制限の利害関係者数の間で、管理されたビデオアクセス、配信、ストレージを可能にします。拡張性の水準を特に高める技術の進歩の1つは、ビデオ分析機能の採用です。

ビデオ分析機能は、特にIPカメラテクノロジーの開発により、時間とともに進化してきました。これは、ホームセキュリティ市場向けのカメラで証明できます。これらの多くには、ある一定の分析機能が組み込まれており、シーン内の動きの検知などを可能にします。クロスラインディテクション、物体の移動、さらには人数計測など、さまざまな追加機能がセットになってカメラに付属している場合があります。

ビデオ分析では、アクティビティを含む映像のみを録画することで、ストレージ容量の要件を取り除くことができます。また、大部分の録画映像をカメラ自体で処理することで(エッジインテリジェンス)、カメラからは関連映像だけがストリーミングされるため、ネットワークの負荷が大幅に削減されます。これは、管理室でのシナリオに明確な利点をもたらし、セキュリティオペレーターはアラートを受信したときに映像を検証するだけで済むため、セキュリティオペレーターと組織の運用における効率性が大幅に向上します。

ビデオ分析を実行するシステムアーキテクチャには、主に集中型と分散型の2つのカテゴリーがあります。集中アーキテクチャでは、ビデオおよびその他の情報はカメラとセンサーによって収集され、分析するために中央サーバーに送信されます。分散アーキテクチャでは、エッジデバイス (ネットワークカメラやビデオエンコーダ) 自体でビデオ処理や関連情報の抽出ができます。エッジで分析を実行することで、専用の分析サーバーが不要になります。また、圧縮は映像データを中央サーバーに転送する場合にのみ使用されるため、非圧縮ビデオフィードで分析を実行できるようになりました。その結果、費用対効果の高い柔軟なアーキテクチャが確立します。実際、必要な処理能力のために通常は少数のビデオストリームしか処理できなかった同じサーバーが、処理の大半がカメラで実行されることで、何百ものビデオストリームを処理できるようになりました。

4.4.1 処理速度とGPU

処理速度と容量の指数関数的な成長に関するゴードン・ムーアの正確な予測 (別名: ムーアの法則) は、一部の主要なテクノロジー企業によって近い将来減速すると予測されていますが、カメラのメーカーと開発者は、現在の能力の向上とサイズの縮小に基づき、処理能力の活用方法を変更することができます。

最近まで、処理能力の向上は、画質の改善、解像度の向上、ビデオ圧縮の効率化に活用されていました。しかし、当面の間、市場のこれまで以上に高い画像解像度を求める需要は、ほぼ頭打ちになっているようです。その結果、メーカーは現在、処理能力を使用して、エッジでかつてない水準のインテリジェンスを提供しています。多くの場合、これは、強力なサーバーベースのビデオ分析が、カメラでの処理による恩恵を受けられることを意味します。

最新プロセッサの小型で高速な特性により、カメラはGraphic Processing Unit (GPU) に対応し、並列処理機能を提供するとともに新しい機会と分析の可能性を開くことができます。この新機能によって、ソフトウェア開発者は、エッジベースモデルに既存の実証済みサーバーベース分析機能の新しいバージョンを提供することに焦点を切り替え、セキュリティや映像監視の枠を超えて価値を提供できる、よりインテリジェントなカメラの需要を促進できるようになりました。

4.4.2 深層学習と人工知能 (AI)

GPUはエッジでの分析性能の飛躍を実現しましたが、監視システムに適用できる、人数計測や占有率管理などの機能を提供する他のタイプのテクノロジーに対する需要が高まっています。AIと機械学習の発展により、ゲームチェンジャーとして実証されている深層学習処理装置 (DLPU) がカメラに統合されるようになりました。

DLPUは、深層学習分析の幅広いアプリケーション向け専用に設計されています。深層学習に基づく分析では、所定の物体一式の外観についてアルゴリズムが効率的に学習するため、検知と分類に優れた精度を提供できます。これは、境界線での侵入検知ソリューションを、ごく特定の物体とシナリオに対してのみアラートを発するよう設定できる、If-this-then-that (IFTTT) の進化型を意味します。

車両のリアバンパーなど、物体の一部しか見えない場合でも、システム分析システムはそれを認識して識別します。この記事の執筆時点で、さまざまな主張はあるものの、市場で最も実証されているソリューションは、人物と車種の識別と区別に限定されています。ただし、人が着用している衣服の色など、より詳細な識別が可能なカメラベースの分析モデルの用例は、試験が進んだ段階にあります。

こういったテクノロジーの進歩は、従業員、顧客、一般の人々、または潜在的な脅威を識別して区別できる、ターゲットを絞った検知システムにつながる可能性があります。セキュリティの観点から考えると、物理的セキュリティが適切に適用された環境における高度な分析は、犯罪を検知・防止するための一層効率的で正確なシステムを確実にもたらします。機能が次の段階に進化するのも、それほど先のことではないかもしれません。

5 コスト

5.1 投資利益率の評価と測定

他のセキュリティ対策と同様、脆弱性または復元力の観点から、周辺保護ソリューションの評価は適切かつ相応である必要があります。通例どおり、脅威は第一に考慮する必要があります。現代のほとんどの大規模な企業または政府の敷地にとって、脅威は偶発的な侵入者から抗議者、さらにはテロリストにまで及ぶ場合があります。

セキュリティに関しては、ITや運用などの他部門からの見解や意見を含める集中型のアプローチが、急速にベストプラクティスになりつつあります。これには、エンジニアリング要件に関する経験を持つ人々を、可能な限り早い段階で含める必要性が含まれます。適用する対策を検討する場合、周辺保護については歴史的に、潜在的な侵入者を阻止して遅延させるという従来型の手段から始めるのが適切であると考えられていました。しばらくして、セキュリティ設計者は「ボルトオン」技術的検知システムに移行しました。しかし、現在では多くの対策やシステムが相互に統合されているため、熟考した包括的なアプローチが必要となります。

インシデントの防止を目的として設計されたセキュリティソリューションの投資収益率 (ROI) を明確にすることは、非常に困難です。これは主に、コストに対して測定する見込み収入 (収

益) がないためです。通常、保安担当者は財務部門の担当者と協力して、資産の損失や破壊に関連する直接的なコストや、評判の喪失に関連する、直接的ではないが同様に損害を与えるコストなど、さまざまなタイプのセキュリティインシデントのコストを明らかにします。

ただし、特定の手動操作を削減したり、保安担当者を他のタスクに再配置したりできるテクノロジーを使用することで、より具体的なROIを提示することができます。例としては、疑わしい行動や侵入について担当者に警告するだけでなく、ソフトな応答を自動的にトリガーできるソリューションが挙げられます。これには、潜在的な侵入者に自身が検知されたことを通知し、そのエリアを離れるように指示するための、事前に録音されたアナウンスを再生できるIPオーディオシステムや、照明付きの標識などが含まれます。

監視カメラがソリューションに組み込まれている場合、キャプチャーされたナンバープレートや侵入者の画像などを画面に表示し、侵入者に識別データの証拠を見せることで、効果を高めることができます。こういった対策が望ましい結果をもたらさない場合にのみ、セキュリティチームを派遣して調査する、またはより直接的な対応を取る必要があります。アラートに対応するこの段階的なアプローチは、境界の外側での使用により適していると言えますが、保安担当者が早い段階で関与する必要性を最小限に抑え、工数を省くことで明確な利点がもたらされます。

5.2 コスト評価

コストの見積りは、総所有コスト (TCO) の計算に基づく必要があります。TCOには、ソリューションのライフサイクル全体にわたるすべてのコスト (材料費、人件費、調査費、システム設置費、運用費、メンテナンス費、廃棄費、リサイクル費) が含まれます。これには、資本を運用予算と資本支出予算の間で再配分する必要がある場合があるため、財務部門と調達部門によるアプローチの変更が必要になることがあります。

あらゆる有形資産と同様に、組織は境界線検知ソリューションの耐用年数を把握する必要があります。セキュリティマネージャーとITマネージャーは、将来のソリューションのプラットフォームとして適切なテクノロジーを調達することによってコストを節約できる仕組みを説明および実証することで、財務部門のスタッフをサポートできます。高度なインテリジェント監視デバイスの特徴は、本質的にある程度の将来性を備えていることです。つまり、適切な処理能力を備えたデバイスは、特にAIと機械学習に基づく処理分析を通じて、長期にわたり技術の進歩を繰り返し活用することができます。

6 アクシスコミュニケーションズの提案

Axisのパートナーソリューションとの統合を実現するオープンな取り組みにより、Axisのネットワーク化されたセンサーを実証済みのビデオ分析機能と組み合わせ、AIを活用することが可能です。これによりお客様は、企業全体で、システムの寿命期間全体にわたり、サイバーセキュアで費用対効果に優れた、パフォーマンスの高い統合周辺保護ソリューションを展開することができます。

サーマルセンサーが適切でないと考えられる場合は、サーマルテクノロジーと同様の利点を多数提供し、誤検知の低減が可能なマイクロ波テクノロジー (レーダー) が優れた代替手段となります。Axisのレーダーテクノロジーは、高度な監視カメラと同じ機械学習と深層学習の恩恵を受けています。Axisのレーダーユニットは、人物や車両を正確に検知、分類、追跡することができ、誤報率はほぼゼロです。

レーダーテクノロジーは24時間365日動作し、影や光線の動き、小動物や昆虫、悪天候などの一般的なトリガーの影響をほとんど受けません。これにより、費用対効果に優れた運用が実現し、保安担当者は実際の脅威に集中することができます。レーダーは物体の速

度に関する情報も提供できるため、シーン内の他の物体に接触する時間を正確に計算したり、速度制限違反を適用したりすることが可能です。

ソリューションのパフォーマンスは、情報提供依頼書 (RFI) や市場分析アンケートの最初に記載されている場合が少なくありません。Axisのカメラは、業界最高水準の容量を誇るAxis独自のARTPECプロセッサを備えているため、最先端の周辺保護ビデオ分析ソリューションをカメラ (エッジ) に組み込むことができます。重要なのは、これにより、ソリューションがサードパーティのコンポーネントではなく、Axis独自のテクノロジーの力を活用しているということを保証できる、ということです。

この「エッジインテリジェンス」は、複数のカメラが、異なる場所で同時に発生する複数のイベントを追跡できることを意味します。このいわゆる分散型テクニカルアーキテクチャにより、集中型サーバーテクノロジーに投資することなく、必要に応じてカメラを追加し、ソリューションを拡張できます。

英国政府承認済みのAXIS Perimeter Defender (APD) を使用すると、1人以上の人物または1台以上の車両について、次の4つのタイプのイベントが検知されます。

- 事前に設定された領域への侵入
- 事前に設定された順序および方向でのゾーン横断
- 条件付きのゾーン横断
- 徘徊者の存在

APDは、侵入アラームや対応するビデオ以上のものを提供することができます。ビデオにオーバーレイを表示するためのメタデータも提供し、境界と、移動する人物や車両の軌道を示します。より統合されたアプローチとして、Axisカメラ (可視光またはサーマル) をIPスピーカーと連動させ、スタンドアロンソリューションとして検知時に自動メッセージをブロードキャストすることも可能です。このタイプの自動警告は、侵入者の意図とその後の必要な対応を判断する上で重要な、対策の「エスカレーション (段階的な強化)」を可能にします。

APDはエンタープライズプラットフォーム (Genetec、Milestone、SeeTec、Prysm、Qognifyなど) で一般的に使用されるソフトウェアに直接統合することができます。

Axisは調査後の計画を支援する補助設計ツールを提供し、特定の基準に基づいた適切な製品の選択からストレージ容量の正確な計算、テクノロジーのインストール、システム管理まで、プロジェクトのあらゆる段階でサポートします。Axisツールを活用することで、コンサルタントは計画と見積りを行い、インテグレーターはプロジェクトをよりスムーズかつ効率的に管理できるようになります。さらに、これらのツールを使用することで、付属のソフトウェアの更新やセキュリティパッチのインストールが容易になり、設置済みシステムの安全性を保証しやすくなります。

脅威と対策が進化する中、1つの重要な事項、境界の完全性とセキュリティは一定に保たれます。周辺保護は、スタッフ、訪問者、一般の人々に安全な環境を提供するという組織の義務を遂行する人々にとって、基本的な考慮事項です。このホワイトペーパーは、周辺保護を計画する際に、テクノロジーの統合による取り組みが組織にもたらす利点を強化することを目的としています。また、セキュリティテクノロジーへの投資は、実証可能なROIによって裏付けられるべきであるという事実を強調しています。どんな場合でも、現在利用可能なテクノロジーの機能を理解し、今後のトレンドを理解することは、部門、役職、業界を問わず、あらゆるセキュリティ担当者にとって理にかなった運用セキュリティであり、調達アプローチです。

製品に関する参照情報

IPサーマルカメラ:

AXIS Q19など https://www.axis.com/ja-jp/products/thermal-cameras

分析ソフトウェア:

AXIS Perimeter Defender

https://www.axis.com/ja-jp/products/axis-perimeter-defender

外部IPスピーカー:

AXIS C1310-E https://www.axis.com/ja-jp/products/axis-c1310-e

IPセキュリティレーダー:

D2110-VE https://www.axis.com/ja-jp/products/axis-d2110-ve

T10169467/ja/M1.3/2107

Axis Communicationsについて

Axisはセキュリティとビジネスパフォーマンスを向上させるソリューションを生み出すことで、 よりスマートで安全な世界の実現を目指しています。 ネットワークテクノロジー企業として、 また業界のリーダーとして、Axisはビデオ監視、 アクセスコントロール、インターコム、音声システムなどのソリューションを提供しています。 これらのソリューションは インテリジェントな分析アプリケーションによって強化され、高品質のトレーニングに支えられています。

Axisは50ヶ国以上に約4,000人の熱意にあふれた従業員を擁し、 世界中のテクノロジーおよびシステムインテグレーションパートナーと連携することで、 カスタマーソリューションをお届けしています。 Axisは1984年に設立され、本社は スウェーデンのルンドにあります。