ホワイトペーパー

インテリジェント映像監視による空港の周辺保護

提供されるサービスと投資利益率に関する考察

7月 2021

目次

1 まとめ

従来の空港周辺保護では、境界を定め、侵入を防ぐフェンスや壁が使用されています。境界には、監視ステーションにアラームを送信する侵入検知も装備されている必要があります。境界とその周辺の検知に利用可能なソリューションには、ケーブル検知器、マイクロ波センサー、赤外線トリップワイヤーなどがあります。これらは役に立ちますが、どれも確実ではありません。問題の1つは検知漏れです。また、同様に厄介なのが誤検知で、長期的には重大なインシデントが完全に無視される可能性があります。

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を拡張することができます。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。

近年、サーマルセンサー技術は大幅に向上し、関連コストは減少しています。ビデオ分析ソフトウェアと組み合わせたサーマルカメラは、照明条件や時間を問わず、いつでもエリアを保護できます。サーマルテクノロジーは、大規模な監視システムに必要な優れた検知機能を提供するため、空港の監視に適していることが多いです。

サーマルテクノロジーを使用できない場合は、多数の同様の利点を提供する、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のレーダーはターゲットを区別し、PTZカメラと統合することでターゲットを効果的に追跡することができます。このテクノロジーは24時間365日、誤検知を最小限に抑え、調査コストの削減によって節約を可能にし、実際の脅威に集中できる小規模なセキュリティチームを実現します。

周辺保護ソリューションの評価は、適切かつ妥当である必要があります。脅威への対処は常に重要な考慮事項ですが、同時にシステムがすべての法的要件に準拠している必要があります。

セキュリティソリューションの投資利益率を明確にすることは、コストに対して測定する収益がないため、一般的には困難です。ただし、手動による介入の必要性を低減するテクノロジーを使用すると、より具体的な結果を得ることができます。カメラを使用して、侵入者に自分の識別データが記録されていることを画面に表示することなどによって、効率性を上げることもできます。

Axisカメラは、画像、ハードウェア接続性、圧縮率の向上を可能にする高度な機能を備えています。また、Axis独自のARTPECプロセッサを備えているため、周辺保護ビデオ分析ソリューションをエッジに組み込むことができます。この分散型技術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することができます。

2 はじめに

重要なサイトのセキュリティは、設計と保護という2つの柱に依存します。一般的に空港は国の重要なインフラ施設の一部と見なされており、物理的な障壁、侵入検知、アクセスコントロール、モバイルセキュリティパトロールが組み込まれた階層構造型アプローチの一部として、適切なセキュリティソリューションを展開し、侵入リスクを制限する必要があります。

もちろん、空港の立入制限区域の保護に使用される対策には、脅威と運用要件の両方、特に航空**地役権**、地形のトポグラフィー、特定の気候条件、および環境上の制約を考慮する必要があります。このホワイトペーパーは、空港保護における現在の選択肢の一部を説明し、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を提供することを目的としています。

3 従来の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。電波航法や通信機器の近くでは、非磁性のフェンスが使用されます。これらのフェンスは多目的で、空港の境界を明確に定義しつつ、人や動物による侵入を防止することもできます。よじ登り防止装置、車両アクセスルート、横断防止装置、基礎、フェンススクリーンなどの機能も追加できます。

セキュリティを強化するため、境界には自動侵入検知ソリューションを装備する必要があります。これは、違反が発生した場合に監視ステーションにアラームを送信し、詳細な調査を可能にします。

3.2 フェンスやゲートでの侵入検知

長い境界線に利用可能なさまざまなタイプのケーブル「検知器」があり、これらはリアルタイムのアラームをセキュリティオペレーターにリダイレクトします。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。

ただし、これらのソリューションは確実ではなく、「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。映像監視がない場合、アラームの原因を確認する唯一の方法は、担当者を派遣して調査することです。誤検知が繰り返されると、スタッフの間に無関心が生じ、アラートが無視され、最終的に実際の脅威が見落とされる可能性があります。

3.3 フェンス外の侵入検知器

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、空港の敷地周辺の戦略的な場所に配置されます。ここでも、設置ルールに厳密に従わなかった場合、誤検知や、距離と高さに対する検知機能の制限などの問題によって、これらの侵入検知器が制約を受ける可能性があります。周辺保護でのレーダー (マイクロ波) の使用は、航空環境で特に問題になる可能性があります。これは、装置が同じスペクトル上にある既存のテクノロジーと干渉するためで、この理由のみで排除されることがあります。これらの装置によって生じる潜在的な問題は、周波数を慎重に選択し、装置の出力を制限する、つまり有効範囲を制限することによって、ほとんど排除することができます。

4 空港周辺保護の課題への取り組み

4.1 新しいインテリジェント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を拡張することができます。

一例として、サーマル (またはサーモグラフィ) カメラがあります。サーマルカメラは、ビデオ分析ソフトウェアと組み合わせることで、照明条件や時間を問わず、いつでもエリア

を保護できます。サーマルテクノロジーを使用したセンサーは、大規模な監視システムに必要な優れた検知機能を発揮するため、空港の監視に適している場合が多くあります。

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。非常に過酷な気象条件以外には影響を受けず、24時間体制で長距離の検知が可能です。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物体を区別し、条件リストの一覧 (方向/速度/人物/車両を含む) に基づいてオペレーターに警告することができます。これは、従来のカメラでも可能ですが、赤外線ではなく可視光に依存するため、固有の明らかな制限があります。

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。ビデオ分析機能を使用する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トリガーされ、同じ人が10メートル以内に近づく、または指定されたゾーンで特定の設定時間を超えて徘徊すると、アラームレベルが高くなるというように設定できます。

近年、サーマルセンサー技術は大幅に向上し、関連コストは減少しています。カメラテクノロジーとして、サーマルソリューションが境界侵入検知に選択されることが多い理由は、あらゆる照明条件下や悪天候条件下で効果的な長距離監視を提供するサーマルベースのソリューションと、競争力のある価格設定の組み合わせによるものです。

5 コストと提供されるサービス

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、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、つまり今日の国際空港では抗議者やテロリストなどを第一に考慮する必要がありますが、同時に、システムが関連するコンプライアンス要件に準拠している必要があります。

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。さらに、広い立入制限区域がある空港では特に、エンジニアリング要件に携わる人々を可能な限り早い段階で含める必要があります。歴史的に周辺保護については、潜在的な侵入者を抑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「ボルトオン」技術的検知システムに移行しましたが、現在では多くの対策やシステムが統合されているため、より考慮された包括的なアプローチが早い段階で必要になります。

セキュリティソリューションの投資利益率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/損害に関連する直接的なコストや、会社やブランドの評判の喪失に関連する、目立ちにく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、特に手動による介入の必要性を削減したり、人材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、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アナウンスの再生や標識の点滅など、「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。

ソリューションにカメラが組み込まれている場合、たとえば、画面を使用して車両のナンバープレートを表示する、または侵入者自身の画像を表示して、侵入者に識別データが記録されていることを示すことで、効率性を高めることができます。こういった予備対策が望ましい効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ためのこの段階的アプローチは、境界の外側での使用により適していると言えますが、保安担当者が関与する必要性を最小限に抑え、リソースの労力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異なるアプローチが必要になることがあります。

6 アクシスコミュニケーションズの提案

パートナーソリューションとの統合を可能にするAxisのオープンなアプローチにより、Axisのサーマルネットワークカメラを実証済みビデオ分析機能と組み合わせ、空港がシステムの寿命全体を通してサイバーセキュアで費用対効果に優れ、パフォーマンスの高い一体型周辺保護ソリューションを展開できるようになります。

サーマルセンサーがあまり効果的でないと考えられる特定のエリアでは、サーマルテクノロジーと同様の利点を多数提供する、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、人間と車両の区別、速度と方向に関する情報の提供、PTZカメラとの統合によるターゲットの効果的な追跡が可能で、境界だけでなく、階層構造のセキュリティソリューションのあらゆる部分に適しています。サーマルテクノロジー同様、レーダーテクノロジーは、影、照明の変化、小動物、雨滴、昆虫、風、悪天候などの一般的なトリガーの影響を受けにくいため、誤検知を最小限に抑えて24時間365日動作します。誤検知を抑えることで、不必要な調査コストの削減と実際の脅威に集中できるセキュリティチームの縮小が可能になり、徐々にコストが削減されます。

技術レベルで言うと、カメラには次のような高度な機能が搭載されています:低振幅と高振幅の動きを管理する電子動体ブレ補正 (EIS)、外部ハードウェアを接続するための複数のアラーム入出力ポート、帯域幅とストレージの要件に合わせた高度な圧縮機能 (Zipstream)。

Axisカメラには、業界最高水準の能力を誇るAxis独自のARTPECプロセッサも搭載されており、周辺保護ビデオ分析ソリューションを組み込むことができます。したがって、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することができます。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。

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

Axisサーマルカメラは IPスピーカーとも連動し、検知すると自動メッセージを再生して侵入を試みる人物に警告します。

上記のAxisテクノロジーは、空港プラットフォーム (Genetec、Milestone、SeeTec、Prysm 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。

高度な周辺保護ソリューションを実現するために必要な設備を決定し、設置コストを明確にするには、机上での検証と実地調査、両方が必要です。Axisは、ソリューションを計画、設計、設置、管理するための設計ツールを提供することで、インテグレーターをサポートします。

Axisの設計ツールは無料で利用でき、特定の基準に基づいた適切な製品の選択から、サイト計画、システムの設置と管理まで、プロジェクトのあらゆる段階でサポートします。インテグレーターは、Axisツールを活用することで、プロジェクトをよりスムーズかつ効率的に実行できます。

これらのツールにより、インテグレーターは適切な製品を選択し、特定の仕様に合わせた見積りや推奨事項に基づいて最適化されたシステムを計画して、最適なソリューションを迅速に提供することができます。さらに、ツールによって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、インテグレーターが提供するシステムの安全性を維持しやすくなります。

7 製品に関する参照情報

IPサーマルカメラ: AXIS Q19シリーズ

https://www.axis.com/ja-jp/products/axis-q19-series

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 C3003-E Network Horn Speaker

https://www.axis.com/ja-jp/products/axis-c3003-e/support

IPレーダー

https://www.axis.com/ja-jp/products/axis-d2050-ve-network-radar-detector/support

T10168973/ja/M1.4/2107

Axis Communicationsについて

Axisは、セキュリティの向上とビジネスの新しい推進方法に関する洞察を提供するネットワークソリューションを生み出すことで、よりスマートでより安全な世界の実現を目指しています。 ネットワークビデオ業界をけん引するリーダーとして、Axisはビデオ監視および分析機能、アクセスコントロール、インターコムおよび音声システムなどに関連する製品とサービスを提供しています。 Axisは50ヶ国以上に3,800人を超える熱意にあふれた従業員を擁し、世界中の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年に創業し、スウェーデン・ルンドに本社を構えています。

Axisの詳細については、弊社Webサイト *axis.comをご覧ください.*