ホワイトペーパー

証拠としての映像データ

AXIS Camera Stationによる映像データの完全性の確保

7月 2021

目次

1 まとめ

高画質で信頼性が高く、改ざんされていない映像データは、証拠として使用することができます。AXIS Camera Stationを使用して、映像データを証拠として処理するためのベストプラクティス:

- システムを適切に設計、設定、検証し、必要な画像、録画、およびセキュリティを提供する
- 定期メンテナンスを実施する
- 設定された手順に従って証拠を処理する

2 はじめに

監視ビデオは、法廷で証拠として使用できるよう、実用的にカスタマイズされています。では、「テープに」録画されたイベントは、拒否されないのでしょうか？それとも拒否される可能性はあるのでしょうか？裁判官は、高画質で信頼性が高く、改ざんされていない映像データは受け入れるでしょう。

しかし、映像の証拠価値が不注意によって低下する場合もあります。たとえば、人物や車両が突然消えたり画像内で「ジャンプ」したりする、時間的なずれのある監視映像は、証拠として使用するには信頼性が不十分であると見なされる場合があります。映像は、タイムスタンプやカメラのMACアドレスなどのメタデータのつじつまが合わない場合にも疑問視される可能性があります。映像が編集、削除、または改ざんされた疑いがある場合、映像の所有者の信頼性が低下する可能性があります。

このホワイトペーパーでは、映像を証拠として管理する方法についてアドバイスしています。具体的には、証拠書類作成におけるビデオ管理ソフトウェア (VMS)、AXIS Camera Stationと、映像所有者の役割について説明します。

Figure 1. 戦略的な場所における映像監視は、適切に設定・管理されていれば、貴重な証拠を提供することができます。

3 証拠としての映像データの処理に関するベストプラクティス

映像監視を使用する企業や組織では、映像データの処理方法と保存方法を決定するプロセスと手順が設定されている必要があります。いずれかのカメラがインシデントをとらえた場合に備え、映像が上書き、改ざん、盗難などから保護されていることを確認する必要があります。また、映像を安全にエクスポートして保管し、法執行機関に提出できる必要があります。

しかし、高品質映像の証拠を作成するプロセスは、目的に基づいた映像監視システムの設計から始まります。また、システムを最新の状態に保ち、不規則性を把握することも非常に重要です。この章では、このプロセスの手順と、AXIS Camera Stationとそのツールボックス、AXIS Camera Station Integrator Suiteを使用して手順を実行する方法について説明します。

システム設計、システムメンテナンス、およびインシデントの処理に関するこれらの原則に従って監視映像を作成することで、現在のサイバーセキュリティ要件に準拠し、必要に応じて証拠としての価値を提供できる可能性が高まります。

Figure 2. AXIS Camera Stationソフトウェアは、映像監視システムのセットアップ、日常の運用、戦略的管理を容易にします。

3.1 システムを適切に設計する

映像監視システムは、慎重に設計する必要があります。ニーズに応じて機器を選択し、必要な画像、録画タイプ、セキュリティを提供できるよう設定します。AXIS Site Designerは、こういった目的を達成するために重要なサポートを提供します。

3.1.1 必要な画像を提供するには

画質はカメラとその配置に依存します。カメラのモデル、レンズ、カメラから撮影シーンまでの距離と角度がわかっている場合は、画像の解像度、より具体的に言うと、イベントシーンの全幅のピクセル密度を計算することができます。撮影シーン内にいる人物の顔の全幅に適切なピクセル密度を確保するには、カメラの台数を増やすか、解像度の高いカメラを使用することが必要になる場合があります。実際の監視サイトにおける特定のカメラの視野や照明要件などのパラメーターを確認する必要があります。これはすべて、AXIS Site Designerでスムーズに設計することができます。

3.1.2 必要な録画を提供するには

録画には、冗長性を備えたパフォーマンスの高い検証済みハードウェアを使用する必要があります。システムの信頼性を高めるため、AXIS Camera Stationは、ネットワークカメラのSDカードに画像を一時的に保存する、フェイルオーバー録画をサポートしています。

VMD (ビデオ動体検知) 分析を使用する場合は、録画がインシデント全体の検証において価値を提供できるよう、十分な録画時間を確保します。最適にキャリブレートされていない動体検知録画は、時間的なずれや、つながりのない映像を生じさせる場合があります。多くの場合は連続録画の方が適していますが、より多くのストレージを要するだけでなく、十分な帯域幅を常時利用できる必要があります。

3.1.3 必要なセキュリティを提供するには

不正アクセスを防止するために必要な、物理的セキュリティをシステムに提供する必要があります。カメラ、ネットワーク機器、ネットワークケーブル、サーバー、データストレージ、電源装置、電源ケーブルなど、すべてのハードウェア要素を保護する必要があります。セキュリティ対策には、サーバールームのアクセスを制限する、サーバーキャビネットをロックする、サーバーをキャビネットに収納する、サーバーの物理ポートを無効にする、ネットワークケーブルを露出させないようにするなどがあります。

また、データの悪用、データの改ざん、悪意のある攻撃のリスクを最小限に抑えるために必要なサイバーセキュリティをシステムに提供するよう努める必要があります。いわゆるハードニング (強化) は、システムが現在のセキュリティ基準を満たしていることを保証するソフトウェアツールとテクノロジーによって、部分的に提供することができます。ただし、ハードニングを行うには、システムの所有者がサイバーセキュリティの理念を適用し、組織内にそれを浸透させるために積極的に取り組む必要もあります。たとえば、システムのすべてのユーザーは、強力で推測の困難なパスワードを使用することの重要性を認識し、パスワードを公開しないように注意する必要があります。また、「最小特権のユーザーアカウント」などの使用により、ユーザーアクセスとユーザー権限を最小限に抑える必要があります。システムの所有者は、スタッフにベストプラクティスに関する情報を提供し、ベストプラクティスが確実に展開されるようにする責任があります。認定インテグレーターはシステムの強化を図ることができますが、一部のサイバーセキュリティ対策は、システムユーザーの積極的な協力がなければ効果を発揮しません。

全体的なサイバーセキュリティの向上を実現するために重要な方法の1つは、暗号化されたデータ転送を使用して映像を保護することです。クライアントとサーバー間のデータ転送において、AXIS Camera Stationは、映像、音声、メタデータにAES暗号化を、その他のデータにはTLS 1.2暗号化を使用します。AXIS Camera Stationは、HTTPSを介して、カメラとサーバー間のデータストリームを暗号化するように設定することもできます。ソフトウェアを保護するためのその他のベストプラクティスとしては、使用されていないサービスの無効化、IP/MACアドレスフィルタリングの使用、IEEE 802.1Xへの対応、SNMPモニタリングへの対応、信頼性の高いNTPサーバーを使用した正確な日時の設定 (映像メタデータのタイムスタンプの正確性を確保するため)、リモート接続に (ポート転送やリモートデスクトップではなく) Axis Secure Remote Accessのみを使用することなどが挙げられます。サイバーセキュリティの対策と推奨事項について詳しくは、Axisサイバーセキュリティ強化ガイド (Hardening Guide) をご覧ください。

3.1.4 システムを設定して検証する

AXIS Site Designerを使用してシステムを設計する際に、カメラ名、解像度、保持時間を指定し、システムの主要部分を設定することができます。システムの設計と設置を完了したら、AXIS Site Designerで設定した構成をAXIS Camera Stationに自動的にインポートし、必要に応じて設定を微調整することができます。

実際の設置が完了したら、AXIS Camera Station Integrator Suiteの一部であるAXIS Installation Verifierを使用して、システムを検証できます。AXIS Installation Verifierは、システムを通常モードとナイトモードでテストし、ノイズレベルが高く、より多くのネットワーク帯域幅を必要とする低光量環境下での動作時に十分な帯域幅があることを確認します。次に、

ストレステストを実行し、最初のボトルネックが見つかるまで、システムで生成されるデータ量を徐々に増やします。これにより、システムの予備容量が明らかになり、システムの改善が必要かどうかがわかります。

3.2 定期メンテナンスを実施する

システムが稼働しているときは、システムの監視と更新を継続的に行う必要があります。

ハードウェアとソフトウェアが、常に正常に機能していることを確認してください。画質を点検し、スケジュールに従ってカメラレンズを清掃し、物理的な改ざんがないこと、カメラの視野と向きが本来の状態に保たれていることを確認します。システムログは、ログイン、接続、およびデバイスの問題に関する情報を提供するため、定期的に確認します。AXIS Camera Stationは、発見された多くの異常を通知し、システムログに記録します。特に重要なインシデントが発生した後は、ログを読み取り専用のリモートストレージに転送します。Axisは、Integrator Suiteの一部としてオンラインシステムヘルスモニタリングも提供しています。これにより、すべてのシステムを監視し、容易なサービスとメンテナンスを可能にするシステムステータスを確認することができます。

ハードウェアとソフトウェア (オペレーティングシステムとVMS) は、定期的に更新する必要があります。常に最新バージョンのソフトウェアとファームウェアを使用することにより、システムは最新のセキュリティパッチとバグ修正による利点を得ることができます。VMSがすべてのソフトウェアとファームウェアの更新を自動的に検出し、更新のインストールを促すか、自動的に更新できることが理想的です。ダウンロードするソフトウェアはすべて、信頼できるソースから入手する必要があります。

3.3 設定された手順に従って証拠を処理する

監視システムの設計とメンテナンスに関する原則が適切に適用されていれば、AXIS Camera Stationは、カメラがキャプチャーしたインシデントの信頼性の高い証拠を提供することができます。次に、手続きを進めるための手順を設定しておく必要があります。

法執行機関の指示に従う必要があります。重大な犯罪が発生した場合、法執行機関は証拠を保護する方法を決定でき、人々はその指示に従う必要があります。

その他の場合の主なプロセスは、証拠を安全にエクスポートすることです。つまり、システムの外部でも、内部と同様の信頼性を維持し、改ざんされていない形式で証拠を提供できるようにします。

エクスポートは、指定されたオペレーターが、できれば証人と一緒に処理します。このオペレーターには、信頼性の高いエクスポートを提供して文書化する目的でのみ雇用された、外部の専門家を使用することができます。エクスポートに独立したサードパーティを使用することで、映像所有者が証拠を改ざんした疑いを受けるリスクを最小限に抑えることができます。オペレーターは、実際のインシデントを含むだけでなく、その原因となったイベントや発生後の状況についての十分な情報も提供できる映像をエクスポートする必要があります。

選択したビデオクリップは、CD-R、DVD-R、Blu-ray (-R) などの読み取り専用ディスクにエクスポートして、法執行機関に渡すことができます。別の方法としては、暗号化とパスワード保護を使用して、ビデオクリップをzipファイルにエクスポートします。このファイルは、ユーザーのパスワードでハッシュ化した署名を使用してデジタル署名することができます。ハッシュを確認し、ファイルの現在のハッシュと照合するには、署名をAXIS File Playerに入力する必要があります。ハッシュが一致する場合、そのファイルのデータは変更されていません。

Axisでは、オペレーター向けの高度なエクスポートツールとして機能する、AXIS Camera Station Incident Reportも提供しています。このツールは、インシデントタグやエクスポート場所などのデータを提供する管理者が、事前に設定する必要があります。これにより、Incident Reportはエクスポートを自動化し、タグをフォルダ名として使用して、インシデントに従って編成された映像をエクスポートできるようになります。エクスポート場所は、ローカルリソース (NAS (Network Attached Storage) など) や、リモートリソース (SMB プロトコル経由でアクセスできる場合はクラウドストレージなど) に設定できます。レポートは、ビデオファイル、.jpg形式のスナップショット (オペレーターがレポートを作成する際にAXIS Camera Stationで手動作成)、. txt形式のブックマーク、および.pdf形式のレポートに集約されたすべての情報で構成されます。

4 サイバーセキュリティリソース

Axisは、デバイスの設計/開発/テストにサイバー強化を適用することにより、攻撃時に悪用される可能性のある脆弱性のリスクを最小限に抑えます。セキュリティの脆弱性の管理、安全なデータの送信と保存の要件、暗号化など、サイバーセキュリティにおける業界のベストプラクティスに従います。適切なセキュリティ管理を簡単にコスト効率よく適用できるよう取り組んでおり、Axisのデバイスは暗号化とセキュリティ管理に対応しています。

Axisは、システムのメーカーおよびプロバイダーとして、包括的かつ安全なシステムやソリューションを提供するために最善を尽くしていますが、エンドユーザーにも、セキュリティのベストプラクティスを適用するという大きな責任があります。Axisでは、エンドユーザーをサポートする、さまざまなツール、ガイド、およびチュートリアルを提供しています。強化ガイド、セキュリティ管理情報、サイバーセキュリティに関するブログ投稿などを確認できる、www.axis.com/cybersecurityをご覧ください。

T10169774/ja/M1.2/2107

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。