

NVR、サーバ、クラウドの映像管理システムに必要な様々な IT 専門知識

イーグルアイネットワークス社創業者兼CEO ディーン・ドレイコ

コストと製品機能。この2点が多くの場合、監視カメラとその映像管理システム・ソフトウェア、映像記録用サーバ、そしてNVR(ネットワークビデオレコーダ)を購入する際の決定要因となります。ただし、3点目として考慮すべき非常に重要な要因があります。それは、記録機器を構築する上で必要とされるIT専門知識のレベルの高さです。

通常、セキュリティ監視カメラとその記録機器(サーバ、コンピュータまたはNVR)の購入者が製品を選択する際に、コストとその製品の機能性を見て検討します。特筆すべきもう一点が、記録機器を構築する上で必要なIT専門知識の豊富さです。システムのサイバー・セキュリティも確立する必要があります。

なぜITの専門知識が必要か?

アナログカメラを映像監視に使用していた時は、ITの専門知識は必要ありませんでした。各カメラのケーブルは、セキュリティカメラとVCR(映像カセットレコーダ)の背面にある入力端子口に接続していました。ネットワークは関係ありませんでした。しかし今では、カメラとレコーダは高度なネットワーク機器です。そのため必要となってくるIT専門知識の内容は、カメラ台数と記録装置の種類によって異なってきます。

それぞれのシステムに必要なIT専門知識は異なりますが、セキュリティ映像記録には次の3つの方法があります。

1. NVR
2. サーバ・ベースのネットワーク映像記録システム(オンプレミス)
3. クラウド・ベースの映像記録システム

NVR

NVRは、機能と構成が固定されたコンピュータ機器です。もし修正すると製品保証が無効になります。NVRは、一定数のカメラ台数に基づいて「平均」使用のために設計および製造されています。そのため、まず画像解像度とフレーム・レートに関する各カメラの映像品質要件を満たすためのセキュリティの専門知識が必要となります。次に、特定のNVRメーカーのモデルが、各カメラに求められている映像品質のカメラ台数を処理できるかどうかを判断するには、ITの専門知識が必要となってきます。

NVRの設計を評価するのにも、ITの専門知識が不可欠です。例えば、多くのエントリレベルのNVRは、RAID HDD(ハード・ディスク・ドライブ)の冗長性を有していません。最新のNVRは最新の大容量HDDを使用するため、1個のHDDが故障すると、記録された映像データの半分または全てが失われます。しかも故障したHDDを交換するまで、映像を記録することができません。

また、NVRのネットワークカードの品質とスループット容量も確認する必要があります。特にNVRで映像解析を処理する場合は、NVRのマザーボードも評価する必要があります。マザーボードには、カメラの映像ストリームをデコーディングするための独立したグラフィックス・プロセッシング・ユニット(GPU)チップが含まれていますか?映像管理ソフトウェアは、GPUプロセッサ機能を最大限に活用していますか?多くのNVRは、特に映像解析が関係する場合、顧客が期待する高解像度と映像フレーム・レートを処理できません。

NVRのオペレーティング・システムを含め、映像システムのサイバー・セキュリティ保護を確立するには、ITの専門知識が不可欠です。ほとんどのNVRメーカーは、デフォルトでサイバー・セキュア構成を有効にしています。一部のNVRには、修正できないほどの重大なサイバー・セキュリティの脆弱性が存在します。また、大部分のNVRはデュアル・ファクタ認証をサポートしていません。例えば、NVRのソフトウェアにアクセスするための従来のログオン名とパスワードに加えて、クレデンシャル・カードまたはテキスト・メッセージとして送信されたコードの使用などです。

したがって、ITの専門知識を持つユーザがNVRを評価するように求められた場合、代わりにNVRではなくサーバ・ベースの記録映像を推奨することがよくあります。サーバ・ベースの記録により、顧客は記録映像サーバの構成を決定できるため、顧客の映像処理およびサイバー・セキュリティの要件に正しく適合させることができます。



サーバ・ベースのセキュリティ映像記録

サーバ・ベースの映像記録には、最高レベルのIT専門知識が必要とされます。その理由の1つは、サーバの構成が異なる市販サーバを様々なシステムで利用できるからです。ほとんどの汎用サーバは、平均使用・ビジネス用途向けに設計されています。映像システムには独特な要件があり、高性能映像システムを設計するには、映像システムの動作をよく理解する必要があります。

例えば、単一の大容量ドライブを使用するのではなく、RAIDの冗長性を利用して、複数の小型HDDで構成されるストレージ・システムを設計する方が適切です。RAIDで大容量ドライブを再構成するには、小さなドライブを再構成することよりも時間がかかります。交換ドライブが再構成されるまで、記録性能が大幅に低下します。

また、一般的に必要とされるよりも高い性能を発揮できるサーバを設計することが求められます。したがって、サーバは、RAIDの再構成時にもピーク時のトラフィックをサポートするように構成する必要があります。これらには複雑な計算が求められます。

カメラ台数が多い案件では、高性能サーバが必須となります。おそらく多くの場合、複数のサーバが必要となります。それぞれが8、10、12、または20コアの複数のCPUを使用することにより、映像処理のボトルネックになるCPUの問題を排除できます。1ギガビットまたは10ギガビット・ポートなどの複数の高速ネットワーク・ポートを使用し、帯域幅を集約することにより、サーバのネットワーク・ポートが映像入力のボトルネックにならないようにすることができます。

さらに、サーバを仮想化するため例えばVMwareを使用して、ハードウェア資源をリソース・プールに集約し、2つの仮想マシンとして共有することで、それぞれがVMS記録アプリケーションを実行します。それにより、CPU、GPU、RAM、ストレージ資源の大規模な仮想化プールを備えた大容量高速サーバを構築することができ、多くの映像ストリームの処理とその映像解析処理計算の必要に応じて共有することができます。

ストレージ資源は、2台か3台、またはそれ以上のHDDの同時損失が起きても、記録を続けるように設計されています。そして、予備のHDDは電源を落とさず、



自動的に交換可能です。

このようなサーバは、映像ストリーム・トラフィックでの最悪レベルに対応できるように設計されています。例えば、絶え間なく降り続く雨のため、常時全ての屋外カメラが動体検知記録してしまう場合です。このようなサーバは、最悪の場合に備えた映像ストリーム量と映像処理のニーズに十分なリソースが利用できるように、サイズをハイスペックにしておく必要があります。これにより、ハードウェアと電気の費用の両方を上げ、更に強力なサイバー・セキュリティのコストを追加する必要があります。サーバ、仮想化、ストレージ、データベース、ネットワーク、およびサイバー・セキュリティに関する高度な専門知識を持つIT部門は、このタイプの高性能システムを設計および維持することはできます。

ただし、初期および継続的なITと高性能機器のコストは、システムの総所有コストを大幅に上昇させます。これが、サーバ・ベースのシステムのセキュリティ映像処理機能を妥協させる主な理由です。高性能システムの作成と保守の費用は許容できません。これで合理的なコストで高性能を得るために、多くの顧客がクラウドベースの映像システムを現在検討している理由が容易に理解できるでしょう。

クラウド・ベースの映像管理システム

クラウド・コンピューティングは、高性能で可用性の高いコンピューティングを安価な値段で提供できるように設計されました。数千または数百万の顧客が、コンピューティング基盤の費用と、それに必要なITおよびサイバー・セキュリティの専門知識を共有しています。クラウド・コンピューティングの鍵となる強みがこれを可能にしています。これらは、国際標準ISO / IEC 17788: 2014で定義されており、クラウド VMSに適用されるときに以下の通り要約されます。

クラウドの主な特徴

広範なネットワーク・アクセス

クラウドVMSはネットワーク経由で利用でき、標準のインターネット・ブラウザを介してアクセスできます。ユーザは、携帯電話、タブレット、ラップトップ、ワークステーションなどの様々な機器を使用して、ネットワークにアクセスできるならば、どんな場所からでもVMSにアクセスし、作業できます。

測定されたサービス

クラウドVMSの顧客には、使用した分のみの料金をお支払いいただきます。例えば、特別な会社のイベントのためだけに映像解析を使用する場合、使用するサブスクリプション期間(通常

は1か月)のみをお支払いいただきます。

マルチ・テナント

1つのVMS顧客のアカウントで、複数の顧客がリソース・プールのリソースを共有します。ただし、各顧客に割り当てられた特定のアプリケーション、コンピューティング、データベース、ストレージ、およびネットワーク資源は、他の顧客から隔離され、アクセスできません。そのため、各顧客のデータは個別に管理され、各顧客に割り当てられたリソースは他の顧客のリソース使用量の影響を受けません。各顧客のVMSは、他の顧客の使用レベルに関係なく、その高パフォーマンス性を保持します。

オンデマンド・セルフサービス

クラウドVMSの顧客は、クラウド・サービス・プロバイダとのやり取りを最小限に抑えるか、あるいは全く行わずに、必要に応じて機能を有効または無効にできます。これにより、変更を行うために必要な費用、時間、および労力が削減されます。

迅速な弾力性とスケーラビリティ

顧客のクラウドVMSに必要なコンピューティング、ストレージ、またはネットワーク・リソースが増減すると、リソースはニーズに合わせて迅速かつ弾力的に自動的に調整されます。例えば、雨が降ってより多くの映像ストレージ容量が必要な場合、自動的に提供され、新しいストレージは不要になった時に解放されます。このプロセスは顧客には見えません。一般的なオンプレミス・サーバとNVRなどのようにリソースが制限されないの、顧客には問題は生じないのです。

リソース・プール

クラウドVMSを非常に安価に手にすることができるのは、リソース・プールの機能があるからです。クラウドの物理リソースと仮想リソースをリソース・プールに集約して、複数の顧客に効率的にサービスを提供することができます。このしくみの複雑さはそれぞれの顧客には見えません。このITの専門スキルのコストは、すべての顧客に的確かつ効率的に割り当てられています。

クラウド VMSの主な利点

最適に設計されたクラウドVMSシステムの強みは、クラウド・コンピューティングのハードウェアおよびソフトウェア・リソースがセキュリティ映像の高性能のために特別に設計されていることです。クラウド・コンピューティングの規模の経済性と専用基盤を組み合わせることで、以下に列記したような機能を安価なクラウドVMSサブスクリプション費用に含めることができます。

- ホット冗長コンピューティング
- ダブルおよびトリプル冗長性を用いた映像データ・ストレージ

- 定期的な情報セキュリティ監査
- 頻繁な脆弱性スキャンニングとサイバー・セキュリティ侵入テスト
- 自動的に適用されるアプリケーション・セキュリティの更新
- 継続的配信

継続的配信とは、ソフトウェアの各作業が完了するたびに、ソフトウェア更新を自動的にできるようにするために使用されるソフトウェア・エンジニアリング・アプローチです。更新は通常、年に1、2回ではなく、数週間ごとに行われます。

クラウドVMSオンプレミス機器

さらに、クラウド・コンピューティング機能の多くは、クラウドVMSに送信する前に映像をバッファリングするローカル設置機器にまで拡張されています。クラウドVMS機器は、自己構成型でクラウド管理されています。新しいセキュリティまたは機能の改善が利用可能になると、アプライアンスは自動的に更新されます。適切に設計されたクラウドVMSの場合、そのローカル設置機器にはルーターとファイアウォールの機能が組み込まれており、マルウェアへのカメラの感染や映像への不正アクセスを防ぎます。したがって、顧客が必要とする唯一の専門知識は、ワークステーション、ラップトップ、タブレット・コンピュータ、またはスマートフォンを使用してアプリケーションにアクセスできることだけです。サービス・プロバイダがカメラをインストールして接続するには、基本的なネットワーク知識が必要だけです。高度なITシステムの専門知識は必要ありません。

これで、映像管理システムに必要なIT専門知識のレベルが高くないかVMS購入の重要な決定要因である理由を簡単にご理解いただけたでしょう。



■ 筆者紹介

ディーン・ドレイコ氏は、世界最大のクラウド・ベースの映像監視会社であるイーグルアイネットワークス社創業者。同氏は、他にも複数の優れたセキュリティ関連企業を設立。またイーグルアイネットワークス社だけでなく、クラウド・ベースのアクセス・コントロール企業Brivo社のオーナー兼会長でもある。ドレイコ氏は

かつてバラクーダネットワークス社の創業者兼CEOとして、業界初となるメール・セキュリティ・アプライアンスや様々なサイバー・セキュリティ製品を開発した。同氏はミシガン大学アナバー校電気工学科学士号、カリフォルニア大学バークレー校電気工学科学修士号を取得。金融グループのゴールドマンサックスはディーン・ドレイコ氏を「2014年の最も魅力的な起業家100人」の一人として挙げた。

質問 イーグルアイネットワークス社の専門分野は？

回答 当社は、クラウド映像監視におけるセキュリティとオペレーションを担う会社です。そして、映像監視のAPIプラットフォームと連携して、オンデマンドでVMSのセキュリティとオペレーションを提供しています。

質問 イーグルアイネットワークス社は、このビジネスを立ち上げてから、どれくらいになりますか？

回答 当社は、2012年夏から開発に取り掛かり、2014年1月、初の製品となるEagle Eye Cloud VMSを正式に発表しました。

質問 Eagle Eye Cloud VMSは、どのようなシステム構成でしょうか？

回答 Eagle Eye Cloud VMSは、Eagle Eye Cloud Video APIをベースに設計・構築されており、アクセス・コントロール・システムなどの様々な異なるタイプのシステムに対しても柔軟に対応いたします。

質問 Eagle Eye Cloud VMSの利用方法について、どのようなハードウェアが必要ですか？

回答 当社では、ユーザの方にBridgeをオンサイト環境で導入していただきます。

質問 Bridgeとは何ですか？

回答 Bridgeとは、監視画像が保存されている当社のデータセンタに接続するための、クラウド管理型のオンプレミス装置です。Bridgeは、インターネット接続が切断された場合に備えて、映像をバッファリングします。Bridgeは、暗号化、データ重複排除、帯域幅管理、動体分析、映像圧縮なども行います。



質問 現在NVRとIPカメラ16台のシステムを稼働しています。現在のシステムのデータのバックアップとして貴社のクラウドVMSと連動させることは可能でしょうか？

回答 はい、バックアップ目的でNVRシステムをEE Cloudに接続することができます。弊社には、Eagle Eye Cloud Replication用の特別な製品がございます。EE Cloudバックアップのコストは、保持期間とカメラの解像度によって異なります。この際に必要なハードウェアは、Eagle Eye Bridgeです。詳細については、当社までお問い合わせください。

質問 現在使用しているNVRとIPカメラにバックドアが付いているため、データの漏洩を懸念しています。データ漏洩を防ぐために貴社のクラウドVMSを導入することは可能でしょうか。その場合、設定期間はどのくらいかかりますか？

回答 Eagle Eye Cloud VMSは、ほとんどのNVRやDVRとは異なり、強力なサイバー・セキュリティが特徴です。Eagle Eyeアーキテクチャは、カメラをインターネットから隔離し、サイバー・セキュリティも保証します。Eagle Eye Cloud VMSの設置時間は通常30分が目安です。

質問 まず現在稼働中のNVRにある過去のデータだけを貴社クラウドVMSに移行して、契約期間が終了してから、システム全体をクラウドVMSに移行することは可能でしょうか？

回答 通常、NVRとDVRはクローズドソリューションであり、このためのオープンAPIがないため、古いNVRまたはDVR映像をEagle Eye Cloudにアップロードすることはできません。Eagle Eye Cloud VMSを並行して稼働させ、契約期間の終了時にシステムの切り替えを完了することをお勧めします。

質問 現在使用しているNVRベースの監視システムと同等の内容で構築していただくことは可能でしょうか？

回答 はい可能です。

質問 NVRとIPカメラ8台のシステムを貴社クラウドVMSに移行する場合の構築期間と概算はどのくらいですか？

回答 NVRおよびIPカメラ8台の場合、切り替えは通常30分以下で完了します。お客様に掛かる月額費用は低コストに抑えられます。システム内容により概算が変動しますので、詳細については当社までお問い合わせください。

イーグルアイネットワークス株式会社

〒150-0034 東京都渋谷区代官山8-5 代官山8.5ビル4階
TEL:03-6868-5527 E-MAIL:APACsales@een.com