よくわかるIPネットワーク

株式会社ジャバテル　代表取締役　佐々木宏至

2018年もあっと言う間に第一四半期が過ぎ去ろうとしている。

今月6日から9日までの4日間にSECURITY SHOW 2018が開催される。今年弊社は出展しないが、ミカミ社(SS7103)ブースでジェネテック社Security Centerをコラボレーションする。ミカミ社製HD-SDIカメラをCellinx社製H.265対応モデルURH900エンコーダに接続して展示する。

見どころはその滑らかな映像だ。URH900はジェネテック社にネイティブ対応し、さらにONVIFによりMilestoneやExacqVisionなどのVMSやNVRと接続可能だ。また、CGIベースAPIも提供しているので、ほとんどのVMSに簡単に組み込み可能だ。

URH900の概要：HD-SDI 入力H.264/H.265エンコーダ。超低遅延(実測250msec)でオーディオG.711、SDカード、PTZシリアル、PoE対応。

Hikvision社、ジェネテック社プロトコルのサポートを削除

ジェネテック社が2016年Hikvision製品を制限付きサポートにしたが、この出来事は決してマーケティングでは無く、ジェネテック社の企業理念に基づいて決断されたことだ。これに対して、今度はHikvision社が新ファームウェアからジェネテック社プロトコルを廃止するようだ。今回のHikvision社の対応は当面は推移を静観する。日本でHikvision社の先駆者として製品を供給した実績を持つ(現在は取扱いしていない)私としてはHikvisionに申し上げたい事があるがやめておく。

Geovision社製品で前例のないセキュリティ脆弱性とバックドア

Geovision社は日本でも比較的知名度が高い台湾メーカだが、あるバージョン以下ではおまじないの操作で簡単にカメラにアクセスできる前代未聞のバックドアが仕込まれていた。Hikvision社やDahua社のバックドアだけでなく、今やどこのメーカでもこの問題が内在している。

例えば、PCの分野でのWindows10で、1年間アップデートを制限してインターネットに晒していたらどうなるか？ 確実にボット･ネットワークに組み込まれるか。こればっかりは断定できないが、狙われたら終わりだ。内部攻撃を想定しない時、ネットワークが一切インターネットに繋がっていなければ、ほとんど問題ないと言える。

VPNだから安心？

しかし、最近間違った考えが増えている。確かにVPNの通信自体はセキュアだが問題がある。VPNを実行するパソコンがVPNルータで、そのルータ設定が一切インターネット･アクセスをブロックしている場合、純粋にLAN/WANと言える。しかし、大半はゲートウェイ経由でインターネットにアクセスできるようになっているだろう？

また、VPNルータではなくソフトウェア機能でVPN通信する場合も、インターネットへのアクセスが可能だ。PCはカメラ映像をVPN経由でストリーミングしていても、そのPC自体が乗っ取られる危険性はVPNでは防げない。ファイア･ウォールでブロックしていても絶対はない。

カメラ側はVPNルータ経由、PC側はルータのゲートウェイを指定せず、VPNルータ経由のL2スイッチに接続すれば完全に閉じた網となる。ここで特に注意する点は、インターネットに接続されていないかを必ず確認することだ。メーカのマニュアル通りに接続することができた場合、それは100%インターネットにも繋がっている。それがデフォルトだ。

先ほど内部攻撃を想定しない時を前提で説明したが、これが無意味だと気が付いていただきたい。どんなに強固なファイア･ウォールでも全くインターネットと通信を遮断することはない。内部の人間が報酬を受けてバックドアを仕掛けたら「ジ･エンド」だ。

インターネット･セキュリティの話題になったが、監視カメラ事業で企業向け市場に取り組むには不可避だ納入時のシステム時は閉じたネットワークだが、その後モバイル対応機能を追加することになり、サーバをVPNで接続するようになると、一気に指摘したリスクが発生する。

ディープ･ラーニング(深層学習)

最近はディープ･ラーニング搭載のNVRが出てきている。値段も当然高額になるが実際はどうなのかだが、少なくとも今は手を出すべき対象でないし、出すべきでない。実装レベルがあまりに低すぎてほとんどが調整不能だ。そして最も悲惨なことは全く学習しないことだ。一応学習した結果を提示するだけで、日々の映像を学習するわけではない。

仮に学習して非常に良い結果が得られたとしても、ディープ･ラーニングを搭載した製品を3,000ドルで提供できるはずがない。真に使い物になるには何年かあるいは十年くらい必要か。画像分析の実用性は以下の二点に集約している。

オンボート分析とサーバ･サイドのレガシー&ディープ･ラーニングのハイブリッド。

カメラは最適な場面照明を得るために、リアルタイムでフィルタリングし、この映像をストリーミングしている。オンボード分析が有利なのはこのフィルタリングしているのが自分だからだ。サーバ･サイドの場合は勝手にフィルタリングされた映像を解析するため、極端な話1fpsの映像に0.5秒しか存在しない物体は見つけることなど最初からできない。しかし、オンボードの場合はそのような影響を無視した設計が可能だ。プロセッサ技術が高度に発達する過程のある段階からは、全てがカメラに組み込まれ、ディープ･ラーニング･クラウドとの連携が一般的になると思う。

さらに進化すると今では想像できない展開があるかもしれない。現実にはオンボード分析をサポートするメーカは増加しているが、実装レベルで優劣が相当にあり、しかもその比較データが存在しない。定量化できないことが最大の原因だが、我々インテグレータは「さわらぬ神に祟り無し」と、指名されない限り積極的に進めない。

桜で有名な施設ではアクシス社オンボード映像分析をフェンスセンサーと併用運用している。国内屈指の侵入検知だ。想定以上に誤報も少なく機能しているようだ。ただし、カメラは可視光ではない。

オンボードの解説をしてきたが、現状では用途にもよるが、サーバ･サイド分析の精度は高いと私は考える。侵入検知系はオンボードに優位性があるが、顔検知や顔認証、置き去りや持ち去り、群衆や人数カウント、待ち行列などはサーバ･サイド方式に軍配が上がる。

当社がジェネテック社 Security Center で推奨しているオンボード分析は、アクシス社Perimeter Defender、ボッシュ社IVA、Hanwha Techwin。サーバーサイドでは、ACIC、AllGoVision、KiwiSecurity、NECだ。

前号からの続きで今回は広域マルチキャスト

同一VLANで済む場合ルーティングは不要なので、IGMPクエリアとIGMPスヌーピングで事足りるが、複数のVLAN間通信を必要とする場合、広域網ではPIM-SM(マルチキャスト･グループ･メンバーがまばらで散らばっているネットワークを選択することを推奨)1 つのマルチキャスト･グループの送信元が1つの監視カメラに特定される特徴を持つ監視カメラネットワークではPIM-SM/PIM-SSM いずれでも適用が可能だ。

送信元とマルチキャスト･グループ･アドレスの対応づけがオンライン中でも変えられる機種が多い。PIM-SM でマルチキャスト中継を止めずに制御系を切り替えることができ、可用性の高いシステムを構築することが可能だ。

広域インターネットでは、GREトンネルとIPsecで構築してPIM-SIMでルーティングすることで超大規模な広域システムの構築が可能だ。この時マルチキャストであることはパフォーマンスの点で申し分ないと言えるが、日本ではあまり事例が無いようだ。当社では某港湾監視の巨大システムで構築運用している。

a&S