ローカル映像システムとクラウド映像システムとのサイバー・セキュリティを比較する

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

今日のネットワーク映像監視システムは、様々な点でサイバー攻撃に対して脆弱です。ネットワークカメラは、標的とされたシステムへの大規模な分散型サービス拒否(DDoS)攻撃を仕掛けるために、ハッカーにより「武器化」されました。2015年には、カメラやDVR、その他のIoT(Internet of Things)機器に対する世界規模のサイバー攻撃が大幅に増加しました。2016年末までに、何百万ものネットワーク映像機器が「Mirai」や「Masuta」そしてその亜種である「Hajime」に感染していました。2017年には、サイバー攻撃の継続的な増加に伴い、サイバー攻撃に関するニュースの見出しを連日のように目にしました。米国では、サイバー攻撃によりワシントンDCの公共区域にある警察監視カメラ用DVRの70%に支障をきたし、米国大統領選挙直前の4日間、映像録画が停止しました。2018年9月に、カスペルスキー社は世界のマルウェアが2017年以降3倍に増えたことを報告しました。「Mirai」とその亜種は、世界全体の約21%の攻撃に関与しています。

ここ数年に報告されている攻撃のほとんどは、米国およびアジア以外の国を標的としていました。日本の情報通信技術研究所(NICT)は、25万台のインターネット・センサを管理しています。図1に示すように、NICTは2017年12月に、ネットワーク接続機器を標的にした「Mirai」マルウェアの大部分で、サイバー攻撃の50倍の増加を検出したと報告しました。

日本初のISP(インターネット・サービス・プロバイダ)であるインターネットイニシアティブ(IIJ)社は、ウイルスに感染した機器数が急激に増加していると報告しました。2017年のIIJ社の調査では、日本でのサービスに関連する感染したIoT機器数が、1か月間で約100から12,000に増加したことがわかりました。

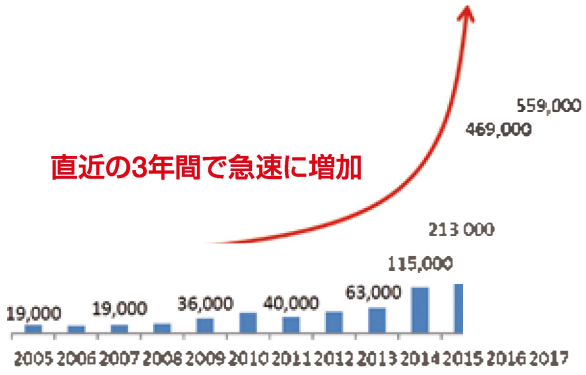

図1. NICTによるサイバー攻撃の動向

イラスト提供：外務省

■監視カメラとレコーダが脆弱な理由は?

40年もの間、セキュリティ映像監視はコンピュータ、イーサネット・ネットワーキング、そして旧来のCCTV(Closed Circuit Television)技術を使用していました。1990年代後半に監視カメラはコンピュータ機器となり、ネットワークカメラあるいはIPカメラと呼ばれていました。各カメラには、Linuxあるいは他のOS(オペレーティング・システム)とWebサーバが含まれています。ネットワークカメラは、ネットワーク・プロトコルを介して標準ベースの映像ストリームを提供し、カメラ設定、編集、ライブ映像を監視用のWebページを提供します。監視カメラがコンピュータ機器になると、他のコンピュータのようなマルウェアに対して脆弱でした。最初は、CCTVカメラのように閉ざされた環境に設置され使用されていたため、問題にはなりませんでしたが、クローズドLAN(ローカルエリアネットワークに接続されることで、少数の限られたセキュリティ・スタッフだけがカメラ映像にアクセスしていました。

当時の監視映像LANは、2つの理由でインターネットやビジネス・ネットワークに接続されていませんでした。まず、セキュリティ映像を内密にしていました。次にほとんどのビジネス・ネットワークの容量が限られていたため、高帯域幅のカメラ映像ストリームをサポートできませんでした。したがって、当時のセキュリティ業界の推奨事項は、ネットワーク監視カメラはスタンドアロンのLANを使用して展開することでした。

■ネットワーキングおよび映像技術の進歩

現在までの15年間で、ネットワーキングやコマーシャル映像、モバイル機器やインターネット・サービスなどの技術は飛躍的に進歩しました。したがって、ほとんどのスマートフォンやタブレットはフルHD映像録画および表示機能を備えており、その中にはNetflix、Hulu、YouTubeなどのインターネット・ベースの映像ストリーミング・サービスへのアクセスも含まれています。企業の有する現在のWAN(ワイドエリアネットワーク)とLANは、一般的なデジタル映像フォーマットを簡単にサポートし、十分な帯

域幅を持っています。

何十年もの間、セキュリティ映像はセキュリティ管制室での利用に限られていました。現在、コンシューマ機器の映像機能により、ファースト・レスポンダ、マネージャ、リモートユーザなど、ビジネス上のニーズがある映像とセキュリティ映像を安全に共有することができます。

■監視映像のビジネス上の利点

例えば、複数サイトによる小売業の管理は、店舗内での顧客の動線を表示および分析し、従業員の作業効率を監視することができます。監視映像分析技術も進歩しており、顧客サービスの待機時間、サービス提供の遅延期間、および商品の表示を見ている顧客の時間などの非常に貴重なビジネス分析を提供しています。このようなデータをマーケティング・キャンペーンや広告キャンペーン、従業員のトレーニングや品質保証プログラムと関連付けることで、貴重なビジネス上の成果を得ることができます。

高解像度のメガピクセル監視カメラは、製造工場ラインでの重要な品質保証ツールにもなっています。製造ラインの機器が稼働している時に、人が安全に行けない場所にカメラを配置できます。毎秒30フレームまたは60フレームの高速映像録画から、人間の視認では不可能で口頭による説明ができないような明確で正確な視覚的証拠を得ることができます。

上記に加えて、他の説得力のあるビジネス上の理由により、映像監視カメラをビジネス・ネットワークに配置し、ライブおよび録画された映像へのアクセスをビジネス・ネットワークへの接続やモバイル機器を介して許可された非セキュリティ要員に利用可能にする必要があります。しかし、これは同時に、防犯カメラとその映像管理システムが、意図せずに外部のマルウェアの脅威やインサイダーの脅威にさらされる可能性があることを意味します。

■サイバー・セキュリティが最も高いのはどのタイプの映像システムか?

強力なサイバー・セキュリティは、VMS（映像管理ソフトウェア）にとって非常に重要になっています。クラウドベースのVMSとオンプレミスのVMSとを比較して大きな違いが何でしょうか?

オンプレミス・システム用クライアント・サーバ技術とクラウドベースのVMS用のクラウド・コンピューティング技術は大きく異なることから、サイバー・セキュリティ対策のコストと有効性は大きく異なります。以下の記事では両者の主な違いについて説明します。

まず、電子による物理セキュリティ・システムのサイバー・セキュリティ危機に対して、誰が責任を持つのかを理解すること

が重要です。オンプレミスVMSの場合、ほとんどの映像監視システムの設置業者は設置されたシステムに対するサイバー・セキュリティの責任を引き受けることを拒否します。これは、システムをユーザの社内に設置し、ユーザのネットワークに接続し、ユーザの担当者によって操作されるからです。この場合、サイバー・セキュリティの問題は基本的にはユーザの責任となります。

次に、クラウドベースのVMSの場合、クラウドVMS提供業者は、クラウド基盤とその運用、そしてサイバー・セキュリティに責任を負います。これには、保存映像の機密性と完全性そして可用性の維持が含まれます。また、インターネットを介したクラウドVMSアプリケーションへの安全なアクセスを保証することも含まれます。

■映像データ保護

優れた設計のクラウドVMSは、オンサイトのバッファ・アプライアンス(専用機器)がカメラから映像データを受信する時に、256ビットのAES暗号化を使用して映像データを暗号化します。その後、それをクラウドVMSに安全に送信します。クラウドVMSデータセンターでは、2倍または3倍のデータストレージ冗長性を使用します。この種の映像データの冗長性は通常、顧客の社内クライアント・サーバ・システムにとっては法外に高価です。

高度に設計されたクラウドVMSは、VMSアプリケーションへのユーザー・アクセスのための2要素認証、およびユーザのモバイル機器用認証も提供します。監査証跡ログは全てのアクセスの記録を保持します

■サイバー・セキュリティの費用

クラウドVMSのサイバー・セキュリティ費用は全てのユーザと共有しているため、クラウドVMS基盤に対してオンプレミス・サーバよりもはるかに強力なサイバー・セキュリティを提供することが可能です。オンプレミスのVMSの場合、サイバー・セキュリティのコストはユーザー人が全て負担します。

クラウドVMSデータ・センターでは、サーバの脆弱性スキャンとデータ・センターの侵入テストが頻繁に行われています。クラウド・データ・センターの担当者に対して綿密なバックグラウンド・チェックが行われ、強力なサイバー・セキュリティ・トレーニングが提供されます。クラウドVMSには、文書化された監査可能なセキュリティプログラムがあり、それに厳密に従っています。

■カメラにおけるサイバー・セキュリティ

効率よく設計されたクラウドVMSのオンサイト映像バッファ・アプライアンスには、ネットワーク・ルータとファイアウォール機能があり、3つの重要なサイバー・セキュリティ機能を実行します。まず、クラウドVMSアプライアンスは、インターネットと組織のビジネス・ネットワークからの全ての接続を拒否します。アプライアンスはデジタル証明書ベースの認証を使用して、クラウドVMSへの接続を保護します。ハッカーやマルウェアがビジネス・ネットワークの外部にいるか内部にあるかにかかわらず、クラウドVMSアプライアンスへのアクセスを取得することはできません。次に、クラウドVMSアプライアンスは、感染したカメラからのアウトバウンド接続の試みをブロックし、マルウェア・ボットネットからカメラを隔離します。3つ目は、クラウド管理のオンサイト・アプライアンスが自動的に最新の状態に保たれるため、顧客や設置者が何もする必要はありません。

理論的には、ユーザのIT部門は、映像監視システムにこのようなセキュリティ対策を実装することができます。しかしながら、それは追加のネットワーク・セキュリティ機器への多大な投資を必要とし、システムの初期および継続的なコストを劇的に増加させることになります。

■クラウドVMSで最強のサイバー・セキュリティを実現

最先端のクラウド・コンピューティング技術と最新のサイバー・セキュリティの実行を使用して、よく設計されて構築されたクラウドVMSを維持しています。オンプレミスのVMSシステムでは再現できない規模の経済性があります。したがって、クラウドベースのVMSは、顧客または設置業者がオンプレミスのクライアント・サーバVMSを提供するよりもはるかに強力なサイバー・セキュリティの保護を低コストで提供することができます。

a&S

■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Eagle Eye Networks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した。また、Eagle Eye Networks社だけで無く、クラウド・ベースのアクセス・コントロール企業ブリヴォ社のオーナ兼会長でもある。ドレイコ氏は、それ以前に、バラクーダ・ネットワークス社の創設者兼社長兼CEOとして、最初のE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ーバ校電気工学科学士号、カリフォルニア大学バークレイ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。