発行／ASJ社　年間購読料　6,000円（税、送料込）　1冊1,000円（税別）

a&S JAPAN

The Professional Magazine Providing Total Security Solutions

www.asj-corp.jp　Jul/Aug. 2019　no.71

特　　集：2019年のアクセス･コントロール技術の新機能

secutech
THAILAND

2019年10月28-30日
タイ王国バンコク

タイで開催される
セキュリティ、防火、スマートライフフェアが、
持続可能な都市開発を促進します。

www.secutechthailand.com

日本問い合わせ先
ASJ合同会社
TEL　03-6206-0448
Email　komori@asj-corp.jp

Concurrent with:

thailand lighting fair　thailand building fair

WORLDEX
Group of Exhibition Companies

messe frankfurt

IDIS SUPER FISHEYE

5MP コンパクト

IR LED (距離:15m)

H.265インテリジェントコーデック採用

スマートDewarping(歪み補正)に対応

ヒートマップ

内蔵マイク

商品に関するお問い合わせは
IDIS Co.,Ltd 日本正規代理店　株式会社セキュア secureinc.co.jp

東京本社 | 東京都新宿区西新宿2丁目6-1 新宿住友ビル 20F
TEL.03-6911-0660 FAX.03-6911-0664

IDIS One Solution. One Company.

SÉCURE

www.idisglobal.com

目　次

広告索引

広告主名（ABC順）	掲載ページ
AVIGILON	19
HIKVISION	5
IDIS	3
日本経済新聞社	表四
SECUTECH THAILAND	表二
SECUTECH VIETNAM	37

次号案内　2019年 9/10月号（9月10日発行予定）

（誌面の都合上、変更になることがあります）

特　集
顔 認 証

連　載
クラウドの利点と活用

a&s JAPAN ©ASJ合同会社　2019年 7-8月号　No.71
The Professional Magazine Providing Total Security Solutions

発行人　小森堅司　　DTP　サンフィール

a&s JAPANは、Messe Frankfurt New Era Media発行のa&s Internationalをはじめとするa&s各誌の独占翻訳権の特約、およびIPVMの抄訳記事掲載の承諾を得て発行するセキュリティ国際情報誌です。

ASJ合同会社
Advanced Security Journal LLC
〒101-0041 東京都千代田区神田須田町1-7-1ウィン神田ビル10階
電話：03-6206-0448　FAX：03-6206-0452

■広告に関するお問い合わせは
E-mail：komori@asj-corp.jp
■購読に関するお問い合わせは
E-mail：info@asj-corp.jp
■記事情報提供に関するお問い合わせは
E-mail：info@asj-corp.jp

■DM代行サービスおよび電子メール配信サービス
当社では、企業の依頼によりDMまたは電子メールで情報をお届けすることがあります。
これらのサービスでは、読者の皆様の個人情報を当該企業には一切公開しておりません。

保護層の追加

- 超高感度火災検知
- ATEXおよびIECEx認証

Hikvisionの防爆サーマルネットワークカメラ

可燃性ガスや粉塵がある暗い地下鉱山エリアでは、各保護層が欠かせないものになっています。Hikvisionの防爆サーマルネットワークカメラは、市場で実証された防爆性能と防食性能を備え、改良されたサーマルイメージングと温度異常アラームが鉱山作業員を火花や可燃物起因の危険から守ります。引火しやすく暗い作業環境の中で、一流な監視があらゆる方法で、鉱山作業員の安全を日々に守りましょう。

日本代理店

Security DESIGN	D's Security	Jsecurity inc.
Tel 03-6230-3021	Tel 076-291-4001	Tel 03-6806-0343
www.security-d.com	www.dss.co.jp	www.jsecurity.jp

HIKVISION
www.hikvision.com

IPVM URL:https://ipvm.com/

IPVMは、セキュリティと映像監視に関する世界有数の情報提供サイト。

【特徴】

●5,000件超のセキュリティ技術に関する報告
●550件超のセキュリティおよび主要映像監視製品のテスト
●豊富なソフトウェア·ツールによる評価とテスト
●映像監視関係者向け教育と講座用情報の提供。
●メンバーからのコメントを含めた活発なコミュニティの形成

【有料メンバー】

●100カ国超1万人以上のセキュリティ業界従事者、関係者

【スタッフ】

●エンジニア、開発者、セキュリティ·システム構築者、サポート·マネージャなど総勢11名

【掲載許諾】

本誌ではIPVMの許諾を得て、ウェブ上で無料閲読することができる内容だけを掲載しています。閲読するにはIPVMとの有料メンバー契約が必要です。IPVMに掲載されている内容は、一切無断転載です。

Verkada社、「比類のない」低照度性能という偽の主張を削除

ジョン·ホノヴィッチ　著

https://ipvm.com/reports/verkada-unrivaled

Verkada(ヴェルカーダ)社は、IPVMが疑問視するまでは「比類のない低照度性能」を達成したと偽って主張していた。同社の低照度性能はIPVMテストで証明されたように事実劣っている。

虚偽の理由

ヴェルカーダ社は、センサとLEDの選択に関する偽った主張に基づいていた。しかし、1/2.8型プログレッシブCMOSセンサは、今日のマルチ·メガピクセルカメラとしてサイズが小さくて、一般レベルなものだ。さらに、IPカメラでは「工業用LED照明器」も一般的だ。

より大きな問題は、ヴェルカーダ社のカメラは、8年前の

Huawei社チップを使用していて、劣った圧縮技術とビットレート制限を抱え、画像品質を低下させている。詳細は下記を参照。

https://ipvm.com/reports/verkada-video
https://ipvm.com/reports/vbr-vs-cbr-surveillance-streaming
https://ipvm.com/reports/video-quality

IFSEC 2019展示会リポート

ジョン·ホノヴィッチ　著

https://ipvm.com/reports/ifsec-19

英国最大のセキュリティ展示会であるIFSECで、IPVMはで何が新しくて起こっているのかを調べた。その内容は下記の通り。

●ファーウェイ社が出展　●GDPRの変更　●Dahua社がアンブレラ·アナリティクスを追加　●Dahua社の顔認証、許可なし　●Hikvision社は顔認証の展示なし　●Avigilon社とHikvision社の猛烈な広告　●交通状況の表示　●展示会場のフロア縮小　●監視カメラコミッショナーのトニー·ポーター氏へのIPVMインタビュー　●ヒューマンライツウォッチ、Hikvision社に声をかける　●中国の市場経済の対外宣伝窓口　●アクシス社がGDPRとLPCを発表　●エニーヴィジョン社の資金調達とオンボードカメラFR　●ジェネテック社のGDPRマーケティング/アンチフェイス　●無名の米国企業が「誤警報なし」と主張　●インフルエンサーの辞退　●ONVIFとPSIAでの厄介なTavcom教育　●IFSECが禁止したライバルメディア　●マイルストーン社が出展せず

再配置可能なマルチ・イメージ搭載カメラの戦い Avigilon社、アクシス社、Dahua社、Hanwhaテックウィン社、Hikvision社、パナソニック、VIVOTEK社

イーザン・エイズ、ロブ・キルパトリック　著

https://ipvm.com/reports/repositionable-shootout

再配置可能なマルチ・イメージ搭載カメラは映像監視の中で最も急成長している分野の1つだ。そこで、どの製品が際立っているかを見るために、我々はメーカ7社から再配置可能なモデル10台を購入してテストした。

●Avigilon社12MP H4マルチセンサ　●Avigilon社32MP H4マルチセンサ　●アクシス社P3717-PLE　●Dahua社マルチフレックス4x2MP　●Hanwhaテックウィン社PNM-9000VQ　●Hanwhaテックウィン社PNM-9081VQ　●Hikvision社PanoVu 8MP　●Hikvision社PanoVu 20MP　●パナソニックWV-X8570N　●VIVOTEK社MS9321-EHTV

生体認証機器利用統計2019

ダン・ジェリナス　著

https://ipvm.com/reports/biometrics-usage-19

スマートフォンでは顔認識と指紋認識が標準的に使用されているが、物理的セキュリティではそれほど一般的ではない。

本稿では、生体認証機器の採用率を検証し、生体認証機器を使用する理由と使用しない理由に関するシステム構築者の意見を分析する。今回の記事の参考資料は、電子アクセス制御に関するバイオメトリクスの長所と短所のレポート、およびお気に入りの生体認証機器2018である。参照していただきたい。

カーネギー・メロンAIで起業したZensors社の情報

ジーン・パットン　著

https://ipvm.com/reports/zensors

共同創立者クリス・ハリソン氏とアヌラーグ・ジェイン氏Zensors(ゼンサーズ社)は、カーネギー・メロン社調査事業部門から分離したカーネギー・メロン社により設立され、カメラごとにカスタマイズされたモデルを提供しているため、はるかに高い精度が得られる。

IPVMはゼンサーズ社と彼らの行動、彼らがどのように彼らのシステムと彼らの市場参入の規模を拡大する計画を立てているかを理解するために話した。本稿では下記について紹介している。

●ゼンサーズ社とは　●ゼンサーズ社が対象としている顧客　●製品価格　ゼンサーズ社の市場参入　●解析機能の種類　●カスタム・データセットの生成方法　●VMS統合

新規立ち上げ企業ロンバス・システムズ社、Verkada社製品の2倍の機能搭載した製品を半値で販売

ジーン・パットン　著

https://ipvm.com/reports/rhombus-startup

クローズド・クラウド・システムは、メラキ社とVerkada (ヴェルカーダ)社と共に最も急成長している映像監視部門だ。現在、カリフォルニア州の新興企ロンバス・システムズ社は、ヴェルカーダ社製品の2倍の機能を搭載した製品を半値で提供している。

IPVMはロンバス社共同創設者たちと、なぜ彼らがセキュリティ製品を始めたのか、その製品と市場投入について話した。

●ロンバス社とは　●サポートしているカメラ　●基本アーキテクチャ　●価格　●提供しているクライアント機能　●提供している解析機能の種類　●対象としている市場は?　●ヴェルカーダ社との比較　●懸案事項と制限事項

NEC、生体認証・映像分析事業を強化

https://jpn.nec.com/press/201906/20190621_02.html

NECは、デジタルビジネスのさらなる加速に向けた新たな取り組みとして、生体認証・映像分析事業のデジタルフレームワーク、デジタルHubを整備した。また、その一環として生体認証・映像分析統合プラットフォームを、先行して北米で2019年7月から提供開始した。同社は本取り組みにより、同事業について2021年度までにグローバルで1,000億円の事業規模を目指す。

これまでNECは、先進的なICTにより顧客のデジタル・トランスフォーメーションに貢献してきた。特に生体認証・映像分析の領域では現在、約70の国や地域に1,000システム以上を提供している。

人を特定する技術である生体認証は、複数の技術をマルチ・モーダルに組み合わせることで、精度だけでなく利便性が向上し、様々な利用シーンで身体を「鍵」や「存在の証明」として活用することができる。これに、映像分析技術を組み合わせることで、生体認証で特定した人の動作や周辺状況を理解することが可能になる。

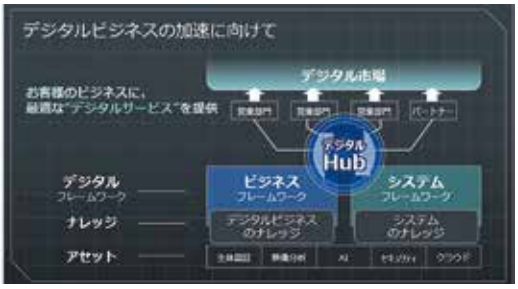
NECが注力するパブリック・セーフティ領域に加えて、個人認証から地域活性化に向けた「おもてなし」まで、社会の様々なシーンに生体認証・映像分析技術の活用を広げていくことで、社会の安全・安心、利便性の向上を進めていく。

生体認証・映像分析による市場価値の拡大

【今回の取り組みの概要】

1.デジタルフレームワークの整備

NEC全社のアセットとナレッジ(ノウハウ・知見)を最大限活用するための枠組みである「デジタル・フレームワーク」を生体認証・映像分析から整備した。顧客への価値提供を起点とし、様々なユース・ケースをビジネス・フレームワークとして体系化している。また個々のユース・ケースを実現するための実装モデルをシステム・フレームワークとして定義している。これにより、顧客のニーズや課題に最適な提案や、高度な価値創出が可能となる。



2.デジタルHubの整備

NECのデジタル・ビジネスにおける中心的役割を担う全社共通機能として個別案件を支援するソリューションコア機能と、事業戦略の構築・実行を支援するビジネスコア機能を有する「デジタルHub」を整備した。デジタルHubが中心となってデジタル・フレームワークを活用することにより、顧客の課題解決に繋がるNECのノウハウ・知見を活かしたソリューションを正確かつ迅速に顧客に提供することを目指す。

3.生体認証・映像分析統合プラットフォームの提供

システム・フレームワークの一つとして、生体認証・映像分析技術をお客様のニーズや課題に適した形で自在に組み合わせて使えるように、統合プラットフォームを整備した。これにより、クラウド、ネットワーク、エッジにまたがり、生体情報や映像データをリアルタイムかつセキュアに分析することが可能になる。

先行して北米で2019年7月から提供開始した。生体認証・映像分析機能のマイクロサービス化を進め、2019年度内の国内展開を目指す。

総務省、マルウェアに感染しているIoT機器の利用者に対する注意喚起を実施

http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html

近年、IoT機器を悪用したサイバー攻撃が急増しており、そのようなサイバー攻撃を防ぐためには、機器の利用者において適切なセキュリティ対策を講じる必要があることを踏まえ、2019年2月より「NOTICE」を実施している。

今般、「NOTICE」の取組に加えて、2019年6月中旬から国立研究開発法人情報通信研究機構（NICT）のNICTERプロジェクトによりマルウェアに感染していることが検知された機器に対して、インターネットプロバイダから利用者へ注意喚起を行う取組を実施している。

1 概要

IoT機器を悪用したサイバー攻撃の深刻化を踏まえ、2018年5月に改正された国立研究開発法人情報通信研究機構法に基づき、2019年2月よりNICTがサイバー攻撃に悪用されるおそれのある機器を調査し、インターネットプロバイダを通じた利用者への注意喚起を行う取組「NOTICE」を実施している。

「NOTICE」の取組に加えて、2019年6月中旬からマルウェアに感染しているIoT機器の利用者に対し、インターネットプロバイダが注意喚起を行う取組を実施している。本取組は、NICTがNICTERプロジェクトで得られた情報を基にマルウェア感染を原因とする通信を行っている機器を検知し、インターネットプロバイダにおいて当該機器の利用者を特定することにより行う。本取り組みは、総務省、NICT、一般社団法人ICT-ISAC、インターネットプロバイダ各社が連携して実施する。実施概要は下記の通り。

2 利用者への問い合せ対応

本取り組みで注意喚起対象となるマルウェアに感染している機器の利用者に対して、総務省が設置しているNOTICEサポートセンター（インターネットプロバイダによっては当該インターネットプロバイダのサポート窓口）がウェブサイトや電話による問合せ対応等を通じて適切なセキュリティ対策を案内する。

■NOTICEサポートセンター

TEL:0120-769-318（無料・固定電話のみ）、
03-4346-3318（有料）
https://notice.go.jp/nicter

■NICTERプロジェクトでは、NICTがインターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施している。

■NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、インターネット・プロバイダが利用者への注意喚起を行う取組「NOTICE」において、利用者への問合せ対応を実施。

IoT機器のセキュリティ対策に係る取組について

別紙

■ 情報通信研究機構（NICT）がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、インターネットプロバイダを通じた利用者への注意喚起を行う取組「NOTICE」を2019年２月より実施。

■ NOTICEの取組に加え、マルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクト※で得られた情報を基に特定し、インターネットプロバイダから利用者へ注意喚起を行う取組を2019年６月中旬より開始。

※ NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICEの概要】

調査対象：パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダが当該機器の利用者を特定し、注意喚起を実施。

【マルウェアに感染しているIoT機器の利用者への注意喚起の取組概要】

調査対象：既にMirai等のマルウェアに感染しているIoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダが当該機器の利用者を特定し、注意喚起を実施

※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群

アクシオン・ソフト社、アクシオン・ネクストVMS4.3.2版を発表

https://www.asmag.com/showpost/28522.aspx?name=news

この新バージョンでは、映像解析とフォレンジック・サーチ、単一のパノラマビューへの複数台のカメラ供給の統合、メンテナンスとアップデートのための集中サーバ管理、その他多くの機能強化と改善の新機能が導入されている。

■映像解析

待ち行列の長さと訪問者計数の検出ツールを追加した。待ち行列の長さ検出ツールは、指定された区域内の待ち数を計数し、制限を超えたときにシステムに通知する。訪問者計数は、指定区域に出入りする訪問者数を計数する。どちらの検出ツールも小売業界を対象にしている。店舗や販売区域内の通行者の正確な人数を提供し、POSスタッフの効果的な管理を可能にする。

ナンバープレート読取カメラからメタデータを処理するためのサポートも追加された。これにより、映像素材でナンバープレート番号を検索する際のサーバへの負荷を軽減することができる。これにより、サーバごとにより多くのカメラを使用することができる。

火災や煙検知ツールでは、性能を向上させるために、ハードウェアの種類ごとに専用のニューラル・ネットワーク（CPU、GPU、およびIntelのMovidius™ VPU）が使用されている。

■映像素材の検索

保存した瞬間追及検索条件が他のチャネルのカメラで使用できるようになった。フォレンジック・サーチは、デスクトップ・ソフトウェアにさらに近づくように、ウェブ・クライアントを通じて利用できるようになった。

ウェブ・クライアントは現在、毎分/毎時のイベント統計を含む検索リポートをサポートしている。リポートは印刷またはエクスポートすることができる。

■マルチカメラのパノラマビュー

新しく導入されたフレームマージ機能は、スポーツ・アリーナ、空港、港、倉庫、生産施設、公共スペースなどの広い範囲をより便利で効率的に網羅する。フレームマージは、隣接するカメラからの映像素材を一つのパノラマ画面に合成する。パノラマは、リアルタイムで表示したり、映像から再生したり、エクスポートしたりできる。パノラマビューの一部を拡大してメッセージ・ボードに表示することができる。

パノラマビューは自動的に合成される。このアルゴリズムは、隣接するカメラからの画像をスキャンして適切な合成ポイントを探し出し、統合映像内のこれらのポイントを照合する。

■フェイルオーバー・サービス

フェイルオーバー・サービスは十分に改善された。システム・ダウンタイムを発生させることなく、クラスタ内の任意のサーバを一時停止してメンテナンスすることができる。一時停止したサーバの構成は自動的にバックアップ・サーバに転送され、サーバの再起動時に復元される。

クラスタ内の全てのサーバは、単一の配布パッケージまたはネットワーク上のファイルへのリンクで更新できる。この方法はシステム更新を簡単にする。

これで、冗長なサーバ・セットを作成し、ウェブ・インタフェイスを介してプライマリ・サーバとセカンダリ・サーバを割り当てることができる。映像をNASまたはローカルに保存できるようになった。設定を転送した後でアクセス可能にするために、ローカルの映像素材をバックアップ・サーバに永久的に複製することができる。

■マクロ

これで、拡張自動化機能の恩恵を受けることができる。次の場合にマクロを起動できるようになった。

- CPU負荷、RAM、またはサーバの帯域幅制限を拡大
- サーバHDDの空き容量が限界を拡大。
- 映像の空き容量の下限の拡大。
- リレーを作動させる。

マクロアクションには、別のマクロを起動し、ステータスを割り当ててアラームを閉じることが含まれるようになった。

SECURITY SHOW

SECURITY SHOW 2020、展示ゾーンが決定

https://messe.nikkei.co.jp/ss/

2020年3月3日～6日の日程で幕張メッセにおいて開催されるSECURITY SHOW 2020の展示ゾーンが決定した。総合セキュリティゾーン、ネットワークカメラ&クラウドゾーン、AI・映像解析ゾーン、災害対策ゾーン、IoT・情報セキュリティゾーン、店舗・オフィスセキュリティゾーンの6ゾーンが設定されている。

なお、出展申込締切日は2019年10月15日までとなっている。

インディペンデント・エクスプレス・カーゴ社、貨物を保護するためにAvigilon社製AIテクノロジを採用

https://www.asmag.com/showpost/28493.aspx?name=news

Avigilon社は、アイルランドのダブリンでインディペンデント・エクスプレス・カーゴ社のセキュリティに選ばれたと発表しました。インディペンデント・エクスプレス・カーゴ社は、アイルランド最大のパレット配送事業者の1つで、全国25拠点と1,000を超える顧客を抱える全国の輸送ネットワーク網および完全なサードパーティ・輸送提供業者として活動している。

約36,870㎡の敷地にある15万㎡の倉庫で構成されるダブリンの敷地全体のセキュリティを向上させるため、インディペンデント・エクスプレス・カーゴ社はインテグレータのUsee.ie社と協力して、完全なAvigilonセキュリティ・ソリューションを導入した。新システムはAvigilon Control Center（ACC）映像管理ソフトウェアを採用している。これはセキュリティ・オペレータに中央管制室から映像をより効率的に管理する方法を提供している。

ACCソフトウェアには、Avigilon Appearance SearchやUnusual Motion Detectionテクノロジなどの高度な人工知能（AI）および映像解析機能を含まれている。さらに、H4 Pro、H4マルチセンサ、H4Aバレットと自己学習型映像解析機能を備えたAvigilonカメラの組み合わせを採用し、セキュリティ・オペレータはリアルタイム分析の利点を活用することができる。

高度なAI技術を活用した完全なAvigilonセキュリティ・ソリューションを実装することで、インディペンデント・エクスプレス・カーゴ社は運用効率の向上とそのサイト、資産、およびリソースのセキュリティの向上を実現した。

ハネウェル社、新しい業務用向け機能搭載管理ソフトウェアを発表

https://www.asmag.com/showpost/28491.aspx?name=news

ハネウェル社は、新しいカテゴリのソフトウェアで運用技術のための業務用向け機能搭載管理を開始した。これは、様々な企業が自社の運用からデータを収集し、分析し、それに基づいて行動する方法を改善する。

ハネウェル・フォージと呼ばれるソフトウェア・ソリューションは、資産および工程制御技術における同社の100年以上の専門知識を活用し、建物や航空会社また産業施設やその他の重要な資産および基盤の所有者および運営者が行なう仕事のやり方を変革する。

ハネウェル・フォージは、機器や工程そして人からの大量データを直感的で実用的な洞察に変換して、単一の画面から企業の業務を監視できるようにする。言い換えれば、これは顧客が効率と有効性そして事業の安全性を最適化するのを助ける。

ハネウェル・フォージは、既存のシステムの使用を可能にするハードウェアおよびソフトウェアにとらわれない方策で、実装するのが迅速で費用対効果が高いように設計されている。ハネウェル・フォージは、予測分析を利用して、メンテナンスで問題発生前に識別するのに役立つ。労働者がより生産的で熟練し、安全になることを可能にして、コストを削減し生産性を高める。同社は最新のサイバー・セキュリティによる保護を組み込むためにハネウェルフォージを引き続き開発している。

トランサム投資グループ、ペルコを買収

https://www.asmag.com/showpost/28398.aspx?name=news

業務を重視するミドルマーケットのプライベート株式投資企業トランサム投資グループは、シュナイダー・エレクトリック社から映像監視ソリューション提供企業ペルコ社を買収したと発表した。

ペルコ社は、カメラと録画および管理システムそしてソフトウェアとサービスを含む映像セキュリティ・ソリューションの設計、開発、製造の世界的企業。今回の買収で、同社の顧客と再販業者そして技術パートナーとの個人的な関わりにおいて、意義のある革新を伴う監視およびセキュリティ・ソリューションの開発と展開を促進します。

買収に関する取引条件は明らかにされていない。トランサムは、この取引のM&A顧問としてラザム&ワトキンス社と、負債顧問としてパーキンス・コイル法律事務所に代理を依頼した。ウェルズ・ファーゴ社はこの取引のために借入をした。

Hikvision社、英国のネットワーク・セキュリティ・カメラ・メーカ向け「デフォルト設定の安全」規格を歓迎

https://www.asmag.com/showpost/28476.aspx?name=news

Hikvision英国&アイルランド社は、ネットワーク映像セキュリティ製品がデフォルト設定で可能な限り安全であることを初めてユーザーに保証する「デフォルト設定による安全(Secure by Default)」規格を歓迎している。「デフォルト設定による安全」規格は、2019年6月20日にIFSECで英国の監視カメラ・コミッショナーのトニー・ポーター氏により初開催の全国監視カメラデーの一環として開始された。

セキュリティ・コンサルタントのマイク・ギレスピー氏によると、新しい規格の背景にある概念は、ネットワーク映像製品が可能な限り最も堅牢でサイバー・セキュリティに最適な形式で業者に出荷され、デフォルト設定は初回使用時の脆弱性を最小限に抑えるというもの。

Hikvision社は、英国の監視カメラコミッショナーと他の4つの主要な映像監視メーカと共同で、これらの画期的な規格の開発プロセスへの参加を依頼された。「デフォルト設定による安全」規格は、英国内務省の監視カメラコミッショナーによる広範なサイバーセ・キュリティ提案内容の一部を構成している。

ダルマイヤー社、パノメーラ・システムでジェネテック社と連携

https://www.asmag.com/showpost/28427.aspx?name=news

カナダのテクノロジ企業ジェネテック社は、セキュリティとインテリジェンスそして運用を含む幅広いソリューション・ポートフォリオを提供している。ジェネテックSecurity Center(GSC)にダルマイヤー社製パノメーラ・システムを統合することで、実績のあるパノメーラの機能が、現在最も広く使用されている統合セキュリティ・プラットフォームのユーザで利用可能になった。これにより、広大な区域や広い空間的状況を観察し監視するための全く新しい可能性がユーザに提供される。

ダルマイヤー社製パノメーラのマルチ・フォーカル・センサ・システムは、2011年以来、広大区域の包括的な監視を可能にしている。パノメーラ・システムをバージョン5.7 SR4以降のGSCプラットフォームに統合することで、ジェネテック社のユーザはパノメーラ・ソリューションの利用が可能になる。なお、統合には通常のジェネテック社カメラ・ライセンスが必要となる。

パノメーラは、最大7つの個別センサと1つのオーバービュー・センサの画像を1つのカメラ・システムで全体的な画像に統合する。メガピクセルカメラとPTZカメラの組み合わせやマルチセンサ・システムなどの従来のソリューションとは対照的に、シーン全体の全領域が高解像度で包括的に監視することができる。全体的な動作の高解像度表示を維持しながら、オペレータは同時に複数の領域にズームインすることができる。

これにより、複雑で面倒なことが多いカメラ切り替えが不要になり、また、監視するカメラと画面の数を大幅に削減しながら、建物や区域のマップで不要な検索を行う必要がなくなる。これにより、カメラ・オペレータの作業がはるかに簡単にできる。さらに、全てのビューが高解像度で記録されているため、オペレータはバックアップ後に、アクション全体の詳細領域で非常に高い解像度でズームをいくつでも実行できる。これは、複雑な状況や、PTZやシングル・センサ・ソリューションでは不可能な法医学的評価の成功など、非常に重要な機能となる。

オプテックス、東京拠点を移転し、名称も変更

https://www.optex.co.jp/news/2019/0718.html

同社はこれまで、東京都新宿区西新宿に構えていた東京営業所を東京都港区海岸に移転する。また、東京営業所を東京支店に名称を変更する。今回の移転により、滋賀県大津市にある本社から東京拠点までのアクセスが改善される。

移転事業所名‥オプテックス株式会社東京支店
移転先住所‥〒105-0022　東京都港区海岸1-9-1
浜離宮インターシティ3F
電話‥03-5733-1722(代表) FAX‥03-5473-3990
業務開始日:2019年8月26日(月)

サイバーセキュリティ市場は2024年までに3000億米ドル超に

https://www.asmag.com/showpost/28277.aspx?name=news

グローバル・マーケット・インサイト社の新しい調査報告書によると、世界のサイバー・セキュリティ市場は現在の1,200億ドルから2024年までに3,000億ドルを超える市場へと成長すると見込まれている。

サイバー・セキュリティ市場は、セキュリティリスクを最小限に抑えるための企業間のニーズの高まりによって推進されています。企業が急速にクラウドプラットフォームや他のネットワーキング技術を取り入れているので、彼らは様々なサイバー攻撃に対してより脆弱になっています。サイバー犯罪に対する平均支出は大幅に増加しました。サイバー・セキュリティ・ソリューションに対する組織の平均支出額は2017年に23%以上増加し、1170万ドルを超えた。サイバー・セキュリティ・ソリューションにおける予算配分の増加は、サイバー・セキュリティ市場の成長を牽引している。

様々なモバイルおよびワイヤレス機器の浸透が高まっているため、サイバー・セキュリティ市場の成長が促進されている。モバイル機器の価格低下と世界中での接続基盤の進歩により、企業と消費者の間でスマート機器の採用が推進されている。これにより、モバイル機器に対するサイバー攻撃数も同時に増加した。2017年には、モバイル機器へのサイバー攻撃が40%以上増加し、1か月に平均120万件を超える攻撃が発生した。このためエンドユーザと企業は、市場の成長につながるサイバー・セキュリティ・ソリューションを採用している。

IAAM市場は予測される期間にわたって年平均成長率17%以上で成長する。大企業や政府機関による支出の増加は、市場の成長を牽引している。さらに、セキュリティ上の懸念による厳格な規制順守の出現が増加し、市場の成長にプラスの影響を与えると予想される。基盤保護市場も、IoT機器の採用増加と電子メールおよびウェブベースのアプリケーションの使用増加により、予測を超えて大幅なペースで成長すると予想されている。

2017年には、大企業市場が世界のサイバー・セキュリティ市場シェアの60%以上を占めた。サイバー攻撃のリスクが高まっているため、大企業ではサイバー・セキュリティ・ソリューションの採用が推進されている。2017年には、大企業はサイバー・セキュリティ違反により平均1000万ドル以上を損失した。2017年のサイバー攻撃の平均コストは11%増加した。これにより、大企業は、サイバー攻撃のリスクを軽減するためのセキュリティ・ソリューションを採用するようになった。中小企業市場は、従業員の生産性を向上させるためのBYODポリシーの広範な採用により、高い成長率が見込まれると予想されている。

輸送市場は、予測される期間にわたって年平均成長率15%以上で成長すると見られていう。スマート輸送やIoTおよびその他の再構築イニシアチブの使用は、巨大なシステムからより広い攻撃面を生み出すことによってリスクをさらに高めている。運輸および物流会社の業務が中断されると、かなりのダウンタイムと収益の損失が生じる可能性がある。これにより、運送会社はサイバー・セキュリティ・ソリューションを導入するようになった。IT&テレコム部門も、一本化したコミュニケーション・サービスを提供するために使用される機密の顧客データを扱うため、急速に成長すると予測されている。

2017年の世界のサイバー・セキュリティ市場で欧州地域は20%以上のシェアを占めた。欧州市場は、政府による投資の増加とサイバー・セキュリティ基盤を強化するための官民の連携により、成長すると予想されている。さらに、企業にセキュリティ対策の採用を義務付けている支援的な政府の方針やコンプライアンス規制の導入もある。アジア太平洋地域のサイバー・セキュリティ市場は、年平均成長率20%で成長すると予測されている。複数の産業分野にわたる広範なデジタル化とスマートフォン・ユーザの増加が、この地域の成長を牽引している。

日本万引防止システム協会、通常総会を開催し、会長と副会長を選任

http://www.jeas.gr.jp/

日本万引防犯システム協会は、2019年6月6日に通常総会を開催し、新たに選任された会長ならびに副会長が就任した。今回就任した会長ならびに副会長は下記の通り。

会長（新任）　稲本義範氏（高千穂交易株式会社）
副会長（再任）　三宅正光氏（株式会社三宅）
副会長（新任）　近江元（NPO法人 全国万引犯罪防止機構）

また、新会員としてアドセック株式会社、株式会社セキュリティデザイン、パナソニック システムズ ソリューションズ ジャパン株式会社の3社が加わった。

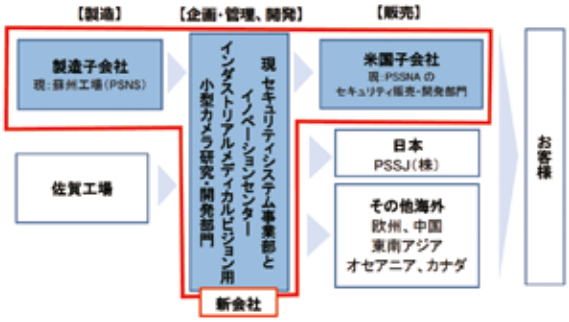
パナソニック、セキュリティ・システム事業の新会社を設立

https://news.panasonic.com/jp/press/data/2019/05/jn190531-1/jn190531-1-1.pdf
https://www.polaris-cg.com/wp/wp-content/uploads/news/20190531_SFC_J2-1.pdf

パナソニックは、国内外のセキュリティ・システム事業を担当する新会社の設立及びポラリス・キャピタル・グループとの戦略的資本提携に関する契約を締結した。

■新会社について

新会社は、コネクティッドソリューションズ社セキュリティ・システム事業部を母体に、イノベーション・センターのインダストリアル・メディカル・ビジョン用小型カメラ研究・開発部門を加えて設立する。また米国のパナソニック システムソリューションズ ノースアメリカ(PSSNA)のセキュリティ販売・開発部門を母体として新たに設立する会社と、セキュリティカメラなどの製造を担当する中国のパナソニック システムネットワークス蘇州(PSNS)を新会社の子会社とする。



●新会社名　パナソニックi-PROセンシングソリューションズ株式会社
(Panasonic i-PRO Sensing Solutions Co., Ltd.)
●発 足 日　2019年10月1日(予定)
●代 表 者　未定
●本社所在地　未定
●株　　主　ポラリス第四号投資事業有限責任組合等(80%)、
パナソニック(20%)
●主要事業　監視システム事業(インテリジェントサーベイランス)
業界特化事業(パブリックソリューション)
モジュール事業(インダストリアル&メディカルビジョン)

本取引に伴い設立されるSPC(特別目的会社)が承継会社の株式の100%を保有し、ポラリスが運用するファンドおよび当社は当該SPCの株式をそれぞれ 80%及び 20%保有する予定。

なお新会社設立後は、米国では新会社が直接、日本国内はパナソニック システムソリューションズ ジャパン株式会社が、上記以外の欧州、中国、東南アジア、オセアニア、カナダ、その他の地域では、現在販売を担当するパナソニックの各地域販売会社がそれぞれ新会社と契約を締結し、パナソニック・ブランドのセキュリティカメラやソフトウエアなどを顧客に提供する予定。

マイルストーンシステムズ社、新たに研究開発担当副社長を任命

https://www.asmag.com/showpost/28335.aspx?name=news

マイルストーン・システムズ社はトム・ビエア氏を新しい研究開発担当副社長として発表した。同氏はマイルストーンシステムズ社映像管理ソフトウェアの計画と開発そしてテストとリリースを監督し、コペンハーゲンとバルセロナそしてソフィアにいる従業員を統括する。

トム・ビエア氏の主な業務の1つは、マイルストーン・システムズ社による投資収益率を45%向上させ、スマート・ソリューションに対する市場の需要を満たすための独自の革新性の創造能力を強化することだ。投資には、ディープ・ドライバ・デバイス統合、高度なビデオ・レンダリング、IoTおよびメタ・データ・ソース、オンライン・サービス、高度なデータ管理、そしてプラットフォームであるソフトウェア開発キット(SDK)の開発能力が含まれている。

トム・ビエア氏は、プラットフォーム・ベースおよび市場を活性化させる企業で働いてきた経験が豊富で、マイルストーン・システムズ社に不可欠な理念をもたらす。「プラットフォーム経済とプラットフォーム・ビジネスモデルの力は、画期的なものだと思う。マイルストーン・システムズ社がプラットフォームの指揮者としてユーザを導くことで、業界がインテリジェントなソリューションを一緒に構築して市場を拡大することで、革新的な機能をユーザに提供すると同氏は抱負を述べている。

さらに、トム・ビエア氏は、大規模でミッション・クリティカルなIT開発および運用の経験が豊富で、サクソ銀行のグローバルIT基盤やアプリケーション基盤、事業支援、そしてITサービスを担当していた。またデンマークTV 2社CIOとして、データ統合およびサービス、IT運用、およびテレビ技術を担当していた。

NTT PCコミュニケーションズ、ASP・SaaS（IoTクラウドサービス）情報開示認定制度において「セキュアカメラクラウドサービス」が認定第一号を取得

https://www.nttpc.co.jp/press/2019/07/201907111500.html

NTTPCコミュニケーションズのIoTサービス「セキュリティカメラクラウドサービス」は、特定非営利活動法人ASP・SaaS・IoT クラウド コンソーシアム(略称：ASPIC)から2019年7月11日に発表された「ASP・SaaS（IoTクラウドサービス）情報開示認定」において、第一号となる認定を取得した。

認証制度名称：ASP・SaaS（IoTクラウドサービス）情報開示認定制度
認 定 番 号：IoT0001-1907
認定サービス：セキュアカメラクラウドサービス
認 定 機 関：ASPIC
認　定　日：2019年7月10日
認 定 期 間：2019年7月10日～2021年7月9日

今回、認定第一号を取得した「セキュアカメラクラウドサービス」は、NTTPCが2011年からサービス提供している、複数拠点に設置したネットワークカメラから送られてくる高精細な画像と音声をローカルとクラウドに記録し、本社や本部で同時に確認、検索、閲覧できるクラウド型ネットワークカメラサービス。店舗や工場、オフィスなどの防犯・セキュリティ監視としてだけでなく、店舗マーケティングや現場育成を含めた店舗改善、また河川・水路の遠隔監視による業務効率化など様々な用途に活用できる。既存のインターネット回線を利用したVPN接続、または閉域網で接続することでセキュアな環境を実現、証跡として活用できる高品質な画質と長期保存を両立できるようにサービス設計がされている。

今回、本サービスのセキュリティ対策や信頼性についての情報等が適正に開示されていると評価され、第一号認定を取得することができた（「セキュアカメラクラウドサービス」は、現時点でIoT分野の本認定を取得している唯一のサービス）。

これにより、自治体や企業等が、より安心・安全にサービス導入でき、さらなる利用の促進が見込んでいる。

※セキュアカメラクラウドサービス

複数拠点に設置したネットワークカメラから送られてくる高精細な画像と音声をローカルとクラウドに記録し、本社や本部で同時に確認、検索、閲覧できるクラウド型ネットワークカメラサービス。店舗や工場、オフィスなどの防犯・セキュリティ監視としてだけでなく、店舗マーケティングや現場育成を含めた店舗改善など様々な用途に活用できる。既存のインターネット回線を利用してVPN接続することでセキュアな環境を実現、証跡として活用できる高品質な画質と長期保存を両立できるようにサービス設計がされている。

https://www.nttpc.co.jp/service/scc/

※「ASP・SaaS（IoTクラウドサービス）情報開示認定」の概要

「ASP・SaaS（IoTクラウドサービス）の安全・信頼性に係る情報開示認定制度」は、今後、ASP・SaaS（IoTクラウドサービス）の利用を考えている企業や地方公共団体などが、事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定するもの。

http://www.cloud-nintei.org/asp-iot/index.html

NECインド現地法人、ケララ州警察に自動指紋認証システムを提供

https://jpn.nec.com/press/201906/20190618_01.html

NECのインド現地法人であるNEC Technologies India Private Limitedは、インド先進コンピューティング開発センター(C-DAC)から、自動指紋認証システム(AFIS)を受注し、同国のケララ州警察に提供する。今回提供する指紋認証システムは、NECの生体認証「Bio-IDiom」の中核技術である指紋認証技術を活用している。

本システムは、ケララ州警察が採取した指紋と犯罪捜査用の指紋の中央データベースとを照合するために使用される。警察署や地区警察本部を含む州全域の600以上の警察施設が、本システムにアクセスすることが可能になる。

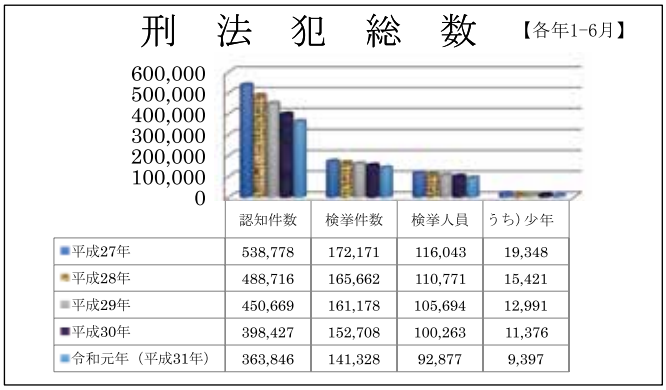
本システムは、従来からの迅速かつ正確な指紋照合を提供することにより、州警察の効率的な捜査を支援するもの。このシステムにより、犯罪現場で採取された断片的な指紋の質を向上させ、中央データベースとの照合を可能にする。

警察庁、2019年1-6月の犯罪統計(暫定値)を発表

https://www.npa.go.jp/toukei/keiji35/new_hanzai31.htm

2019年1-6月における日本の刑法犯総数は363,846件で、前年比91.3%と8.7%の減少となった。詳細を見ると下記の内訳となる。

- 凶悪犯(殺人、強盗、放火、強制性交等)‥2,352件(前年比増減率-5.1%)
- 粗暴犯(凶器準備集合、暴行、傷害、脅迫、恐喝)‥27,967件(前年比増減率-3.2%)
- 窃盗犯(侵入盗、乗り物盗、非侵入盗)‥257,183件(前年比増減率-9.1%)
- 知能犯(詐欺、横領、偽造、汚職、斡旋利得処罰法、背任)‥18,132件(前年比増減率-14.8%)
- 風俗犯(賭博、猥褻)‥3,952件(前年比増減率-14.0%)
- その他の刑法犯(占有離脱物横領、公務執行妨害、住居侵入、逮捕監禁、略取誘拐・人身売買、盗品、器物損壊)‥54,260件(前年比増減率-7.8%)



	認知件数	検挙件数	検挙人員	うち)少年
平成27年	538,778	172,171	116,043	19,348
平成28年	488,716	165,662	110,771	15,421
平成29年	450,669	161,178	105,694	12,991
平成30年	398,427	152,708	100,263	11,376
令和元年（平成31年）	363,846	141,328	92,877	9,397

【本誌の見解】

■犯罪件数の減少とその背景

刑法犯認知件数は2002年の2,853,739件をピークに一貫して減少しており、犯罪情勢には一定の改善がみられる。その背景として、店舗や住居また市街地などにおける監視カメラの設置台数の増加により、犯罪防止効果が高まったことも考えられる。さらに、カメラ解像度の向上により人物特定化が容易になっている状況も犯罪防止効果に貢献していると言えるだろう。

■深刻化する特殊詐欺とサイバー犯罪

特殊詐欺とは面識のない不特定の者に対し、電話その他の通信手段を用いて、預貯金口座への振込みその他の方法により、現金等をだまし取る詐欺を指す。特殊詐欺の件数および被害金額の両面で深刻な状況が継続している。

また、インターネットバンキングに係る不正送金事犯等のサイバー犯罪やサイバー空間における脅威も増大している。さらに、重要社会基盤の基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロ、情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバー・インテリジェンス(サイバーエスピオナージ)といったサイバー攻撃による犯罪が増加することが懸念されており、サイバー空間における脅威は深刻化している状況にある。

CNLソフトウェア社、MOBOTIX社と強化型PSIMで提携

https://www.asmag.com/showpost/28438.aspx?name=news

CNLソフトウェア社は、IFSEC International 2019のMOBOTIX社ブースでエコシステム・パートナーとしてIPSecurityCenter PSIMソリューションの最新の機能強化をした、最高レベルのサイバー・セキュリティを備えたセキュリティ・ソリューションを発表した。CNLソフトウェア社は、同社のPSIM技術が、大規模な連合システムが重要な国内社会基盤をサポートすることを可能にするために、状況認識、センサ、システムおよび装置の広大な状態の統合および管理を強化する方法を実証している。

15年以上の開発実績を持つIPSecurityCenterは、その機能、性能、および高度さでPSIM市場をリードし、最近プラットフォームに高度な生体認証を追加した継続的な開発プログラムを誇っている。

毎年新たな脅威が発生するとそれに対抗するための新技術の開発に、数十億ドルが費やされている。また2025年までにオンラインで75億個のモノのインターネット(IoT)機器が登場すると予測されている。これは1人あたり約10台の機器に相当する。CNLソフトウェアは、これが業界にとってどのような意味を持つのか、そしてセキュリティ担当者がコントロールルーム内でより多くの情報を準備するのにどのように役立つかを次のように説明している。

「私たちは、IFSECでMOBOTIXとパートナーを組むことができ、

彼らの広範なエコシステムと技術的なパートナーシップを構築することができるかどうかを議論できることを楽しみにしている。セキュリティ、生命の安全、設備管理の各業界で最先端技術を駆使して開発している。当社はオープン・プラットフォームを開発し、パートナーと協力してデータを活用して複雑なセキュリティの課題を解決する最先端のソリューションを作成できるオープン・アプローチを採用している」。

IPSecurityCenterは、組織の全てのミッション・クリティカルなセキュリティ・システムの単一のビュウを提供し、緊急時の備えを強化し、必要な場所に情報を提供し、セキュリティ対応を強化するための工程解説を提供している。自動化による時間の節約と効率化の利点を超えて、IPSecurityCenterは現代のセキュリティ部門にとって不可欠なプロセスを可能にしている。具体的にはスケジュールされたリポート、ダッシュボードの概要、インシデント記録、継続的な工程改善への取り組み、トレーニング・ドリル、システムヘルスチェックなどを含む。

モジュール型データセンタの市場規模、2025年までに500億ドル超と予測

https://www.asmag.com/showpost/28317.aspx?name=news

グローバル・マーケット・インサイト社の新しい調査報告によると、モジュール型データセンタ市場は2025年までに500億米ドルに達すると予測されている。

IT施設で発生する主な費用には、展開や設置、運用そして保守費用などがある。これらのうち、小規模企業は資本支出を削減しながら容易に事業を展開し維持することができる。大規模施設では、高い運用経費と保守サービスを必要とする最新の技術が組み込まれている。

事業運営におけるエッジ・コンピューティングの需要の高まりは、モジュール型データセンタの市場シェアの拡大に繋がる。事業は費用対効果が高く、ネットワーク・ソースに近いIT基盤に依存しており、データ転送速度と正確性が向上している。エッジ・コンピューティングは、小規模の分散型サーバを展開することで、コンピュータ、スマートフォン、その他の機器がデータを利用する場所により近いネットワークの中心からエッジに処理能力をもたらすという点で、従来のデータセンタとは異なる。プレハブ設備は、展開の容易さ、独自の設計とアーキテクチャ、および移植性などの幾つかの機能を提供している。これらのモジュール型データセンタは、必要に応じて地域のデータセンタにリンクし、ユーザ・エクスペリエンスを向上させることで、待ち時間と帯域幅の問題に対処するために遠隔地/サイトに設置されている。このような要因がエッジ・コンピューティングの採用を促進し、モジュール型データセンタの市場規模を拡大している。

ITおよび通信業界企業は、データセンタの迅速な展開を必要としている。モジュール型設備は、ネットワーク接続、サーバ、電力線、監視装置、火災検知装置、セキュリティ、保管、および冷却と完全に統合されている。ユーザは、これらの追加のハードウェア構成機器を個別に購入し、それらをインストールおよび管理するために社内の技術チームを任命する必要はない。モジュール型データセンタ市場では、ITおよびテレコム業界が、事業運営のスケーラビリティと柔軟性を向上させるためにこの施設を広く採用していることを目の当たりにしている。急速な事業拡大または事業基盤の移転に伴い、企業はIT機器に依存しているため、容易に新しい場所に移動または配置することができ、市場の成長が加速する。

モジュール型データセンタ市場に参加している主要企業は、シスコシステムズ社、IBM社、Baselayerテクノロジ社、ファーウェイ社、ヒューレット-パッカード・エンタープライズ社、デル社、シュナイダー・エレクトリック社、SGI社、IOデータセンタ社、BladeRoomグループ、ヴェリティブ社、Cannon、イートン社、フェレックス・エンクローシャ社、コムスコープ社などがある。

独国メッセフランクフルト社、欧州でセキュリティ展示会を初開催

https://intersec-building.messefrankfurt.com/frankfurt/en.html

Intersec Buildingは、近年のビルやスマート・シティにおける安全との連携およびセキュリティ技術への需要の高まりに応えて、2020年3月8日から13日までの日程でドイツ連邦共和国ヘッセン州フランクフルイン市において初開催される。Intersecブランドを冠にしたイベントを欧州で開催するのは初。

開催の背景にあるのは、情報化基盤には保護が必要であり、安全およびセキュリティ技術の成長分野は、様々な建築サービス区分にとってますます不可欠な側面となっていることだ。

バッファロー、Windows Server IoT 2019 for Storage搭載の法人向けNAS 6シリーズを発売

https://www.buffalo.jp/press/detail/20190612-02.html

本製品は、マイクロソフト社が提供する最新の組み込みシステム向けOS「Windows Server IoT 2019 for Storage」を搭載する法人向けNAS。

【主な特徴】

■「シャドウコピー」の搭載

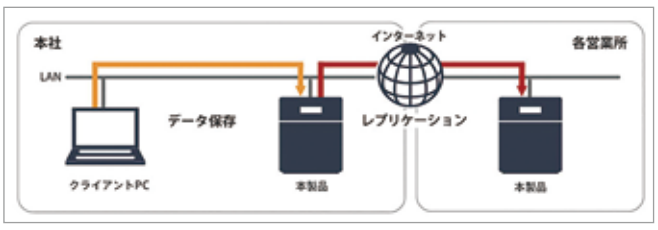
Active Directoryサーバに登録されているアカウント情報を利用したファイル・フォルダのアクセス制限に対応し、大規模なユーザ・グループのアクセス管理を容易にするActive Directoryの完全連携や、管理者が設定したスケジュールに基づいて共有フォルダのスナップ・ショットを作成し、ユーザが誤って共有フォルダのファイルを変更してしまった場合などに、履歴をさかのぼって変更したファイルを以前の状態に復元できる「シャドウコピー」を搭載。

■「DFSレプリケーション」機能の搭載

Active Directory環境下で遠隔地の本商品にネットワーク経由で自動同期する「DFSレプリケーション」機能、マイクロソフトが提供するクラウドストレージサービス「Microsoft Azure」との連携機能など、Windowsとの親和性の高さが特徴となっている。

■CALの別途購入が不要

Windows Server OS搭載サーバへのアクセスには、ユーザまたはデバイスごとに有料のCAL（クライアントアクセスライセンス）が必要となるが、本製品が搭載する「Windows Server IoT 2019 for Storage」では、クライアント数に応じたCALを別途用意する必要がなく、ファイルサーバとして導入・運用コストを大きく削減できる。



■10Gbps（規格値）の高速イーサネット「10GbE」に対応

ファイルの読み書きやバックアップ作業の高速化を実現。また、IEEE802.3bz規格にも対応しており、多くのビルで既に敷設されているカテゴリー6ケーブルやカテゴリー5eケーブルの環境であっても、同規格に対応したスイッチに変更するだけで、5GbEや2.5GbEのスピードで利用できる。

■エラー訂正機能「ECC」対応メモリを8GB搭載

メイン・メモリにはエラー訂正機能「ECC」（Error Checking and Correction）に対応したメモリを8GB搭載し、複数のアプリケーションを追加して運用する場合のメモリ不足を軽減。バックアップやウイルス・スキャン・ソフトウェアを同時使用した場合にも安定した運用を可能にする。

■「WSH5620DNS9シリーズ」は、国内で開発されたハードウェアRAIDを搭載

Windows Server IoT 2019 for Storage標準のソフトウェアRAID機能では未対応のRAID 6に対応。専用のコントローラでRAID処理を行うためCPUへの負荷が小さく、ソフトウェアを複数同時に使用した場合でもソフトウェアRAIDに比べて高速で安定した処理が可能。

■セキュリティ・ソフトとバックアップ・ソフト同時使用時のバックアップを大幅に時間短縮

ソフトウェアRAIDモデルと比べて約69%も時間短縮する。加えて、ハードディスク交換時のRAIDリビルド中のシステムへの負荷を軽減し安定したパフォーマンスを維持する。また、RAID 6設定時でもRAID 5設定時と同等のパフォーマンスを実現する。OS領域用SSDを搭載しており、ハードディスク全てをデータ領域として利用できる。また、RAID設定変更時もOS再インストールなどの手間が発生しない。

■Windows OSのデータ暗号化機能「BitLocker」に対応

万一のハードディスク盗難などの際にも他のパソコン・NASではデータが読み出せないよう暗号化が施されるため情報漏洩の防止に役立つ。また、マイクロソフト社が推奨するTPM（Trusted Platform Module）2.0チップを搭載しており、再起動毎の手動によるBitLocker解除は不要。暗号キー保存用USBメモリも必要ない。

アクシスコミュニケーションズ、エッジ分析ソフトウェア「AXIS Live Privacy Shield」を発表

「AXIS Live Privacy Shield」は、最大でフル·フレーム·レートに対応し、ビデオ·ストリーム内に映っている人の部分をリアルタイムでマスキングする。このソリューションは、優れた信頼性と高い費用対効果を発揮する。これにより、プライバシーに関するルールや規則を遵守できるようになるとともに、ユーザは施設内での人の動作や活動を見ることができる。このアプリケーションは所定のアクシス社製カメラで直接動作するため、高額なサーバが不要で、システム規模の拡大·変更を簡単に行うことができる。

AXIS Live Privacy Shieldは、カメラのライブ·ビューと予め設定された背景シーンとを比較し、変更のあった領域に詳細で動的な透明マスクを適用する。すなわち、動いている人や物が背景上に透明に表示される。これらの全てのプロセスは瞬きをするよりも速く行われ、映像上の個人データが効果的に取り除かれる。

初期設定では、動的マスキングはカメラの全ての視野に適用される、例えばベルトコンベヤが運んでいる物を見えるようにしたい場合など、ユーザはマスキングを適用しない領域を定義することができる。動的なマスキングの無いビデオ·ストリームを別途配信するようにシステムを設定することもでき、インシデントが発生した場合でも許可された閲覧者は映像の詳細部分にアクセスすることができる。

AXIS Live Privacy Shieldは、遠隔による映像モニタリングや録画において、プライバシー·ルールや規定で問題となりえる領域を撮影する場合に適している。このシステムは、映像監視が主にプロセス監視に使用される際の処理、製造、輸送などの用途のほか、小売店舗、医療機関、教育機関、官公庁施設にも応用できる。

■主な利点:

●プライバシーの保護
●高フレーム·レートで信頼性の高いリアルタイムの動的なマスキング
●費用対効果に優れ、パフォーマンスの高い、エッジベースのソリューション
●簡単な設置、設定、管理
●良好で安定した照明条件のある屋内向け

■URL・・https://www.axis.com/ja-jp/products/axis-live-privacy-shield

---

記事訂正とお詫び

弊誌2019年5/6月号29ページに掲載した「SECURITY SHOW 2019リポート」の記事の一部を下記の通り訂正し、関係各社にお詫び申し上げます。

アクシスコミュニケーションズ

映像監視システムの世界トップブランドであるアクシス社のブースにおいては、主に小規模システム向けエンドツーエンド·ソリューションとして様々な提案事例を展示していた。これは、流通業界や店舗経営層の来場者が多いSECURITY SHOWを意識した展示内容だと見て取れる。同社はAXIS CompanionやAXIS Camera Stationと同社製ネットワークカメラの構成によるエンドツーエンド·ソリューションなどを提供しているが、今回同社ブース内ではAXIS Camera Station および同ソフトウェア搭載のレコーダ(AXIS S10 シリーズ、AXIS S20 シリーズほか)による、中規模システム向けのエンドツーエンドソリューションを展示していた。

ADLINK社、MCMソリューションをアップグレード

https://www.adlinktech.com/Products/SearchResult.aspx?lang=ja&SiteID=17110823495731470&key=MCM

本製品は、ダッシュボードを使ってセンサ管理、データ収集、エッジ・プラットフォーム、振動解析を一括操作できるリモート・ファシリティ・インフォメーション・ダッシュボードの提供により、同社のMCM機器環境監視用ソリューションがアップグレードとなった。ユーザは複数のシステム装置の監視およびマシン動作のリアルタイム情報の管理を同時に行い、停止時間の削減と生産能力の拡大に役立つ効率的でダイナミックな予防保全戦略を構築できる。

強力なMicrosoft Azureクラウドプラットフォーム構造とSaaSサービスを採用したADLINK社製DataConnect Proは、より高精度の通知に役立つスペクトル機能を利用した専用の内蔵機器監視システムを提供する。同製品はプログラムの開発やアーキテクチャの変更を必要せずに、様々なフィールドに容易に配置できる。システム装置を拡張したり、追加したりする場合、システム全体の再配置や再構築は必要ではなく、ダッシュボードを使用した既存機器の情報によって拡張の管理が可能で、拡張費用を大幅に削減できる。

【MCMソリューションの特長】

- オールインワン設計の採用で配線の手間やコストを削減できるだけでなく、最小のフットプリントで装置の間近に迅速かつ容易に設置できる。
- プログラミング不要な直感的な指示により、ダッシュボードのカスタマイズとアラーム規則の作成が可能で、開発のための労力と時間の削減を実現。
- 機器異常時の高精度な予測アラートで、予期せぬ故障や多額の損失をもたらす停止時間防止が可能。

【問い合わせ先】ADLINKジャパン

TEL：03-4455-3722　　Email：japan@adlinktech.c

VIVOTEK社、スマート360 VCA 深層学習テクノロジーを搭載 H.265フィッシュアイ・カメラを発表

https://www.forcemedia.co.jp/vivotek/fisheye/fe9191

https://systemk-camera.jp/camera/lineup/vivotek/fe9191/

https://www.forcemedia.co.jp/vivotek/fisheye/fe9391-ev

https://systemk-camera.jp/camera/lineup/vivotek/fe9391-ev/

今回発表した製品は、フィッシュアイカメラFE9191とFE9391-EV。この2機種の業務用昼夜対応12メガピクセル・フィッシュアイ・カメラは、死角ゼロの360度サラウンドビュウを提供し、VIVOTEK社独自開発の深層学習テクノロジー「スマート360 VCA」を装備している。

このテクノロジーには、侵入検知、群衆検知および徘徊検知が含まれている。これらの機能を装備したことで、フィッシュアイカメラFE9191とFE9391-EVは単なる映像機器から先進的な通知装置に変わり、その過程で誤警報を大幅に削減した。

IDIS社製フルHD マイクロ・ドーム型ネットワークカメラDC-C4212RX

■主な特長

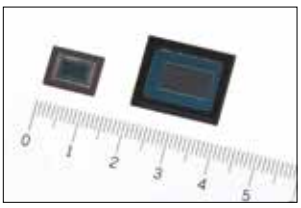
- DirectIP NVRで簡単インストール
- フルHD (1080p) 解像度
- 電動バリフォーカルレンズ (f=2.8mm)
- PoE (IEEE 802.3af クラス1)
- デイ&ナイト (ICR)
- トゥルー・ワイド・ダイナミック・レンジ (WDR)
- IR LED (距離: 15m)
- 設置用の3軸機械設計
- ONVIFをサポート

■セキュア

URL：secureinc.co.jp　TEL：03-6911-0660

SONY ソニー、4K解像度を実現するCMOSイメージセンサを商品化

https://www.sony.co.jp/SonyInfo/News/Press/201906/19-058/index.html



『IMX415』(左) 『IMX485』(右)

【主な特長】

■積層型CMOSイメージセンサ『IMX415』

セキュリティカメラ向けとして、世界最小1/2.8型で4K解像度を実現するCMOSイメージセンサ。独自の高感度・低ノイズ技術を駆使し、画素サイズを従来比約80%の1.45um角に微細化することで、1/2.8型の小型でありながら、低照度性能が従来のCMOSイメージセンサに比べて1.5倍向上した。また、低ノイズ回路を搭載した積層型構造を採用することで、暗いシーンでも鮮明な映像の撮像が可能となる。1/2.8型は、小型で設置場所を選ばず、セキュリティカメラ用途で需要の高いラインアップ。

■1/1.2型4K裏面照射型CMOSイメージセンサ『IMX485』

4K解像度で高い低照度性能を実現する、1/1.2型のCMOSイメージセンサ。画素サイズを従来比2.1倍の2.9um角にし、最新の画素技術を適用した低ノイズ化により、低照度性能が従来のセキュリティカメラ向けCMOSイメージセンサに比べて3.3倍と飛躍的に向上した。これにより、暗いシーンでも物体を正確に検知し撮像できる。

【サンプル価格(税抜き)】

■『IMX415』 2,500円 ■『IMX485』 10,000円

【主な仕様】

型名		IMX415	IMX485
有効画素数		3864(H)×2192(V) 約 846 万画素	3864(H)×2176(V) 約 842 万画素
イメージサイズ		対角 6.43mm (1/2.8 型)	対角 12.86mm (1/1.2 型)
ユニットセルサイズ		1.45um(H)×1.45um(V)	2.9um(H)×2.9um(V)
フレームレート	全画素	10bit 90fps、12bit 60fps	10bit 90fps、12bit 60fps
感度(標準値 F5.6)		2048 Digit	9530 Digit
センサー飽和信号量(最小値)		3895 Digit	3895 Digit

2019年のアクセス・コントロール技術の新機能

ユーザのさらに高い利便性とセキュリティの要求により、アクセス・コントロール市場での新技術の採用が進み2019年も成長する。

●エイファ・ストロム(フリー記者)

市場調査会社メムーリ社によると、アクセス・コントロール製品の世界市場は2018年に8%成長し、約75億米ドルの売り上げを記録した。これは、IPネットワーキング製品、サービスとしてのアクセス・コントロール（ACaaS）、生体認証読取機およびID管理ツールが牽引した。同社は他の物理セキュリティとビル・オートメーション・システム（BAS）との統合により、これまで以上の成長を予測している。

2019年にはワイヤレス・ロックやアイデンティティ・ベースのシステムが増加

ワイヤレス・ロックの採用の増加から認証とアクセス管理の統合に至るまで、アクセス・コントロール業界関係者は2019年に出現する傾向について議論している。

全般的にアクセス・コントロール市場は最新の技術動向の採用に遅れが見られる。採用が遅くなる理由の1つは、企業などの組織が、携帯電話などの他のテクノロジを更新するほど定期的にアクセス・コントロールシステムを更新しないことにある。

AMAGテクノロジ社APAC営業部長ギャオピン・シャオ氏によると、従来のアクセス・コントロールは依然として他の分野より10年遅れている。それにもかかわらず、シャオ氏はセキュリティの利点に対する意識の高まりが2019年に新技術を受け入れると考えている。「これらの新技術にはより厳格な規制があり、そして今後12～18ヵ月以内に安全な環境を提供するには、重要な場所で近接カードやMifare CSNカードを使用したり、技術を更新したりするなど、従来のプラットフォームに関連するリスクがあることを理解するべきだ」と話している。

アイデンティヴ社製品管理責任者ジェイソン・スピールフォーゲル氏は、2019年にワイヤレス・ロックの使用が拡大することを期待している。「ワイヤレス・ロックは、読取機とロックの結合を表すだけでなく、ワイヤレス・ロックの使いやすさも表している。運用上のアクセス・コントロール・システムをインストールすることで旧来の有線方法にすることもできる」と同氏は述べている。

同氏はまた、ホスピタリティ業界は数年前にこの方向に移行していることを付け加え、現在では主な商業/産業分野でも急速に追随している。ワイヤレス・ロックは、即座に一時的なアクセス・コントロール環境を確立するための方法でもある。

ジェムアルト社アイデンティティ&アクセス管理担当副社長フランソアズ・ラズニア氏は、2019年の興味深い開発として、物理およびデジタルの両方の環境においてユーザがIDベースのアクセス・コントロールを使用している点を強調している。


ジェムアルト社アイデンティティ&アクセス管理担当上級副社長フランソアズ・ラズニア氏

「各アクセス・トランザクションを個別に見るのではなく、各アクセス・コントロール・システムは異なるIDシステムに依存し、グローバルなアクセス・コントロール・プラットフォームは様々なIDシステム（エンタープライズ・アプリケーション用AD、物理的アクセス・データベース、生体認証など）から給電し、情報化する。物理的およびデジタルの両方のコンテキスト情報を使用したグローバル・アクセス・ポリシーに基づく意思決定が考えられるとラズニア氏は説明している。

同氏はまた、認証とアクセス管理の統合が今後数年間で勢いを増すことに期待を寄せている。「認証は、組織が必要とするリスク軽減を実現し、エンドユーザのために複数のアプリにログインする負担を軽減化するために、アクセス管理により密接に統合される必要がある」と述べている。「これは、絶えず拡大する脅威の存在と高まる脅威の水準により、アプリケーション段階でアクセス・セキュリティを提供するというこれまでにない要求により浸透している。脅威の存在が拡大しているのは、クラウドベースおよびウェブベースの配信が急激に拡大した結果だ。一方、過去数年間の侵害の範囲とその影響の範囲で、脅威の水準が高まっていることは明らかだ」。

アレジオン社国際技術&エンジニアリング担当副社長ヴィンス・ウェノス氏によると、今年注目される他の潮流には以下の通りだ。

- クラウド・ホスト・ソリューションの継続的な需要と採用
- 従来のオンプレミス・ソリューションに対するもの
- 電源管理と低コストコンピューティングの向上により、「エッジ」機器の情報化の向上
- モバイル・アクセスと、物理的および論理的セキュリティをさらに収束させる能力
- 高度な機械学習とAIそして生物測定学

カード・ベース認証からモバイル・アクセスへの移行

カード・ベース認証は、長い間アクセス・コントロール業界の主力だったが、エンドユーザはより安全で便利なアクセス方法を求め始めている。これらの懸念に対処するためにヒントを得た技術の一つがモバイル・アクセスだ。

業界関係者間での共通認識は、モバイル・アクセスが2019年に中心となることだ。BluetoothやPIRなどの技術がますます読取機に導入されており、ユーザは自分のポケットに携帯電話を入れたままにして、単に読取機に向けて手を近くに振ることで入場することができる。

IHSマーキッツ社では、今後5年間でのモバイル・アクセス市場の力強い成長を予測している。同社レポートによると、世界のモバイル認証情報のダウンロード数は、2017年から2022年の間に年平均成長率が100%超で増加すると推定している。現在設置されているアクセス・コントロール読取機の約20%は、2022年までにモバイル対応になると見ている。

「最も安全な環境特に商業/産業/住宅市場では、多要素認証スキーマの一部としてカードを引き続き使用するが、カードからスマートフォンへと移行して主要な認証情報として使用する」アイデンティヴ社製品管理部長ジェイソン・スピールフォーゲル氏は述べている。

ギャラガー・セキュリティ社英国&欧州地区担当責任者リチャード・ヒューイソン氏は、モバイル・アクセスはもはやギミックとは見なされず、その便利さとセキュリティの強化により注目を集めていると語った。同氏は、モバイルは複数のサイトにまたがって使用でき、資格情報をインターネット経由で遠隔送信できるなど、紛れもない利点をもたらしたと付け加えている。「これは、管理上の顧客にとって大きなメリットだ。それは全てのカード印刷から開放され、カードを目録化することができている」。

ジェムアルト社アイデンティティ&アクセス管理担当副社長フランソアズ・ラズニア氏は、電話がユーザの識別と認証だけでなく対話の中心となっている。そして物理的またはデジタル的なアクセス要求を開始する際には、グローバルなアクセス・ポリシーを構築し、全体的なユーザの移動に基づいてアクセスを決定する方が簡単だと述べている。

さらに、ギャラクシー・コントロール・システムズ社社長リック・カルザース氏は、アクセス・コントロール・システム映像付きのプッシュ通知がレビュー用に携帯電話に送信されるモバイル・アプリケーションを要求する顧客が増えていると述べている。ギャラガー・セキュリティ社ヒューイソン氏は、スマートフォンの普及はアクセスカードよりも明らかに優れていると考えている。アクセスカードを忘れたことに気付いた場合、何人が帰宅するでしょう?現実的には誰もいないと考えるでしょう。しかし、ほとんどの人は、自分の携帯電話を自宅に置いたままでいることに気付いたら帰宅するだろう。電話を使って商品の支払いをしたり、映画のチケットやレストランを予約したり、許可されているドアを通り抜けるように装備しないだろうか?」。

この見解には、ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏も同意している。「現在、携帯電話を組織内の特定のアクセス・レベルに統合する方法を模索しているエンドユーザから、モバイル・アクセス・コントロールの需要が高まっている。現代では、携帯電話は常に使用されている。モバイル・アクセスをオフィスや様々なレベルのアクセスに統合する機会がある」と彼は述べている。

TDSi社MDジョン・デイヴィス氏は、モバイル・アクセスは既に住宅で普及していると話す。いくつかのより大きなエンドユーザ組織が既にモバイル識別技術の準備として新しい読取機を買っていたことを示している。見積もりによると、2020年までにモバイル・アイデンティティ・読取機が市場の売り上げの約10%を占める可能性がある。

AMAG テクノロジ社APAC営業部長ギャオピン・シャオ氏は、セキュリティ部門が遠隔監視、アラームの設定、および従業員のシステムへの登録にモバイル・ソリューションを使用するなど、出入口だけでないアクセス・コントロールにも使用されていると述べている。

「モバイル・ソリューションは、開発および展開されているシステムの機能制御をユーザの手に提供している。その機能目的が受け入れられ、適応されていくだろう。さらにモバイルは門戸の開放にはまだ広く受け入れられていないが、やがて登場するだろう。大学やエネルギー/ユーティリティ市場などの遠隔ビルが存在する個別市場で採用されるようになるだろう」と話している。

このような利点にもかかわらず、ヒューイソン氏は、「カードの統制の欠如」に対する懸念のために、採用しないと考える分野、例えば英国の国民健康サービスおよび地方自治体があると考えている。

モバイル・アクセスの長所と短所のバランス

今年増加する傾向にあるモバイルアクセスソリューションの採用により、幾つかのモバイル・アクセス・ソリューションを実装する際に考慮すべき利点と課題

利便性は、モバイルアクセスの変換につながる最大の要因の1つだ。

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、「私たちの多くにとって、携帯電話を持っている方がバッジやキーカードを持ち歩くよりもはるかに簡単だ。特に、ホテルの環境などで大量に使用されると、無駄になる可能性がある。その他の利点としては、ほぼ即時の認証、高速で便利なアクセス、および多要素認証のための総所有コスト（TCO）の低下などがある」と指摘している。

ギャラクシー・コントロール・システムズ社社長リック・カルザース氏は、「クレデンシャル配信の手段が改善され、読取機自体のコストが下がっている。このため、今後のプロジェクトでモバイルアクセスを検討する企業が増えていると説明し、「我々は、モバイル・アクセス技術が引き続き受け入れられ、伝統的な近接技術からより多くの市場シェアを獲得すると直感している」と彼は付け加えた。

モバイル・アクセスは便利だが、履歴記録をモバイル機器に保存するかクラウド・サーバに保存するかについても考慮する必要がある。

AMAGテクノロジ社APAC営業部長ギャオピン・シャオ氏は、次のように述べている。「一部のベンダにとっては投資が高くなる可能性があるため、従来の物理カードによるソリューションとの比較も考慮しなければならない」。

マクスセス・システムズ社社長ナンシー・イスラス氏は、既存のカードおよび近接アクセス読取機の代わりになるには、モバイル認証情報アクセス読取機の速度と容量が少なくとも既存機器と同等の必要があると述べている。

AMAG社シャオ氏は、オフィス環境の課題の1つは、従業員、訪問者、請負業者を区別するために、従業員に写真付きの物理的バッジを付けることを依然として要求することだと指摘する。それでも、このシナリオでのモバイル・アクセスには明らかな利点がある。ほとんどの人がほぼ常にスマートフォンを持ち歩き、スマートフォンは通常パスワードで保護されているためより安全だ。


提供：ギャラガー・セキュリティ社


AMAGテクノロジ社APAC営業部長ギャオピン・シャオ氏

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、これらのプログラムが構築されている多数の異なるプラットフォームの存在が課題だと述べている。「誰もが同じタイプの携帯電話を持っているわけではない。あるいはスマートフォンをあるからだ。もう1つの考慮事項は、施設への短期または長期のアクセスを必要とする可能性がある訪問者および請負業者の処理方法、ならびにプライバシーの問題の処理方法だ。つまり、従業員がアクセスにパーソナル携帯電話を使用する場合その電話が資格情報として使用されている場合は、雇用主がアクセスする。企業がこれらの種類のソリューションを実装する前に、これらの全ての課題に対処し、議論する必要がある」。

私たちが仕事に携帯電話を使う方法と個人的な問題との間の境界線がますますぼやけてくるので、サイバー・セキュリティの懸念も対処しなければならない。ジェムアルト社アイデンティティ&アクセス管理担当副社長フランソアズ・ラズニア氏によると、このため、モバイル機器はより魅力的だが脅威にもなる可能性がある。

「ユーザは自分がインストールするアプリについてより注意深く警戒する必要がある。企業は、モバイル機器のエンド・ポイントおよびセキュリティへのアクセスに、より多くのリソースを注ぐ。本質的にモバイル機器にはセキュリティの面で幾つかの制限があり、私たちの生活を支える役割が増え続けるにつれ、サイバー攻撃の中心となるだろう。そのため、モバイル機器が危険にさらされる可能性があると想定しながら高レベルの信頼性を維持するためのセキュリティ・メカニズムの「ゼロ信頼」がますます重要になる」と同氏は指摘している。

その他の問題としては、携帯電話のバッテリ寿命の低下がある。Bluetoothを使用するほとんどのモバイル・アクセス・ソリューションでは、この機能を常にオンにする必要があるためだ。

アクセスが期待される映像統合

エンドユーザが様々な機能を単一のプラットフォームにグループ化するためのシームレスなソリューションを模索しているため、映像監視のアクセス・コントロール・システムへの統合の動きはは2019年も続くと予想される。

アクセス・コントロールと映像との統合は何年も前から行われており、アクセス・コントロール業界関係者は、これがさらに広範な統合傾向の一つとして続くと考えている。

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、「一般的な統合は、カメラや管理システムなど、アクセス・コントロールと映像構成機器の両方の製造元にとって非常に重要になる。アクセス・コントロールと統合された映像への移行はこの傾向の自然な延長であり、これを自社製品の重要な要素とする製造業者は、そうでない製造業者よりも成功するだろう」と語っている。

マクスセス・システムズ社ナンシー・イスラス氏は次のように述べている。「NoCまたはSoCを持つ企業は、全ての重要な監視、アクセス・コントロール、セキュリティ・システム、および双方向通信を統合プラットフォームに統合することで、直ちに利益を得る。このような高度な統合により、セキュリティと運用管理に総合的な状況認識を提供し、緊急事態の際に必要な情報を使ってファースト・レスポンダと保護する人々の活動を調整することができる」。

ギャラクシー・コントロール・システムズ社社長リチャード・カルザース氏は、業界の専門家たちが「業務を統合し連携

提供：ギャラガー・セキュリティ社

ギャラクシー・コントロール・システムズ社
社長リチャード・カルザース氏

マクスセス・システムズ社社長
ナンシー・イスラス氏

するために、より高度なシステム統合をますます求めている。例えばこれまでとは異なるシステム機能で統一されたプラットフォームなどだ」と述べ、「当社は過去数年間VMS統合をサポートしてきた。新しい統合パートナーが発生した場合は、今後も拡大していく」と付け加えた。

アイデンティヴ社製品管理部長ジェイソン・スピールフォーゲル氏は、次のように述べている。「映像はアクセス・コントロール・イベントを視覚的に検証する簡単な方法を表し、アクセス・コントロールは監視調査に使用できる追加データを表す。このような統合の前提条件は、エンドユーザがシステムをどのように使用するかによって異なるが、アクセス・コントロールのチェックポイントの近くにカメラを配置する時は、統合せずに驚くほど高速な方法を提供するのは投資の無駄になる。イベントは正しいか/正しくないかのプラクティスを検証すべきだ」。

アレジオン社国際技術&エンジニアリング担当副社長ヴィンス・ウェノス氏によると、ライブ映像と録画映像の両方が引き続き価値がある一方で、セキュリティを強化するために画像を活用できるソリューション（映像・ストリームでの顔認識など）が最も普及する可能性がある。「コンシューマ・エレクトロニクス分野での論理的なアクセス・コントロールと支払いのための映像技術の利用拡大が、エンドユーザの認識を積極的に変えていることに注目することは重要だ」。

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、アクセス・コントロールと映像管理の両方をよりクラウド・ベースのフォーマットで提供するソリューションが、価格帯と提供されるサービスにより中小企業が選択していると述べた。映像統合から恩恵を受ける可能性がある分野としては、アクセス・コントロールにとって映像が重要な要素であるヘルスケア、教育、金融サー

ビスなどの他、教育、カジノそして「おもてなし」を挙げている。

ギャラガー・セキュリティ社英国&欧州地区担当責任者リチャード・ヒューイソン氏は、市場のニーズや欲求ではなく製造業者や提供企業が差別化を図ろうとしているため、映像監視とアクセス・コントロールの統合を考えている。同氏は、あらゆるアプリケーションに必要なものではなく、映像とアクセス・コントロールの統合は個々のニーズに基づいているべきだと考えている。「映像の統合は、アクセス・コントロールのスループットが非常に高いところでは、映像を監視するためのマンパワーがないため、実際的ではなく、また価値もない。私はここでは例えば病院や教育を例に挙げる。例えば、ロンドンのキングス・カレッジでは、ギャラガー社製アクセス・コントロール・システムは毎月100万回のドアの動きを制御している」。

非接触生体認証アクセス・コントロール

分野を越えて広がるアクセス・コントロールにおける生体認証は既に潮流であり、現在は非接触技術に焦点が当てられている。

非接触生体認証は、より正確で先進的な技術のおかげで、アクセス・コントロール市場においてこの先1年間の継続的な成長が予測されている。世界の生体認証システム市場は、マーケッツ&マーケッツ社のリポートによると2023年までに20%の年平均成長率（CAGR）で418億米ドルに達するとみられている。

分析が10年以上にわたってその傾向を予想していたのと同様に、生体認証の爆発的な成長も予測されていた。先端技術の大幅な進歩により、コストが削減され、事実上すべての生体認識の性能が向上し、導入が容易になった。「論理アクセス・コントロールと電子決済とのためにスマートフォンに生体認証を適用したことによるユーザの受け入れの一般的な変化と相まって、これらの進歩は加速するだろう」とアレジオン社国際技術&エンジニアリング担当副社長ヴィンス・ウェノス氏は話している。

アレジオン社
国際技術&エンジニアリング担当
副社長ヴィンス・ウェノス氏

アイデンティヴ社製品管理部長ジェイソン・スピールフォーゲル氏は、ユーザの特別な協力を必要としないアクセス・コントロール・システムの作成は、常に非接触型生体認証システムのアキレス腱であると話している。これは、そのようなシステムは一般に、対象が正確な場所にいること、またはシステムがユーザを認識および認証するための特定の場所を見ることを必要とするためである。しかし、虹彩や顔を認識できる技術ならば、直接ではない角度でもこれらの障壁を克服することができる。「この技術の共謀を防ぐように設計されたシステムと組み合わせると、セキュリティに革命を起こす可能性がある」と同氏は説明している。

ジェムアルト社は最近、生体認証を搭載した大手航空会社との共同パイロット計画を発表した。ジェムアルト社アイデンティティ&アクセス管理担当上級副社長フランソアズ・ラズニア氏によると、「このテストでは、旅客のニーズを確認し、顔認識と従来の搭乗券の使用、および米国の出口要件であるCBP（税関と国境保護）の満足度を満たすことで期待に応えている」。

アレジオン社国際技術&エンジニアリング担当副社長ヴィンス・ウェノス氏は、政府と公共の安全がもはや生体認証技術を利用する唯一の主要分野ではなくなると指摘し、教育と医療もまた一般的なアクセス・コントロールのための利用拡大を見ていると付け加えた。

「医療分野では、アプリケーションにスタッフの利用率と

患者の転帰を改善する合理化されたワークフローが含まれる可能性がある。非接触型の実装でより清潔になった。そして患者情報やその他のデータにアクセスするための身元確認ができるようになった。ソフトウェア企業スパイスワークス社によると、企業も論理アクセス・コントロールのための生体認証の使用を劇的に増加させる可能性があり、2020年までにその技術を使用する可能性が90%になる」と同氏は話している。

TDSi社MDジョン・デイヴィス氏は、建設現場が生体認証アクセス・コントロールが有益である可能性がある場所の好例であると述べている。このような環境では、トークンを携帯することは実際的ではなく、また、労働者の手がさらされるという厳しい条件のために指紋を読むことが困難になるため、労働者にとって手のひら静脈や顔認識システムの使用ははるかに実用的となる。

このようなシステムは、資格を保持するためのポケットまたはバッグを利用する可能性がなくプロ競技者が非公開のアクセス領域にアクセスする必要がある運動場または競技場にもよく適している。

ウェノス氏によると、音声アシスタントの採用が2桁成長していることからも明らかなように、もう1つの非接触型生体認証取得基盤は音声技術だ。「音声認証が物理的セキュリティとデジタル・セキュリティの橋渡しをし、必要に応じて保護を強化することができる」と同氏は話している。

それでも、採用には障壁がある。ギャラガー・セキュリティ社英国&欧州地区担当責任者リチャード・ヒューイソン氏は、GDPR適用後におけるデータ・プライバシーの意識の高まりを指摘する。「当局が…私の写真を撮っている」と心配しているのではなく、「何をしているのか」を知らずに心配しているという。

「システムが特定の顔の特徴を測定し、それらをアルゴリズム画像に接続するだけであるという事実は重要ではない。これは、現金自動支払機のスキャナーが20年前に発売されなかったのと同じ理由だ。つまり人々の恐れるという心情だ。しかし、結局のところ、消費者の利便性のために、それは成長傾向にあり、技術はこれを容易にするために、恐怖要因を克服するための公共の啓蒙活動と共に改善されるだろう」。

非接触バイオメトリック成長を促進するための顔認識

顔認識の進歩と技術の受け入れの増加は、アクセス・コントロールのための非接触生体認証としての使用のために成長を推進している。

ヴァンダビルト社
アクセス・コントロール製造管理
主任アンドリュー・ファルトン氏

当初の消費者からの懐疑論にも関わらず、顔認識技術の遍在の増加は、アクセス・コントロールとしての非接触生体認証使用への道を滑らかにした。マクスセス・システムズ社ナンシー・イスラス氏は、主要なスマートフォンでの顔認識の実装により、学習曲線が劇的に減少したと指摘している。

これは現在広く一般に受け入れられており、アクセス・コントロールなど、より多くのアプリケーションで顔認識の展開がさらに加速されるだろう。マーキッツ&マーキッツ社のリポートによると、世界の顔認識市場は13.9%の年平均成長率(CAGR)で、2022年までに約78億米ドルに達すると予想されている。成長は公共の場での強化された監視と視認の必要性の増加と政府部門などの分野での技術の使用の増加によるものだ。

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、モバイル認証情報と同様に、アクセス・コントロールに関しては柔軟性を求めていると述べた。生体認証機器はこれを達成することを支えた。それと同時に組織を保護するために追加のセキュリティの層を提供すると同氏は付け加えた。

新しい技術が絶え間なく公開されているが、顔認識や虹彩など最も人気のある生体認証システムが一般的に最も確立されており実用的だ。「顔読み取り装置はここ数年で急速に開発が進み、便利で安全性が高いため、多くの顧客が指紋読取装置や掌読取装置の代わりに使用するよ

うになった。また、顔テンプレートの容量は、幾つかの用途で必要とされる多数の人々を満たすために、10,000でも対応できるとAMAGテクノロジ社APAC営業部長ギャオピン・シャオ氏は話す。

顔認識技術は何年にもわたって著しく進歩しており、そしてそれは今や虹彩認識よりも正確だとギャラガー・セキュリティ社英国&欧州地区担当責任者リチャード・ヒューイソン氏は話している。

「当社は、もともとオーロラ・コンピュータ・サーヴィス社が開発した顔認識を、空港でのパスポート管理のような管理された状況で効果的に採用したのを見た。しかし、パスポート管理のような高度に管理された環境でも、ヒット率は必ずしも理想的ではない」とヒューイソン氏は言う。「我々は、カメラの制約が一部の人々を管理するには厳し過ぎるというさらなる問題を抱えている。私の身長は198cm以上あり、私を連れて行くのに十分な高さのカメラを見つけることができないのに対し、車椅子の人は120cm以下になるかもしれない」と彼は付け加えている。

ヴァンダビルト社アクセス・コントロール製造管理主任アンドリュー・ファルトン氏は、「地域で見ると、顔認識ソフトウェアが非接触生体認証アクセス・コントロールおよび分析機能の手段としてアジア太平洋市場に参入しつつある」と説明している。今や、この装置が欧州や米国市場で浸

透する技術として進んでいくのを目にし始めた。企業はこれらのタイプの技術的進歩の採用に向けて動き続けており、企業は前進し続けている」。

アレジオン社国際技術&エンジニアリング担当副社長ヴィンス・ウェノス氏は、その顔認証について指摘している。特に中国では、顔認識と人工知能（AI）の組み合わせが大きな混乱の原因になっていると認識されているため、認識への投資は著しく増加している。

「過去2年間の生体認証へのベンチャーキャピタル投資は40億米ドルを超え、その約半分が中国の顔認証企業に向けていたことを報告が示している」と彼は言う。

クラウドとサイバー・セキュリティの意識

ストレージがますます手頃な価格になるにつれて、クラウドへのアクセス・コントロールの移行は2019年に増加するとみられている。

クラウドベースのアクセス・コントロールおよび映像管理ソリューションの受け入れは、2019年も続くと予想されている。業界関係者は、エンドユーザの間でクラウド製品を採用する意欲が高まっていると指摘している。ほとんどの消費者はより伝統的なアクセス・コントロール・ソリューションに投資したいと考えているが、インストール時間の短縮、ソフトウェアの自動更新、柔軟性とモビリティ、マネージド・サービス、サイバー・セキュリティの強化などのクラウドのメリットはユーザを魅了している。

「来年度の大幅な成長は、クラウド・ホスティング型のア

TDSi社MDジョン・デイヴィス氏

アイデンティヴ社製品管理部長
ジェイソン・スピールフォーゲル氏

クセス・コントロール・スペースになると予想される。小売業者にとって新たな収益が生まれ、高度なアクセス・コントロール機能を経済的に展開するための中小企業のビジネス機会が増える」とギャラクシー・コントロール・システムズ社社長リック・カルザース氏は述べている。

アイデンティヴ社製品管理部長ジェイソン・スピールフォーゲル氏は、「その結果、クラウド/ホステッド・アクセス・コントロール・ソリューションも2019年にはより多くの機能と統合によって進化し続けるだろう」と話し、アクセス・コントロール・システムの制御と管理をクラウドに移行することは、管理と制御の向上、セキュリティの向上など、様々な理由から意味があると付け加えている。

「また、オンプレミス環境で追加のパネルが必要になることで、アクセス・コントロール・システムのスケーラビリティがほぼ無限になる。現在の状況は、クラウドがシステムの主要な頭脳であり、オンプレミス・バックアップであるというハイブリッドな構成だ。アクセス・コントロール・メーカがより多くのシステム機能を最先端の接続機器や読取機に移行し続けるにつれて、クラウドはアクセス・コントロールにとってさらに魅力的な選択肢になるだろう」と同氏は述べている。

IHS マーキット社は、アクセス・コントロール・サービス（ACaaS）の市場収益が2022年までに9億5000万ドルに達すると予想している。同社リポートによると、中小企業がACaaSの採用を主導するという。中小企業は、2017年の市場収益の21%を占めていた。

「アクセス・コントロールをクラウドに搭載することで、エンドユーザはセキュリティを強化できるが、必ずしも高価なIT基盤に投資する必要はない。サービスとしてのアクセス・コントロールは、中小規模のプロジェクト（最大50ドア）で堅牢で急速に成長している市場の領域になることを断言する」とTDSi社MDジョン・デイヴィス氏は述べ、次のように語っている。

「興味深いことに、サービスとしてのアクセス・コントロールは供給企業にとって新しいパラダイムを提示しているので、結果として新しい企業が市場に参入することになる。これは新規参入は競争の激化を意味しているため、市場がどのように反応し、供給企業がこれらの新たな課題にどのように対処しているかを見るのは興味深い」。

アクセス・コントロールがクラウドに移行し、IPベースになることが予想されるため、サイバー・セキュリティの問題は重要な検討事項になる。

ギャラガー・セキュリティ社英国&欧州地区担当責任者リチャード・ヒューイソン氏は、サイバー・セキュリティへの意識がアクセス・コントロールの技術開発を推進している主な要因であると語っている。これはGDPRと密接に関連しており、モバイル・クレデンシャルと部分的に関連していると付け加えている。

しかし、同氏は「サイバーは大きな問題であり、ますます高レベルで共鳴している」と強調する。「多国籍企業では、銀行などの特定の業界や企業レベルの企業で、ネットワークに接続されているものが何であっても、ハッカーがアクセス・コントロールや映像監視システムを介してアクセスすることは容易にできない」と話し、「モノのインターネットでは、英国のサイバー・アシュアランス・プロダクツ（CAP）、米国のFIPS、オーストラリアのタイプ1Aなど、様々な世界標準を満たすシステムが、本物のサイバー回復力を見い出すだろう。例えば英国では、約40社メーカのほんの一握りだけがこのレベルの規格準拠とサイバー回復力を提供することになるだろう」と彼は言う。

一般的に低レベルの知識や専門知識そしてリソースしかない中小企業の場合、ヒューイソン氏氏は、ユーザがネットワークの回復力、および長期的に見てセキュリティへの投資が将来にわたって証明され、「サイバー・セーフ」であるかどうかを確信する必要があると確信している。

TCO分析により分かる 一般的VMSとクラウドVMSの違いとは?

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

TCOとは、「Total Cost of Ownership」の略称で、システムの総所有コスト分析を意味します。特定システムの導入から運用後までも含むライフサイクル全体にかかる総所有コストを明確にします。その結果、TCOは「ライフサイクル·コスト分析」と呼ばれることがあります。TCO分析により、テクノロジの所有と運用にかかる「目に見えるコスト」と「目に見えないコスト」の両方が明らかになります。

セキュリティ技術を購入し、展開、運用していくにあたり、リスク目標と財務目標とを設定します。これらの目標は、一般的によく見られる下記の購買目標にも反映されます。

·セキュリティ·リスクを低減させるための目標を達成するために、最高なテクノロジの価値を獲得する。

·無計画な技術運用やサービス·コストによる想定外の出費を回避する。

衝撃的なのは、セキュリティ技術の「目に見えない」運用上のコストが、いかに大幅にシステムの総所有コストを引き上げているか、ということです。セキュリティ技術の所有コストが当初の購入価格の2倍さらには4倍になることは一般的にはよくあることです。ITサーバの総所有コストは通常、元のコストの4倍です。

しかしながら、クラウド·コンピューティングによって、映像管理システム(VMS)のTCO係数が大幅に変わりました。VMSコンピューティングと映像ストレージ基盤をクラウドに移行することで、かなりの規模の経費削減を実現します。さらに、クラウド·システムの信頼性、広域遠隔アクセス、そして強力なサイバー·セキュリティ·システムは、一般的なオンプレミスで適用しているケースを遥かに超えています。

今や購入価格だけではなく、VMSの所有と運用にかかる全てのコストを把握し、一般的なオンサイト·システムよりも遥かに低く済むクラウド·システムを選ぶことが可能になっています。コスト削減の幅は、システムを展開する事業のタイプによって異なりますが、一般的には次の通りです。

·中小企業·····5-15%

·複数店舗の小売業·····25-40%

·大規模商業施設·····15-25%

さらに、これ以外にも、自社のVMSアプリケーション·データセンターをホストとする大企業向けシステムのTCO節減もあります。これらのデータセンターはオンサイト、オフサイト、または第三者により運営されています。企業のデータセンターのITコストがどのように割り当てられているかにより、TCO削減が30%を超える場合もあります。

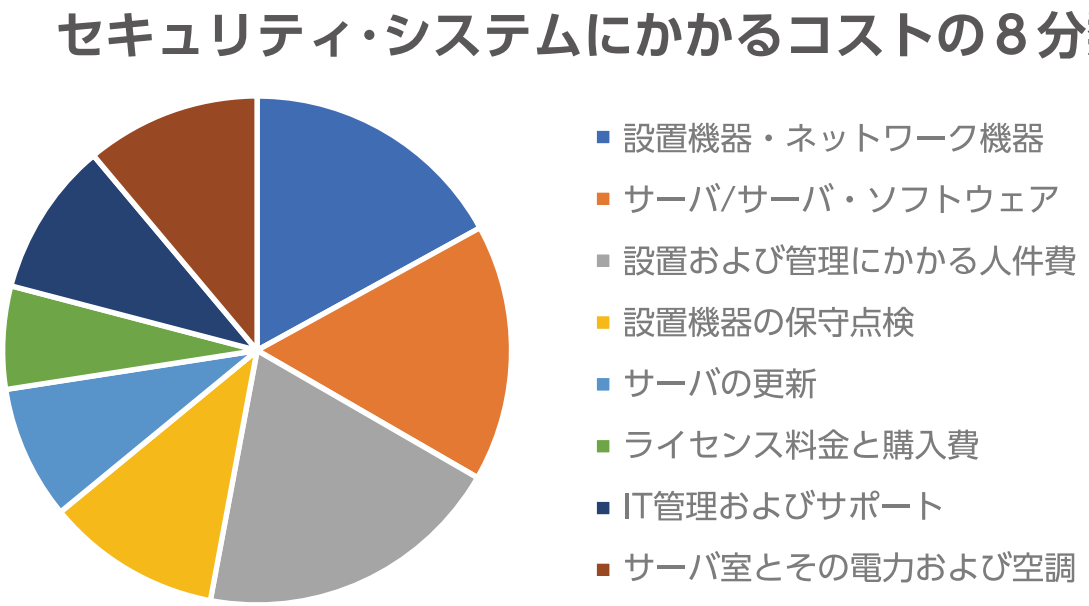


図1　電子セキュリティ·システムのTCOコスト分類

企業向けマルチサイト　Eagle Eye Cloud System							
設定容量		1年目	2年目	3年目	4年目	5年目	
	サイト数	45	45	45	45	45	
	カメラ台数(1080p フルHD　15fps)	810	810	810	810	810	
	映像ストレージ日数	30	30	30	30	30	
費用概要		1年目	2年目	3年目	4年目	5年目	計
1	定期システム費						
1-1.	イーグルアイ・クラウドVMS費用	¥34,992,000	¥34,992,000	¥34,992,000	¥34,992,000	¥34,992,000	¥174,960,000
1-2.	インターネット・サービス費	既存設備の利用					
2	ハードウェアの購入と人件費						
2-1.	イーグルアイ・ブリッジ製品のセットアップ人件費	¥4,491,000	¥0	¥0	¥0	¥0	¥4,491,000
2-2.	ブリッジとスイッチのインストール人件費	¥412,912	¥0	¥0	¥0	¥0	¥412,912
2-3.	LANルータ費用と人件費	クラウドVMS購入費に含む					
2-4.	インターネット・ルータ費用と人件費	既存設備の利用					
3	アップグレードとアップデート費						
3-1.	クラウド・データ・センター設備アップデート費	クラウドVMS購入費に含む					
3-2.	VMSソフトウェア・アップデート費	自動化により人件費なし					
3-3.	LANルータのアップデート費と人件費	自動化により人件費なし					
4	オンプレミス電気料金						
4-1.	ブリッジ製品用	¥884,520	¥884,520	¥884,520	¥884,520	¥884,520	¥4,422,600
4-2.	LANルータ用	ブリッジ製品に含む					
5	コンピュータとストレージのホット冗長						
5-1.	ソフトウェア・ライセンスのホット冗長	クラウドVMS購入費に含む					
5-2.	コンピュータとストレージのホット冗長	クラウドVMS購入費に含む					
6	サイバー・セキュリティ対策費						
6-1.	情報セキュリティ監査	クラウドVMS購入費に含む					
6-2.	連続侵入テスト	クラウドVMS購入費に含む					
TCO(総保有コスト)		¥40,780,432	¥35,876,520	¥35,876,520	¥35,876,520	¥35,876,520	¥184,286,512

■セキュリティ・システムのTCO

セキュリティ・システムのTCOの計算方法は、データ収集などに課題があり、他の種類の製品コスト比較分析よりも複雑です。図1は、セキリュティ・システムにかかる8つのコストのカテゴリ分類を示しています。これらの相対的なコスト規模は、ビジネスの展開と設定によって異なります。

小規模な単一サイトでの導入では、TCOの計算は簡単です。複数拠点のサイトや、大規模商業施設、または企業向けのTCOの計算は複雑になります。

果たしてセキュリティの管理者が競合ブランドの映像監視システムのTCOを計算することに一体どんな利点があるのでしょうか?商用映像監視システムの強みは、本来企業のIT部門が担うサーバやネットワーク基盤にはありません。競争力の違いは一般的には映像管理システムのソフトウェア自体のみにあるのです。

10年以上にわたり、サーバとネットワークの設置と保守そして修理のコストは、どのVMSでもほぼ同じでした。競争力の違いとして表れたのは、ソフトウェアの購入価格と利用中のライセンス料のみでした。しかしながら、クラウド型VMSの登場からは、もはやその限りではありません。

まず、良い機能を備えたクラウド型VMSには、サーバとデータの冗長性、通信域幅の広域なネットワーク基盤、非常に強力なサイバー・セキュリティなど、オンプレミス・システムでは叶えることのできない機能があります。第二に、VMSは経済的で購入しやすくなっています。なぜなら、広域ネットワーク基盤の大規模経済性、クラウド・データセンターとインターネットの柔軟なコンピューティング、そしてデータ・ストレージがあるからです。下記のクラウド型VMSの機能は、オンプレミス・ベースのVMSでは、お手頃な値段で提供されません。

・ホット冗長性コンピューティング
・二重、三重の冗長映像データ・ストレージ
・定期的に実施される情報セキュリティ監査
・頻繁な脆弱性スキャンとサイバー・セキュリティの侵入テスト
・継続的な機能の提供
・自動的に適用されるアプリケーション・セキュリティ・アップデート

ここで一例として、複数拠点を有する商業施設でのTCO分析を見てみましょう。この例では44箇所の事業所と本社にそれぞれ1台の高品質なNVR計45台で構成するシステムと、高品質なクラウド型VMSシステムのコストを比較します。この分析では、高品質なブランドのNVRとクラウド型VMSのコストを比較します。ここでは、図1に示されているセキュリティ・システムにかかるコストのほとんどが含まれます。ただし、例えば、サーバ設置場所の暖房と換気および空調のハードウェア・コストは含まれていません。これらがコスト分析の結果です。

オンプレミスVMS‥‥‥‥‥‥266,479,841円
クラウドVMS‥‥‥‥‥‥‥‥‥184,286,512円
クラウドTCOとの差額‥‥‥‥‥82,193,329円

企業向けマルチサイト　Eagle Eye Cloud System							
設定容量		1年目	2年目	3年目	4年目	5年目	
	サイト数	45	45	45	45	45	
	カメラ台数(1080p フルHD　15fps)	810	810	810	810	810	
	映像ストレージ日数	30	30	30	30	30	
費用概要		1年目	2年目	3年目	4年目	5年目	計
1	定期システム費						
1-1.	NVR/VMS基本プラン	¥1,288,338	¥1,288,338	¥1,288,338	¥1,288,338	¥1,288,338	¥6,441,690
1-2.	インターネット・サービス費	既存設備の利用					
2	ハードウェアの購入と人件費						
2-1.	NVR購入費とライセンス費	¥88,623,400	¥0	¥0	¥0	¥0	¥88,623,400
2-2.	NVRインストール費とセットアップ費と人件費	¥1,048,798	¥0	¥0	¥1,048,798	¥0	¥2,097,596
2-3.	LANルータ費用と人件費	¥1,495,508	¥0	¥0	¥0	¥0	¥1,495,508
2-4.	インターネット・ルータ費用と人件費	既存設備の利用					
3	アップグレードとアップデート費						
3-1.	NVRリプリース費とライセンス費	¥0	¥0	¥0	¥88,623,400	¥0	¥88,623,400
3-2.	VMSソフトウェア・アップデート費	¥0	¥349,599	¥349,599	¥0	¥349,599	¥1,048,797
3-3.	LANルータのアップデート費と人件費	¥0	¥349,599	¥349,599	¥349,599	¥349,599	¥1,398,396
4	オンプレミス電気料金						
4-1.	NVR用	¥2,750,715	¥2,750,715	¥2,750,715	¥2,750,715	¥2,750,715	¥13,753,575
4-2.	LANルータ用	¥12,599,496	¥12,599,496	¥12,599,496	¥12,599,496	¥12,599,496	¥62,997,480
5	NVRのホット冗長						
5-1.	ソフトウェア・ライセンスのホット冗長	配置から除外					
5-2.	コンピュータとストレージのホット冗長	配置から除外					
6	サイバー・セキュリティ対策費						
6-1.	情報セキュリティ監査	配置から除外					
6-2.	連続侵入テスト	配置から除外					
TCO(総保有コスト)		¥107,806,255	¥17,337,747	¥17,337,747	¥106,660,346	¥17,337,747	¥266,479,842

クラウドTCOによる節約‥‥31%

■クラウド型VMSのTCOの方が優れている理由

先ほど述べたTCO分析の比較により分かることは、一般的VMSよりもクラウド型VMSの方に利点があるということです。クラウド型VMSの利点は明らかで、以下の通りです。

・TCOの削減‥総所有コストを低減することができます。

・初期費用コストの削減‥初期支出コストを抑えます。

・完全ホット冗長性‥データ保存や映像記録と処理のための完全な冗長性があります。

・サイバー・セキュリティ‥伝送中および保存中のデータ暗号化を含む強力なサイバー・セキュリティがあります。

・携帯機器の性能‥広域携帯機器の性能が向上します。

・自動更新‥顧客やサービス提供企業による対応を必要としない、セキュリティと機能のアップデートが自動更新されます。

・ユーザが使用した分だけの料金発生‥クラウドのユーザは映像解析やその他のシステム機能をオンデマンドで増減することができ、しかも使用期間に対してのみ料金を支払います。

・瞬時に変更可能な映像保存‥クラウドのユーザは、オンプレミス基盤を変更することなく、カメラごとに映像の保存期間と記録解像度およびフレームレートを拡張することができます。

・サーバ更新コストの増加がない‥オンプレミス・システムでは通常次のことが必要となります。

a 新しいソフトウェア要件を満たすため、プロセッサの電力とメモリを増やし、古いサーバのアップ・グレードが必要。

b 交換時期に近いハード・ディスク・ドライブの交換

・アップ・グレードによるダウンタイムのない新機能の追加‥真のクラウド・システムは、継続的なソフトウェア・エンジニアリング供給により最新状態を維持し、数ヶ月または数年ではなく数週間の間隔でソフトウェアを徐々に改善しています。スタッフの学習曲線が伸びれば、セキュリティおよびバグ修正のアップデートとバージョン・アップ・グレード・ダウンタイムが削減されます。

■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ーバ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。

アクシスコミュニケーションズ、Axis Solution Conference 2019 Tokyoを開催

アクシス社は、2019年7月5日東京秋葉原UDXギャラリーにおいてAxis Solution Conference 2019 Tokyoを開催した。

冒頭の同社エンタープライズ営業本部長寺田大輔氏の開会挨拶に続いて、同社北アジア・リージョナル・テクニカル・ディレクター落合大氏が、「よりスマートでより安全な毎日を」と題して基調講演を行なった。同氏は、北アジア地域の技術部門トップとして、日本・中国・韓国・台湾・香港に在籍するセールス・エンジニアおよびテクニカル・サービス・エンジニアおよびアカデミー・トレーナーの各部門を統括している。

本稿では、基調講演をもとにアクシス社の現在の事業コンセプトを紹介する。

【直近10年間の潮流】

2008年から2018年までの世界企業ランキングをみると、世界の変化の速さを象徴している。具体的には、物事はかつてないほど速く変化し、将来を予測することは非常に困難である。一方、現状に留まっていてはビジネスで勝ち残ることができないことも確かである。そのため、技術、社会、ビジネス・モデルの実りある組み合わせが最重要課題となっている。特に技術に関して、潮流(トレンド)としてサイバー・セキュリティ、エッジ分析、IoTプラットフォームの3つのテーマを挙げる。

■サイバー・セキュリティ

今やサイバー攻撃の被害は全世界に及んでいる。そのため、サイバー・セキュリティへの取り組みが喫緊の課題となっている。顧客からは、同社製品の評価以前に、アクシス社のサイバー・セキュリティに対する成熟度と、継続して透明性を高く維持してオープンなスタンスで取り組む姿勢に評価を得ている。

■エッジ分析

セキュリティ・システムで末端に繋がれているIoT機器上におけるインテリジェンス(情報)機能をどのように取り扱うか。具体的には圧縮したデータを幾つもの目的で活用することができるかが話題となっている。

■IoTプラットフォーム

2025年には700億以上に増え続ける接続デバイスにより、さらに多くのネットワーク帯域およびさらに優れた圧縮技術そして一層中央化されたコントロールとセキュリティが必要となってきている。これについて、アクシス社はプラットフォームとしてAXIS Device Managerをコアにして大規模なデバイス接続を管理している。次世代APMの開発にも着手している。

【アクシス社の取り組むテーマ】

■革新性

その代表的な例が、アクシス社独自開発ASICであるARTPEC-7の提供で、高品位な映像ソリューションを実現している。さらにネットワークカメラを超えたラインアップの拡大により革新性を推進している。

■グローバルな展開

アクシス社は世界50カ国に事業所を開設し、様々なニーズに対応したソリューションを提供し、それらの情報を世界規模で共有している。また、15ヶ所にエクスペリエンス・センターを設けパートナーや顧客とともにソリューションについて議論し改良する機会を用意している。

■顧客重視

世界各地の異なるニーズや異なる顧客に取り組める顧客重視の技術企業であるために、異なる文化を理解するためコミュニケーションにおけるオープン性や考えに基づいて長期的な事業継続が可能になると考えている。

ロックシステム、「Locksystem Reception 2019」を開催

ロックシステムは2019年7月23日に神奈川県横浜市において、「Locksystem Reception 2019」を2018年に続いて開催した。今回のテーマは「安心と安全の違い　副題：迫りくる人手不足とIoT時代に備えたセキュリティシステムの運用と管理」だった。まず、同社代表取締役社長澤和男氏がイベント開会挨拶とテーマ説明を行なった。

【テーマ説明】

■安心と安全

この言葉を的確に表すために、米国の暗号・情報セキュリティの研究者・専門家、作家であるブルース・シュナイアー（Bruce Schneier）氏の著書を引用して説明した。「安心」とは主観的なもので、一方「安全」とは客観的なもので、セキュリティ提供者は、「安心」と「安全」の両方を提供しなければならない。

そして、「安心」と「安全」に対する脅威は、時代と共に変化している。日本においては犯罪の認知件数は劇的に減少しているが、新たに経済犯罪に区分される犯罪が増加している。そのため、産業界における脅威に対しては、自社管理によるセキュリティ対策の必要性が高まってきている。

この自社管理によるセキュリティ管理は、大きく4要素に分類することができる。具体的には組織的セキュリティ、人的セキュリティ、物理的セキュリティ、技術的セキュリティを指す。そのうち物理的セキュリティは、人の目につきやすい対策となることから、規制を強化することで対策認知度が得られやすい。そして、入退管理の履歴や監視カメラの録画映像などはトレーサビリティ(追跡可能性)を有するため、内部犯罪発生後の対応そして内部犯罪の抑止に大きな効果を得ることができる。　このことから、物理的セキュリティ・システムの導入により安心するのではなく、そのシステムを適切に運用することが安全な状態の条件の一つとなると言える。

ロックシステムがエンドユーザに対する役割は、物理的セキュリティを適切に運用することでセキュリティ風土の醸成を支援し、内外の不正行為が行なわれにくい環境と仕組みを提供することだと捉えている。これによりコーポレート・ガバナンス(企業統治)の実現をサポートすることができる。

■人手不足とIoT時代に備えたセキュリティシステムの運用と管理

日本では現在、様々な分野で深刻な人手不足が顕在化している。セキュリティ・システムのユーザ側においても、システム管理者や担当者が不在という事例も多い。またシステム提供側においてもエンジニア不足という問題も抱えている。

さらに、2020年から次世代通信5Gの本格運用が始まることからIoT時代に一層の拍車がかかることになる。セキュリティ業界においても例外ではなく、映像監視だけでなくアクセス・コントロールもIoT化しつつある現状を見るとここでもエンジニア不足という難題が生じてくる。

■上記の課題に対応するソリューションの提供

そこで、ロックシステムはその一つの解としてモニターBOXの導入を提案している。モニターBOXを導入することで、安心と安全の確保し、新しい機能によりエンジニアの負荷を軽減し、IoT時代に沿ったサービスやインテリジェント機能を実現するソリューションを提供するものだ。

引き続き、キロックス取締役副社長である福井将裕氏によるモニターBOX新機能発表および導入事例の紹介、ロックシステム児玉政文氏による新サービスの発表があった。

なお、モニターBOXの新機能については、次号で詳細に紹介する。

2019年8月

SECUTECH VIETNAM
会期：2019年8月14日～ 16日
開場：10:00 - 17:00
会場：サイゴン・コンベンション・センター (SECC)
799 Nguyen Van Linh, Tan Phu Ward, Dist. 7. Hachiman City
主催：MESSE FRANKFURT NEW ERA BUSINESS MEDIA LTD.
URL：www.secutechvietnam.com

9月

Global Security Exchange (GSX)2019 (旧名称・・ASIS INTERNATIONAL2019)
会期：2019年9月8 - 12日
会場：マコーミック・プレイス 米国イリノイ州シカゴ
主催：ASIS International
URL：https://www.gsx.org/

第21回自動認識総合展
会期：2019年9月11日～ 13日
開場：10:00 - 17:00
会場：東京ビックサイト南ホール
主催：一般社団法人日本自動認識システム協会
URL：https://www.autoid-expo.com/tokyo/

センサーエキスポジャパン2019
会期：2019年9月11日～ 13日
開場：10:00 - 17:00
会場：東京ビックサイト南ホール
主催：フジサンケイ ビジネスアイ
（日本工業新聞社）
URL：http://www.sensorexpojapan.com/

フードセーフティジャパン(FSJ)2019
会期：2019年9月11日～ 13日
開場：10:00 - 17:00
会場：東京ビックサイト青海展示棟
主催：(一財)食品産業センター、
(公社)日本食品衛生協会
URL：http://www.f-sys.info/fsj/

第46回 国際福祉機器展 H.C.R.2019
会期：2019年9月25日～ 27日
開場：10:00 - 17:00
会場：東京ビックサイト西ホール、南ホール
主催：全国社会福祉協議会
保健福祉広報協会
URL：https://www.hcr.or.jp/

10月

CEATEC 2019(シーテック 2019)
会期：2019年10月15日～ 18日
開場：10:00 - 17:00
会場：幕張メッセ
主催：CEATEC実施協議会
一般社団法人電子情報技術産業協会(JEITA)
一般社団法人情報通信ネットワーク産業協会(CIAJ)
一般社団法人コンピュータソフトウェア協会(CSAJ)
一般社団法人 組込みシステム技術協会
URL：https://www.ceatec.com

危機管理産業展（RISCON　TOKYO）
会期：2019年10月2日～ 4日
開場：10:00 - 17:00
会場：東京ビックサイト　青海展示棟
主催：株式会社 東京ビッグサイト
URL：http://www.kikikanri.biz/

テロ対策特殊装備展(SEECAT) '19
会期：2019年10月2日～ 4日
開場：10:00 - 17:00
会場：東京ビックサイト　青海展示棟
主催：株式会社 東京ビッグサイト
URL：http://www.seecat.biz/index.html

第5回 IoT/M2M展【秋】
会期：2019年10月23日～ 25日
開場：10:00 - 18:00
会場：幕張メッセ 4-7
主催：リード エグジビション ジャパン
URL：https://www.japan-it-autumn.jp/iot/

第10回 クラウド コンピューティング EXPO【秋】
会期：2019年10月23日～ 25日
開場：10:00 - 17:00
会場：幕張メッセ 4-7
主催：リード エグジビション ジャパン
URL：https://www.japan-it-autumn.jp/cloud/

SECUTECH THAILAND
会期：2019年10月28日～ 30日
開場：10:00 - 17:00
会場：バンコク国際貿易展示場(BITEC)
88 Bang Na-Trat Rd, Khwaeng Bang Na, Khet Bang Na, Krung Thep Maha Nakhon 10260
主催：MESSE FRANKFURT NEW ERA BUSINESS MEDIA LTD.
URL：www.secutechthailand.com

11月

Embedded Technology 2019 ／ 組込み総合技術展
IoT Technology 2019 ／ IoT総合技術展
会期：2019年11月20日～ 22日
開場：10:00 - 17:00
会場：パシフィコ横浜
主催：一般社団法人 組込みシステム技術協会
URL：http://www.jasa.or.jp/expo/

第6回鉄道技術展2019
会期：2019年11月27日～ 29日
開場：10:00 - 17:00
会場：幕張メッセ　5-8ホール
主催：フジサンケイビジネスアイ
URL：http://www.mtij.jp/

2020年1月

INTERSEC　Middle East
会期：2020年1月19日～ 21日
開場：10:00 - 17:00
会場：ドバイ国際会議展示場
アラブ首長国連邦 ドバイ
主催：MESSE FRANKFURT
URL：https://intersec.ae.messefrankfurt.com/dubai/en.html

2020年3月

SECURITY SHOW 2020
会期：2020年3月3日～ 6日
開場：10:00 - 17:00
会場：幕張メッセ1・2・3ホール
主催：日本経済新聞社
URL：https://messe.nikkei.co.jp/ss/

リテールテックJAPAN 2020
会期：2020年3月3日～ 6日
開場：10:00 - 17:00
会場：幕張メッセ1・2・3ホール
主催：日本経済新聞社
URL：https://messe.nikkei.co.jp/rt/

フランチャイズ・ショー 2020
会期：2020年3月4日～ 6日
開場：10:00 - 17:00
会場：幕張メッセ1・2・3ホール
主催：日本経済新聞社
URL：https://messe.nikkei.co.jp/rt/

INTERSEC　Building
会期：2020年3月8日～ 13日
開場：10:00 - 17:00
会場：フランクフルト・メッセ
ドイツ連邦共和国ヘッセン州
フランクフルト・アム・マイン
主催：MESSE FRANKFURT
URL：www.intersec-building.com

ISC WEST 2020
会期：2020年3月18日 - 21日
会場：サンズ・エクスポ &
コンベンション・センター
米国ネバダ州ラス・ベガス
主催：SIA education
URL：https://www.iscwest.com/

青色文字の海外展示会についてはASJ合同会社までお問い合わせください。
赤色文字の展示会への出展についてはASJ合同会社が出展申込取り扱いを行なっています。

■問い合わせ先
ASJ合同会社
TEL・・03-6206-0448
E-MAIL・・komori@asj-corp.jp

読者の声

サイバー攻撃の被害を受けにくい高解像度監視システムの実現は可能か？

IPネットワークを活用する監視システムの有用性に異論を唱えるはほとんどいないだろう。しかし、サイバー･アタックやサイバー･テロなどの被害を受けやすいことに対しても共通した認識を持っているだろう。その一方で、サイバー･セキュリティ対策の難しさに頭を痛めているのもまた事実だろう。しかも、その対策費用が結構な負担となっていることも頭の痛い問題だ。

では、サイバー･セキュリティの危険が少なく、しかも高画質映像を提供することができる監視システムの構築はできないものだろうか。そうは言いものの単にアナログ監視システムだけを使用するのではなく、サイバー攻撃に耐久することができ、映像活用のできる複合システムの実現だ。カメラ台数が少ない大半の案件では、このように考えているユーザは決して少なくないのではないだろうか。

(東京　設置施工業)

初歩のセキュリティ対策の説明と確実な実行の指南を普及させるべきだ

ネットワーク監視システムにおけるサイバー･セキュリティの重要性について、漠然と理解しているがその実際の処方について、ユーザ側がどれだけ理解し実行しているだろうか。まず、カメラやレコーダの取扱説明書を開いたことがあるのだろうか。その役割はシステム構築者に委ねているのが実情だが、ユーザ側も初歩段階からのセキュリティ対策を理解していることが不可欠だと認識すべきではないか。被害を受けた時にその全責任をシステム構築者に負担させるという考え方では被害を回避することはできない。言い換えれば、どんな堅牢な鍵を装備してもそれを正しく施錠しなければ安全は確保できないのだ。

そのため、初歩段階からの映像監視システムのセキュリティ対策をユーザ側に理解し実行してもらう活動が必要ではないだろうか。その役割は、各製品やシステムを提供する側だけでなく、メディアを含めた業界に携わる全て層が担うべきだろう。

（千葉　ソフトウェア開発業）

「読者の声」を募集しています。

本誌では、セキュリティに関する読者の皆様のご意見やご提案を募集しています。セキュリティ機器やシステムを供給している側、セキュリティ・システムを既に導入あるいは導入を予定している側、いずれの側からの応募をお待ちしています。ただし、特定企業や団体または個人に対する誹謗中傷または批判的な内容はご遠慮ください。

一例を挙げると、導入する場合の手順はどのように進めれば良いのか。導入前の事前説明についてはどこに相談すべきなのか。メーカなのか販売会社なのか、システム構築企業や設置施工企業なのか、それともセキュリティ・コンサルタント企業なのか。セキュリティに関する疑問や意見また提案など、セキュリティ関連であれば詳細は問いません。掲載する場合は匿名扱いとしますので、個人情報が漏洩することはありません

なお、具体的な導入相談については、導入条件や環境についてできるだけ具体的な内容をご連絡ください。ご応募をお待ちしております。

a&s JAPAN編集部
TEL：03-6206-0448
FAX：03-6206-0452
MAIL：info@asj-corp.j

secutech
VIETNAM

ベトナムのセキュリティ、防火、スマートビルの専門家が集う B2Bプラットフォーム

会期 2019年8月14-16日
会場 ベトナム社会主義共和国ホーチミン市
www.secutechvietnam.com

本部問い合わせ先
Messe Frankfurt New Era Business Media Ltd.
ミッシェル・チュウ
TEL +886 2 8729 1099 ext. 768
Email michelle.chu@newera.messefrankfurt.com

日本問い合わせ先
ASJ合同会社
TEL 03-6206-0448
Email komori@asj-corp.jp

VIETFAIR

messe frankfurt

第28回 セキュリティ・安全管理総合展

SECURITY SHOW 2020

出展申し込みはウェブサイトで!
申込締切日:2019年10月15日(火)

http://www.securityshow.jp/

日本のセキュリティが進化する4日間

2020年 3月3日(火)▶6日(金) 幕張メッセ[1・2・3ホール]

NIKKEI MESSE 街づくり・店づくり総合展

お問い合わせ先:日本経済新聞社 イベント・企画ユニット事業部
Tel:03-6256-7355 info@securityshow.jp

主催 日本経済新聞社