

- **特集** 集：GDPR時代の映像監視データの保全
- **製品特集**：監視カメラ用SDカードの選択
- **業種別市場**：ショッピング街の安全を確保する上で不可欠な統合とは



GDPR



SECURITY SHOW 2019 併設

映像セキュリティテクノロジーフォーラム

～AIからクラウドまで、映像セキュリティのトレンドとは～

会期：2019年3月8日(金) 会場：東京ビッグサイト

協賛企業募集中



AI技術、映像解析、クラウド、ストレージ、IoTセキュリティなど、高度化する映像セキュリティビジネスにインパクトを与える最新のトレンドを紹介する「映像セキュリティテクノロジーフォーラム」を開催します。国内最大級のセキュリティ総合展「SECURITY SHOW」に併設して、セミナーや新聞、ウェブなど複数のメディアで総合的に紹介する企画です。現在、本フォーラムに協賛いただくスポンサーを募集しています。詳しくは事務局までお問い合わせください。

協賛費用：プラチナ・スポンサー 2,500,000円、ゴールド・スポンサー 1,500,000円、シルバー・スポンサー 800,000円

<http://www.securityshow.jp/>

お問い合わせ先：日本経済新聞社 文化事業局 イベント事業部 Tel：03-6256-7355 info@securityshow.jp

Dahua社IVSS - AIを備えた NVR

リアルタイムの顔認識と高度な解析を提供



- **リアルタイム映像分析:** ディープ・ラーニング(深層学習)アルゴリズムにより、対象人物の迅速な発見と潜在的な脅威予測とが可能になり、入場管理と通過効率とを向上させます。
- **画像による映像検索:** 産業用GPUを搭載し、最大10人の顔を同時に検索し、いつ、どこで出現したかを素早く特定できます。
- **オールインワン・デバイス:** 映像管理、ストレージ、サーバ、およびAIによる映像解析を1台の機器で実現します。バックエンド構造の簡素化と導入コストの削減を可能にします

Recommended Models



DHI-IVSS7008-1T



DHI-IVSS7016-4T

CE FC CCC UL RoHS ISO 9001:2000



DAHUA TECHNOLOGY

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

DAHUA社日本正規代理店
三星ダイヤモンド工業株式会社

本社西日本営業所
〒566-0034大阪府摂津市香露園32-12
Tel: 072-648-7526 Fax:072-648-7582

東日本営業所
〒222-0033神奈川県横浜市港北区新横浜2-3-4
Tel: 045-548-4731 Fax:045-548-4732
URL:http://www.mitsuboshidiamond.com



目次

特集	
GDPR時代の映像監視データの保全	18 - 21

製品特集	
監視用SDカードの選択	22 - 24

業種別市場	
ショッピング街の安全確保	25 - 29

キーマン・インタビュー	
EAGLE EYE社ディーン・ドラコCEO	4 - 7

特別企画	
国土交通省、無人飛行機の飛行ルールの周知を強化	30 - 32

イベント情報	
VIVOTEK、プライベート・セミナー	34
GEOVISION、新製品内覧会	35
展示会、プライベートショー日程	36



産業ニュース	8 - 13
新製品情報	14 - 17
読者の声	37
※連載は紙面の都合により休載します。	

広告索引

広告主名 (ABC順)	掲載ページ
DAHUA TECHNOLOGY CO. LTD.,	1
IDIS	3
SECUTECH 2019	表四
日本経済新聞社	表二

次号案内 2019年 1/2月号 (1月15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
SECURITY 50

連 載
市場慧眼、技術探訪

a&s JAPAN ©ASJ社 2018年 11-12月号 No.67
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、a&s Asiaをはじめとするa&s各誌の独占翻訳権を特約し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：reader@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いません。

Russian stadiums change the game with IDIS surveillance

最高の安心と安全を目指して

世界クラスのスポーツスタジアムにおいて、スタッフ及びビジターの健康、安全、セキュリティを確保するためにどのようなソリューションが重要であるかとの課題に対して、ロシアで唯一のIDISパートナーであるAVIX社は、スタジアムの管理者、イベントプランナーと緊密に協力して詳細なリスクアセスメントを実施しました。

詳細な調査の結果、各会場で重要な内部エリアとチェックポイントを含むリスクの比較的高いエリアを24時間365日監視するためには新しい監視システムが必要であるとの判断がされました。

IDIS トータルソリューション

IDISの技術は、スタジアムとその周辺を包括的にカバーするために選ばれました。それぞれのロケーションにフルHD、H.265コーデックのPTZカメラ、トゥルーワイドダイナミックレンジのIRパレットカメラ、ボックスカメラからなる3,000台のIPカメラを設置し、屋外に設置されるすべてのカメラはロシアの厳しい気象条件に耐えうる仕様になっています。

すべてのIDIS PTZカメラには、Smart UX Controls v2.0が搭載され「スリングショット」「ラバーバンド」コントロールといった直感的な操作を可能にしています。優れた性能を発揮するPTZカメラは、最大30倍光学ズームとパワードIR LEDを使用し、暗闇の中でも最大150メートルにおいて円滑なモーション検知と画像解析が可能です。

また、今回設置されたシステムには、高度な独自技術であるIDIS インテリジェントコーデックが採用され、H.265コーデックとMotion Adaptive Transmission (MAT) を組み合わせることで、ストレージと帯域幅を最大90%まで削減することが可能です。

<集中監視システム>

55インチのビデオウォールで2つのスタジアムの監視デバイスを集中コントロール
セキュリティスタッフは、遠隔に設置された50台のNVR(DR-8364)にアクセスすることができ、保存される60日間の録画データを検索再生することが可能
セキュリティスタッフは、いかなる違反行為、不正行為を迅速に検出し、即時に対応することが可能



重要な録画データの損失を防止するために、IDIS Critical Failoverを採用。
システムは、ネットワーク障害、ストレージ障害、レコーダーハードウェア障害、電源障害といった障害が発生した場合に自動的に録画が継続されるようシステムを構築しデータの損失を防ぎます。

実績と効果

AVIXによって導入されたIDISのテクノロジーは、堅牢な監視機能をスタジアムのセキュリティチームに提供し、多大なる成果に貢献しました。特に試合の前後、最中に発生するピークストレスに対してSmart UX Controls V2.0による直感的かつ最適化されたPTZ操作を可能にし、IDISインテリジェントコーデックは複雑な群衆シーンの映像からもスピーディな検索とモニタリングを可能にしました。



AVIXのCEO, アレクサンダー・クリコフ 談

「今回のハイプロファイルでミッションクリティカルなアプリケーションには、非常に高い技術が求められました。この広いスタジアムにて起こる様々な出来事に対して制御可能にする必要があり、60日間の長期に渡っての録画映像の保証を求められました。IDISトータルソリューションは、期待通りのパフォーマンスで機能しておりお客様も大変満足されています。」



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

イーグル・アイ・ネットワークス社CEO ディーン・ドラコ氏に聞く



弊誌は、イーグル・アイ・ネットワークス社設立者兼CEOディーン・ドラコ氏にインタビューする機会を得た。本稿では、同氏へのインタビューを通して、クラウド型VMSという特長を有する同社製品Eagle Eye Networks Camera VMSを紹介する。



[Q]Eagle Eye VMSの概要

Eagle Eye Network Cloud VMSは、無制限のサイト、カメラ、およびユーザに対応できるように設計されたスケーラブルなクラウド映像管理ソフトウェアで、主な特長は次の通りである。

- フル機能のVMSをクラウド内に構築

- 運用コストを削減する設計で、TCOを削減
- ソフトウェア更新が不要
- 100%ブラウザとモバイル・ベース
oクロス・ブラウザ互換、インストールするプラグインまたはドライバは不要



o専用のiOSとAndroidアプリ

- 新機能のコストが不要
- 現場でのハードウェアの交換が容易
- サポートするサーバが不要
- 比類のないユーザ・サポート
- 全てメーカーのアナログ、IP、HD同軸カメラで動作



Eagle Eye Cloud VMSのコンポーネントは次の通り。

- 1)ユーザ・サイトに設置されたカメラ。
- 2)敷地内にあるEagle Eye Bridge で映像を暗号化してクラウドに送信。
- 3)Eagle Eye Cloud データセンターに暗号化された映像を冗長して保存。
- 4)ウェブ・ブラウザまたはモバイル・アプリケーションにより、いつでもどこからでも実況または録画映像を表示したり、設定を管理したり、アラートを受信したりできる。

[Q]Eagle Eye VMSの概要

Eagle Eye VMSはフル機能の映像管理ソフトウェア。そして、中小企業オーナーや大企業が必要とする全ての機能を備えている。例えば20カ所にあるレストラン・オーナーのために使用することができる。工場、倉庫、オフィスビルなどでも使用可能だ。また、アパートなどの建物、住宅、市街地のモニタリングにも適している。1000箇所全てを1つのインタフェースで表示したいユーザに適している。

Eagle Eye VMSは、映像をクラウドに記録することも、ローカルに保存することもできる。Eagle EyeのFlex Storage™テクノロジーは、ユーザが映像の保存場所を選択することができる。オンサイト・ハードウェアの領域に限らず、ユーザは映像の一部または全部をクラウドに保存できる。ほとんどのユーザは、より安全であることを理由に、映像の大半をクラウドに送信する。

Eagle Eyeのオンサイト・ハードウェア(ブリッジとCMVRS)は、カメラの録画停止を防止する。インターネットはダウンする可能性があるが、Eagle Eye Security Camera VMSは機能し続ける。Eagle Eye・ブリッジは、カメラと常時通信し、ステータスを監視し、





改竄されていないことを確認することができる。ブリッジはまた、動体検知、画像解析、画像圧縮、安全な伝送のために映像を暗号化できる。

[Q]Eagle Eye VMSの映像管理システムの特長は？

以下の機能をサポートしている。

- ユーザ・アカウントごとに最大100万台のカメラ映像を録画する
- 50種類のメーカーの2,000種類以上のカメラをサポート
- 同軸使用のアナログとHDカメラの双方をサポート
- PTZ、360度カメラをサポート
- 無制限のユーザの同時使用を実現
- フル・アクセス・コントロールとユーザごとのアクセス権設定システム
- ライブ・ビューと録画ビュー
- AndroidとiOS双方のモバイル・アプリのフル機能をサポート
- 無制限のカスタム設定
- クラウド解析機能を組み込み
- 統合およびIoTアプリケーション用のオープンAPI
- アクセス・コントロール・システムとの統合
- カメラ性能の監視
- カメラ死活状況の警告
- 動体やその他の活動に関するアラートを電子メールで送信
- 識別のためのAI技術の統合
- 全ての映像の完全な暗号化
- トリプル・リダンダント映像ストレージ
- 世界地図とGoogleマップとの統合



Eagle Eye Networks Camera VMSはイーグル・アイ・ネットワークス社が管理するソフトウェア。具体的には、同社がプラットフォームおよびデータセンターオペレーションそしてオンサイト・アプライアンスを管理し、最大の可用性と稼働時間、サイバー・セキュリティを保証している。これはディーラーとユーザには非常に便利だ。

[Q]競合他社のVMSとの違いは？

競合他社のVMSは、通常、映像をオンサイトまたはユーザ管理のサーバールームに記録する。そのため、IT部門のサポートや修理また保守点検が必要となる。Eagle Eye Networks Cloud VMSは、エンド・ユーザまたはインテグレータをこれらの業務作業から解放するサービスを提供している。その結果コストおよび総所有コスト(TCO)を削減している。

Eagle Eye VMSには、完全に機能するモバイル・アプリが含まれている。インストーラとインテグレータは、Eagle Eye VMSをインストールするための専用コンピュータを用意する必要がない。



Eagle Eye Networks Cloud VMSは、あらゆる方法でハッカーに対してサイバー・セキュアになるように設計されている。本製品には、常時システムを監視している熟練のセキュリティ・チームがいる。保存映像は常に暗号化されている。ほとんどのオンサイトVMSでは、限られた範囲の異なるIPカメラにのみ対応している。そのため、通常サポートしているカメラ・メーカーは限定的だ。

一方、イーグルアイ・ネットワーク社製クラウドVMSは、他のVMSとは異なり、50種類の異なるメーカーの2000種類以上のカメラをサポートし、IPカメラだけでなく、アナログカメラやHD Over Coaxカメラの混在を共有することができる。

Eagle Eye Networks Cloud VMSは、インテリジェントな帯域幅管理と呼ばれる独自機能を備えている。これにより、サイトおよびユーザの好みの設定で使用可能な帯域幅に基づいて、必要な帯域幅の消費を50%も削減できる。



また、Eagle Eye Networks Cloud VMSでは、標準オプションとして7日間から5年間の映像の保持期間を選択することができ、5年間を超えるデータ保存にもカスタマイズが可能だ。

Eagle Eye Networks Cloud VMSでは、カメラごとにライセンス料金が必要となる。ユーザは、必要なものを購入し、希望する保持期間を選択するだけで済む。HDDスペースを計算する必要もない。ユーザは、いつでもカメラの追加や削除、カメラ設定の変更、分析の追加や削除を簡単に行うことができる。ユーザは、自分が使用しているものに対してのみ料金を支払うだけで済む。

一般的には、ほとんどのオンサイトVMSが、限られた範囲の異なるIPカメラにのみ対応している。Eagle Eye Networks Cloud VMSは、他のVMSと異なり、IPカメラとアナログカメラまたHD Over Coaxカメラに対応している。

ほとんどのVMSはライブや履歴のビデオを見るための遠隔操作を提供しているが、多くの場合、VPNの制限、特に本物のクラウド・ソリューションではないため、アカウントに同時にログインできるユーザ数を制限している。

イーグル・アイ社のクラウド・ソリューションは、全て映像を現地のデータ・センタに保存するため、ユーザはブラウザやモバイルアプリを使用してライブ映像と履歴映像に簡単にアクセスでき、アカウントに同時にアクセスできるユーザ数に制限もない。



[Q] ONVIFの対応は?

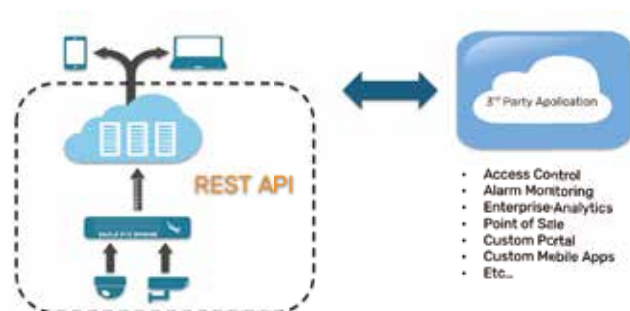
イーグル・アイ・ネットワークス社はONVIFのサポータであり、Eagle Eye Networks Cloud VMSは、ONVIF規格に準拠して数千台以上のカメラ機種をサポートしている。

[Q] サードパーティのソフトウェアの親和性は?

イーグル・アイ・ネットワークス社はEagle Eye Cloud Video API

を使用しているサードパーティと技術パートナーシップを結んでいる。実例のアプリケーションには、1)アクセス・コントロール、2)アラーム監視、3)映像解析、4)POSデータ、5)カスタム・ポータル、そして6)カスタム・モバイル・アプリケーションがある。

Eagle Eye Video APIは、監視映像の録画、タグ付け、および保存のための包括的なRESTベースのAPIである。Eagle Eye Video APIは、カメラとのインタフェース、映像録画、クラウドへの安全な送信と保存、そしてサードパーティのアプリケーションでの使用を可能にするなど、全ての高負荷を処理する。多くのサードパーティとの統合があり、開発中のものも数多くある。



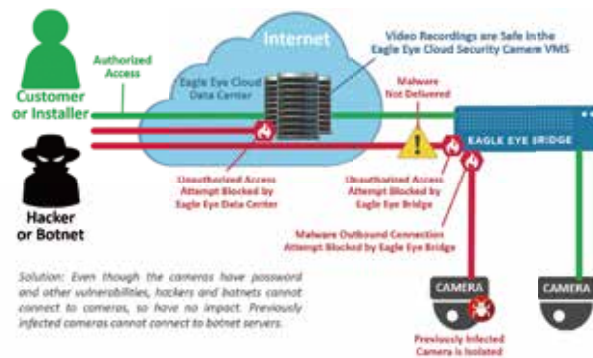
具体的な事例は当社技術パートナーシップを参照することができる。

www.eagleeyenetworks.com/ja

[Q]サイバーセキュリティの取り組みについて

Eagle Eye Cloudは、Eagle Eye Cloud VMSのサイバー・セキュリティと、Eagle Eye Cameraサイバー・ロックダウン機能などの特定のサイバー・セキュリティ機能に関する複数のホワイトペーパーを提供している。

- Eagle Eye Cameraサイバー・ロックダウンでは以下のことが行われている。
 - カメラとインターネットとの通信をブロックする。
 - カメラが攻撃されたり、侵害されたりするのを防ぐ。
 - カメラにインストール済みのトロイの木馬がインターネット



と通信することを許可しない。

サイバーセキュリティのホワイトペーパーは、下記から見る
ことができる。

www.een.com/docs/white-papers/

[Q] Eagle Eye Network Camera VMSの導入手順と費用は？

Eagle Eye Networks Cloud VMSのアカウントは、各国の販売代理店と協力して設定することができる。販売代理店は、小規模な独立したセキュリティ統合企業から大規模なセキュリティ・サービス企業まで対応したソリューションを幅広く取り揃えている。再販業者は現場に設置するための適切な機器を提案し、新規または既存のカメラに接続している。敷地内に設置される典型的な機器には、再販業者の提案するアーキテクチャに応じて、イーグル・アイ・ネットワークス社で「ブリッジ」または「CMVR」と呼んでいる小型機器などがある。イーグル・アイ・ネットワーク社と販売代理店がアカウントを開始し、選択したブリッジとPOEスイッチを設定する小さな「セットアップ料金」を使用してイーグル・アイ・ブリッジを提案している。

システムをインストールし、カメラを追加すると、再販業者とユーザは、カメラごとに希望の映像解像度とサブスクリプション期間を選択する。インストール後に、再販業者はユーザに対して選択したサブスクリプション内容の請求書を毎月あるいは毎年請求する。

[Q]世界の地域(EMEA、APAC、NCSA)導入実績は？

イーグル・アイ・ネットワーク社は、米国シリコンバレーで創業した。創業者は、ニューヨーク証券取引所に上場しているバラクーダ・ネットワークス社を創設したディーン・ドラコ氏で、バラクーダ・ネットワークス社は、現在も世界のトップ・サイバーセキュリティ企業である。

イーグル・アイ・ネットワーク社は、米国の5大セキュリティ企業であるタイコ社、ADT社、プロテクション1社、セキュリタス社、ディーボルド社と提携している。イーグル・アイ・ネットワーク社は、米国でトップクラスのクラウド映像監視企業と評価されている。

また、イーグル・アイ・ネットワーク社は2017年にパナソニックのクラウドカメラ部門を買収した。これにより、当社は欧州での事業展開を加速し、欧州市場で代表的なクラウド映像監視企業に成長した。

イーグル・アイ・ネットワーク社は現在、米国とカナダ、英国とオランダ、ドイツとアラブ首長国連邦、そして香港と東京で11のデータセンターを運営している。



[Q]パートナー企業向けのトレーニング・システムの内容は？

イーグル・アイ・ネットワーク社は、イーグル・アイ大学を運営している。イーグル・アイ大学では、販売および技術のトレーニングを提供している。トレーニングは世界各地で教室形式で提供し、オンラインでも提供している。

販売トレーニングの内容には、クラウド映像の概要および利点、価格やサービス、ハードウェアの互換性と選択、適切なコートやカメラ選択などで、なぜクラウド映像がオンプレミス映像よりもサイバーセキュアである理由などがある。

技術トレーニングの内容には、基本的なネットワーク、イーグル・アイ・システムのセットアップと構成、システムのデバッグ手法、帯域幅の管理と監視、カメラの選択、スイッチ管理、ネットワーク構成などが含まれている。これらは、生徒が研究所の全ての機器をセットアップしてテストするトレーニングとなっている。

エグゼクティブ・トレーニングの内容には、経常収益ビジネスを構築する方法、クラウドを販売する利点、ユーザ・サービスと満足度を最大限に高める方法がある。クラウドを売る方法については、従来のハードウェア販売からより多くの定期的な収益に移行したい経営幹部向けの内容で構成されている。

[Q]ユーザ向けトレーニング・システムの内容は？

イーグル・アイ・ネットワーク社の代理店および再販企業は、通常、Eagle Eye Networks Cloud VMSの使用方法についてユーザを訓練する。しかし、イーグル・アイ・ネットワーク社は、深い訓練を希望するユーザには、代理店や再販企業とともに提供されるユーザ・トレーニングを提供している。

イーグル・アイ・ネットワーク社

〒150-0036 東京都渋谷区南平台町16-28 グラスシティ渋谷 6F

TEL・03-6866-2926

EMAIL・APACsales@een.com



キヤノン、アクシス社の完全子会社化を発表

2018年10月22日、キヤノンはアクシス社の株式を Elliott International L.P.ならびにThe Liverpool Limited Partnership より株式数:7,825,516株を取得することで合意し、株式譲渡契約を締結したと発表した。



これにより、キヤノンは、アクシス社の発行済普通株式総数の90%超(97.9%、株式:68,000,798株)を保有することになるため、アクシス社の取締役会に対し、Nasdaq Stockholm証券取引所への上場廃止申請を要請するとともに、スウェーデン

会社法に基づき、強制株式買い取り手続きにより同社の残りの全株式を取得し、完全子会社化する予定。

<https://global.canon/ja/news/2018/20181022.html>

今回のアクシス社の完全子会社化により、今後キヤノングループが映像監視市場でどのような行動に出るかが注目される。具体的には、アクシス社本社との関係をどう構築し維持していくか、そして、日本市場でのキヤノン製品とアクシス社製品とをどのように連携するか、さらには、VMS世界大手のマイルストーン社を含めたキヤノン連合としての事業展開に注目が集まる。

URL・<https://global.canon/ja/news/2018/20181022.html>

ルネサス エレクトロニクス、IDTを買収

今回買収した米国の半導体会社Integrated Device Technology, Inc.(IDT)は、センサ、コネクティビティ、ワイヤレスパワーを中心としたアナログ・ミックスドシグナル製品を提供している。

本買収により、電子機器の性能・効率の向上に強みを持つ、組み込みプロセッサとアナログ・ミックスド・シグナル製品の大手企業が統合することとなる。本買収は、両社の取締役会にて全会一致で可決された。買収完了は、IDTの株主総会における合併の承認、および関係当事国において必要となる当局の承認の取得を前提としており、2019年上期中を予定している。

【今回の買収効果】

● アナログ・ミックスドシグナル企業を買収し、補完的に製品ラインアップを拡充。ルネサスの成長戦略を着実に推進

● IDTのセンサ、高性能インターコネクト、RF/オプティカルおよびワイヤレスパワーなどのアナログ・ミックスドシグナル製品とルネサスのマイコン/SoCおよびパワーマネジメントICとの組み合わせにより、IoTやビッグデータ処理などで増大・高速化する情報処理要求に対応可能な網羅的なソリューションを提供

● IDTのメモリアンターコネクト製品や特定用途向けパワーマネジメントICを足掛かりに、ルネサスは成長著しいデータエコノミー関連分野での成長機会を創出するとともに、産業・自動車分野でのポジション強化を実現

エグザック・ヴィジョン社共同設立者、Qumulex社を創業

エグザック・ヴィジョン社共同設立者であるダン・リットマン氏、トーマス・バックリィ氏、デイヴィッド・アンダーウッド氏はQumulex社を創業した。3氏は2000年にDVRベースのアンダーバ(Andover)社を5千万ドルでインテグラル社に売却後2002年にNVRベースのエグザック(exacq Vision)社を設立し、2013年に同社をタイコ社1億5千万ドルで売却し、2017年に退職した。

今回設立したQumulex社は、クラウドおよびIoT技術を活用し

て、商用分野での映像監視およびアクセス・コントロール製品を2019年から提供する。製品キーワードは、Cloud, Commercial, Easy(クラウド、民間、簡単)としている。

そしてその市場は、クラウド・ベースの映像監視システム分野で先行しているマイルストーン関連企業アーカス・グローバル社製アーカス・ソリューションやEagle Eye Networks社製Eagle Eye Security Camera VMSと競合する。

今回の新会社設立は、映像監視プラットフォームがDVR/NVRからサーバそしてクラウドに技術遷移する潮流を象徴しているとも言える。

URL・<https://qumulex.com/>

ジェムアルト社、2017年上半期「Breach Level Index(情報漏洩危険度指数)」とデータの消失に関する意識調査を発表を発表

世界中で公表されたデータ漏洩事例のデータベースである「Breach Level Index」(BLI、情報漏洩危険度指数)の最新の集計結果によると、2018年上半期に世界中で発生したデータ漏洩は945件で、45億件のデータが漏洩しており、前年同期と比較すると、紛失、盗難、漏洩したデータ数は、133%も増加している。また、データ漏洩事例件数は前年同期との比較で減少しているため、各事例におけるデータ漏洩数が増加していることが分かる。

ケンブリッジ・アナリティカフェイスブック事件を含む合計6件のソーシャルメディア関係の漏洩が、漏洩データ数の56%以上を占めた。945件のデータ漏洩のうち、189件(全データ漏洩の20%)については、漏洩データ数が不明または非公開だった。

BLIはグローバルなデータベースで、データ漏洩を追跡しその深刻度を漏洩したデータ数、データの種類、漏洩源、データがどのように利用されたか、データが暗号化により守られていたかどうかなどの複数の要因を考慮して数値化している。BLIは、各漏洩事例に深刻度スコアをつけることで、「それほど深刻でない」データ漏洩と「危険な」データ漏洩を区別した比較リストを生成している。

BLIによると、公表されたデータ漏洩の評価を始めた2013年以来、今日までに150億件近いデータが漏洩している。2018年上半期には、医療データ、クレジットカード/口座番号、個人を特定できる情報など、毎日2500万件以上の、言い換えると毎秒291件のデータが漏洩または暴露されている。特に問題なのは、盗難、紛失、漏洩したデータのうち、情報を無価値化し利用できないよう暗号で保護されていたのは1%に過ぎなかったことだ。これは、2017年上半期と比較して1.5ポイントの減少だった。

■データ漏洩の主な漏洩源

悪意のある部外者がデータ漏洩の原因で最も大きな割合を占めた(56%)。2017年下半期と比較すると、7%という減少だが、紛失、盗難、漏洩したデータ数の80%以上を占めた。不慮の事故による漏洩は、当半期中に8億7900万件を超え(9%)、データ漏洩事例件数の3分の1を超える2番目に多い原因となっている。悪意のある部内者による攻撃が関係するデータ数と漏洩事例件数は、前年同期と比べて50%減少した。

■データ漏洩の主な種類

個人情報の盗難が引き続きデータ漏洩の最も一般的な種類

となっている。これは、2013年にジェムアルト社が追跡を開始してから変わっていない。個人情報の盗難の件数は2017年下半期と比べて13%増加して64%強となった。漏洩によって盗まれたデータ数は539%の増加となり、全盗難データ数の87%強を占めた。

■データ漏洩の影響を最も受けた業種

漏洩事例件数は、ほとんどの業種で前半期と比較して増加した。例外は、官公庁、土業、小売り、テクノロジーだが、官公庁と小売りは、漏洩事例件数は減少したものの漏洩データ数は増加している。漏洩事例件数では、ヘルスケアが引き続き最も多く被害を受けている(27%)。

ソーシャル・メディアは、大きく報道されたフェイスブックとツイッターでの顧客データ漏洩件数(それぞれ22億件と3億3600万件)の影響があり、漏洩データ数で最上位となった(56%)。

■データ漏洩の地域的分布

引き続きトップは北米で、全データ漏洩事例件数および漏洩データ数の多数を占め、それぞれ59%、72%となっている。攻撃対象では、米国が抜きん出て最も多くターゲットとされ、世界の漏洩事例件数の57%以上、盗難データ数の72%を占めている。ただし、全体的な漏洩事例件数は2017年下半期と比較して17%減少している。

欧州では漏洩事例件数は36%減少したが、漏洩したデータの数は28%増加し、攻撃の深刻度が増していることが分かる。欧州で最も漏洩の多かった国は、引き続き英国となった。2018年下半期にはGDPRが完全実施されることから、報告される漏洩事例件数は増加が始まると予想される。

関係資料:

・業種、漏洩源、種類、地域別のデータ漏洩事例の詳細

First Half 2017 Breach Level Index Report

<https://dl.nxlk.jp/449f788a-f0d1-49f3-81f5-4b9b703e8ecf>

・インフォグラフィック

<https://dl.nxlk.jp/10bb4cf8-caa6-43c7-9ea3-173d0c6cec87>

・BLIウェブサイト

https://www.breachlevelindex.com/request-report?utm_campaign=breach-level-index&utm_medium=press-release&utm_source=&utm_content=&utm_term

シマンテック、エンドポイント・セキュリティの強化と簡素化を実現する新しいSymantec ITMS 8.5を発表

サイバー・セキュリティ企業のシマンテック コーポレーションは、Symantec IT Management Suite (ITMS) を強化したことを発表した。新しいITMS 8.5は、リアルタイムのエンドポイント管理機能に加えて、Symantec Endpoint Protection (SEP) およびControl Compliance Suiteとの統合により、攻撃や深刻な脆弱性からの保護をさらに高めた。これにより、クラウド世代のエンドポイント管理とコントロールに必要な柔軟性と多用途性を顧客に提供する。

米国Enterprise Strategy Group (ESG)社の調査によると、IT部門がサイバー・セキュリティ・ツールの調達と管理に関わる機会はこれまで以上に増えている。これに伴い、困難で時間を要する脆弱性の修復とエンドポイントへのパッチ適用作業が増え、IT運用に多大な労力、課題や障害をもたらしている。

ITMS 8.5はIT部門にリアルタイムのエンドポイント管理機能、自動化、および柔軟性を提供し、運用をさらに簡素化すると共にその有効性を高める。ITMS 8.5はデスクトップ、ラップトップ、およびサーバを含むエンドポイントとそのOS設定を対象とし、そのライフサイクル全体を通じて管理、パッチ適用、および修

復を行う。またネットワークの境界外にあるエンドポイントも管理するため、従業員がリモートワークを行う際にも継続して保護される。

■主要なアップデート

- スピーディーな管理・オンデマンドかつリアルタイムでデータが収集され、多くの情報に基づくセキュリティ関連の判断をより迅速に行うことを可能にするインテリジェンスを実現。
- エンドポイント検疫・コンプライアンススキャンではじかれたエンドポイントを、インストールされているSEPで直接ネットワークからブロックすることにより、WannaCryのようなエンドポイントでの感染を防止。
- 脆弱性スキャンと修復の自動化・Control Compliance Suite Vulnerability Managerとの統合により、脆弱性をスキャンして修復を必要とするエンドポイントへ自動的にパッチを適用。
- モダンなUIワークスペース・日常作業向けにシンプルさとスピードを主眼として設計された新しいUIにより、経験のないスタッフでも特別なトレーニングを受けることなくITMSを活用することが可能。

ダファ社、一般消費者向けIoT製品「imou」を発表



中国大手映像監視機器メーカーのダファ社は、業界専門家や主要販売協賛会社そして一部ユーザを招いて、「スマートライフを享受する」をコンセプトにしたimouブランド発表会を北京で開催した。同社は、Imouを同社の消費者向けIoT製品ブランドとして、

消費者に高品質な製品とサービスを提供するための世界市場における新しいブランドと位置づけ、製品は「ダファHeart of City (HOC)」の枠組



みに基づいている。

発表会場ではimouブランド製品を多数展示した。その中には、スマートロックを搭載した世界初のスマートロックを搭載したインテリジェント・フェイススペースでロックを解除する、業界初のAI顔認識技術があった。この技術によりユーザはキー操作から解放される。

さらに、imou ワイヤフリー・セキュリティ・システムも発表した。本システムは、わずか5時間の充電でカメラを6カ月間使用することが可能で、カメラを「フリー」にして「完全なワイヤフリー」での操作を実現することができる。



「エアロボクラウド」と「エアロボマーカ―」、基準点測量に対応

エアロセンスでは、この度、産業用ドローンのためのクラウドサービス「エアロボクラウド」およびGNSS測位機能付き対空標識「エアロボマーカ―」を基準点測量に対応した。エアロボマーカ―で観測したGNSSログデータをエアロボクラウドへアップロードするだけで、基準点測量に必要な一連の三次元網平均計算が自動で実行される。この結果、多くの工数を要していた基準点測量の工程の大幅な効率化が可能となる。



エアロボクラウド・ドローンでの測量や点検といった業務をサポートするためのクラウド・サービスで、大量の撮影データやフライトの管理、点群や3Dメッシュを作成する写真測量処理など一連のワークフローをブラ

ウザだけで簡単に実現できる。 <https://aerobocloud.com>

エアロボマーカ―・エアロセンスが開発したドローン測量専

用の対空標識。同社は、GPS 測位機能を搭載したエアロボマーカ―を開発し、そのマーカ―位置情報と3Dモデルとの対応処理を自動化させ、i-Construction 基準に沿ったドローン測量をより簡便にできるようにした。

基準点測量に対応

エアロボマーカ―は、これまでUAV測量用対空標識として、現場に設置するだけで標定点を自動計測し、高精度3次元モデルを誰でも簡単に作成できるように、今回基準点測量に対応したことで、標定点の基準となる基準点の測量をも可能となった。本対応により、エアロボマーカ―で計測した観測ログをエアロボクラウドへアップロードするだけで、基準点測量に必要な下記の処理がエアロボクラウドが自動で実行する。

- 観測ログのマルチセッション分割
- 多角網の生成
- 基線解析
- 点検計算
- 三次元網平均計算(仮定網・厳密網)
- 帳票出力(準則に沿った手簿、記簿、成果簿、網図、精度管理表)

ジョンソンコントロールズ社、タイコ社セキュリティ事業の提供を開始

ジョンソンコントロールズは、タイコ社ブランドのセキュリティ事業について、グローバル顧客として既にビルオートメーション事業でお取引のある多国籍企業を対象に、日本国内での提供を開始した。

同社は全世界でスマートビルやスマートシティを実現することでエネルギー効率を最適化し、ビルオートメーション業界で事業を展開してきた。2016年9月には防火・防災、セキュリティシステムの国際供給企業だったタイコ社と戦略的に統合、両社のビジネス基盤を一体化することで、ビルの安全性を向上し、効率化を促進するトータル・ソリューションをワンストップで提供で

きる体制を整えてきた。

物理セキュリティ情報管理(PSIM:Physical Security Information System)を実現する、旧タイコの状況認識(Situational Awareness)プラットフォームは、監視カメラや入退室管理、防火など様々なセキュリティ関連システムを1つのインタフェースで統合・管理できるため、ジョンソンコントロールズ社のMetasys®ビル・オートメーション・システムと連携させることで、さらに効率的で相乗効果の高い建物全体のシステム統合を実現する。

国土交通省、空港制限区域内の自動走行の実証実験を計画

当実験は国土交通省航空局が、深刻化する空港の地上支援業務の労働力不足に対応するため、空港の制限区域内において、乗客・乗員の輸送を想定した自動走行車両の実証実験を行う国内初の取り組みで、実証実験実施時期は2018年11月頃～2019年2月頃の間を予定している。

本プロジェクトでは、成田国際空港において、地上支援業務の一部を請け負っているKONOIKEグループの日本空港サービ

ス株式会社(JASCO)の作業スタッフの空港内移動を、ZMPが提供する自動運転実験車両で実施し、空港制限区域内という一般道路とは異なるルールが適用される環境下で、自動運転技術実装に向けた検証および課題の抽出を行う。

ZMPは自社で自動運転技術や自動運転車両管理システムなどを開発し、自動運転プラットフォームとして提供している。

Eagle Eye Networks、18ヶ月間にわたるグローバル化プロジェクトを完了

Eagle Eye Networksは、世界各地に存在するユーザの要望を満たすための18ヶ月間に及ぶグローバル化プロジェクトが完了しとを公表した。同社は、グローバル化への取り組みを、ユーザの要望を満たすだけでなく、再販業者やユーザに付加価値をさらに提供するという重要な使命の一部と位置づけている。



完了したグローバル化プロジェクトの内容は下記の通り。

●データセンター

Eagle Eye Networksは、ロンドン、ドバイ、ドイツなどで成長と拡張に合わせデータセンターを増設し、欧州や中東での同社のチャンネル拡大の準備を行ってきた。さらにユーザの要望により、モンテリオールとアムステルダムのもデータセンターも大幅に拡張した。ユーザには世界各地のデータセンターに映像保存ができるオプションが用意されている。世界各地にある同社データセンターを拡張していくことで、企業ユーザは国が固有に定めている映像ストレージ要件を遵守しやすくなる。同社では、2018年、2019年にかけてデータセンターをさらに拡張する計画がある。

●Eagle Eye ユーザ・エクスペリエンス

Eagle Eye ユーザ・インタフェイスは複数の言語にローカライズされている。言語はユーザごとに設定でき、ユーザのプロファイルに基づいて変更することができる。全ての通知、メール、アラートは、ユーザ設定した言語で送信される。運営担当者は、自身に合った言語で映像をフル活用できるようになり、運営効率を向上させることができる。

●Eagle Eye リセラー・ダッシュボード

Eagle Eye リセラー・ダッシュボードは英語のほか、スペイン

語と日本語、ドイツ語とオランダ語そしてフランス語などの言語にローカライズされている。このダッシュボードを使用して、再販業者はEagle Eye セキュリティ・カメラ VMSを使用する顧客のアラート設定や、選択した言語でのオペレーション、モニタリング、アラート受信、その他設定ができる。この新サービスの機能により、世界各地のチャンネル・パートナーは、大幅な運営改善ができる。

●マーケティング・ウェブサイト

Eagle Eye Networksのウェブサイトは、英語のほかスペイン語、日本語やドイツ語、オランダ語やフランス語などの言語で利用することができる。ローカライズされたコンテンツを提供することで、ウェブサイトを訪れる世界中のユーザが、Eagle Eyeのウェブサイトを利用し閲覧することができる。

●Eagle Eye University

Eagle Eye Networksは、欧州でもEagle Eye University事業を拡大した。Eagle Eye Universityには、オンサイト・トレーニングとオンライン・トレーニングがある。Eagle Eye Universityは現在、チャンネル・パートナーの要望により、英語とオランダ語そしてスペイン語で利用することができる。認可されたEagle Eye Networksパートナーは、Eagle Eyeのウェブサイトで、オンサイト・トレーニング、またはオンライン・トレーニングにサインアップできる。

●カスタマーサポート

Eagle Eye Networksはサポート営業時間を延長し、サポートは新しく多言語対応が可能になった。Eagle Eye Networksのカスタマー・サポートは、英語、オランダ語、スペイン語、および日本語で、1日24時間、週5日の利用が可能。サポート営業時間の延長とローカライズされた対応により、Eagle Eye Networksのユーザは、より迅速な問題解決とユーザ・エクスペリエンスの向上を実現した。

■URL <https://www.een.com/ja/>

米運輸保安局、新型X線検査装置の全米各地空港への導入を発表

米運輸保安局(TSA)は2018年7月、医療用のコンピューター断層撮影(CT)技術を応用して荷物を全方位からスキャンする新型のX線検査装置を、全米各地の空港に導入すると発表した。従来の2次元画像とは異なり、高精度の3D立体画像が表示されるため、荷物に隠された爆発物や武器を検知しやすくなる。乗客がペットボトルなどの液体やノートパソコンをいちいち手荷

物から取り出す手間も省ける可能性がある。

価格は1台が約30万ドル。マサチューセッツ州ボストンやアリゾナ州フェニックスなど一部の国際空港では既に導入が始まっており、年内に全米の15カ所の空港に計40台、19年度末までには145台以上が設置される見込み。加えて、連邦政府の施設にも16台が導入予定だという。

<https://www.tsa.gov/>

アクロニス、「Acronis Backup ストレージバンドルライセンス」を発表

アクロニス・ジャパンは、Acronis Backupとストレージを自由に組み合わせて購入するライセンス「Acronis Backupストレージバンドルライセンス」の提供を開始した。同製品は、株式会社ネットワークワールドを通じて販売される。

本製品は、ストレージの容量に合わせてAcronis Backup ストレージバンドルライセンスを購入することができ、途中で容量を追加することも可能。ストレージバンドル専用として新しい価格体系となっているため、自社のサイズに合わない高額な大容量のバックアップ・アプライアンスなどを導入する必要はない。PC、物理サーバ、仮想マシンを台数無制限でバックアップすることができ、バックアップデータ以外のデータもストレージに保存することができる。また、管理サーバも任意のロケーションに展開が可能。

【製品概要】

■対象のストレージ・メーカー

- ・NetApp
- ・EMC

■ストレージ容量(RAW容量)

- ・最小容量:4TB
- ・最大容量:無制限

- ・ストレージの容量に合わせてAcronis Backup ストレージ・バンドル・ライセンスを購入
- ・容量の途中追加やストレージの保守延長に合わせてサブスクリプション期間更新も可能

【製品】

■Acronis Backup Advanced Data Storage Appliance 1TB 5年間のサブスクリプションライセンス

型番:SCWBEBLOS91

標準価格(税抜):100,000円

■Acronis Backup Advanced Data Storage Appliance 1TB 1年間のサブスクリプションライセンス、追加ストレージ

型番:SCXBEDLOS91

標準価格(税抜):20,000円

■Acronis Backup Advanced Data Storage Appliance 1TB 1年間のサブスクリプションライセンス、更新

型番:SCXBHBLOS91

標準価格(税抜):20,000円

【問い合わせ先】

ネットワークワールド Acronis製品 お問い合わせ

URL: <https://info-networkworld.smartseminar.jp/public/application/add/202>

ウェスタンデジタルジャパン、新製品を続々と投入

■iNAND® MC EU321 EFD



96層3D NAND技術および高度なUFS 2.1インタフェース技術を採用した組み込みフラッシュドライブ。ウェスタンデジタルのiNAND SmartSLC 5.1アーキテクチャを活用。

■Ultrastar DC HC620



容量15TBのホスト・マネージドSMR ハードディスクドライブ(HDD)。大規模な映像監視システム、ビッグデータに対応するストレージ、ハイパー・スケール・クラウド、データセンターのワークロードに最適。

■iNAND® AT EU312 EFD



UFS2.1規格に準拠した車載用組み込みフラッシュドライブ。車載アプリケーション向けの追加機能を搭載。最先端3D NAND メモリ技術の採用。記憶容量:16GB~ 256GB。

■Ultrastar DC ME200 拡張メモリ



本製品の投入により、ウェスタンデジタルのデータセンター・ポートフォリオをさらに拡大し、急速に成長を遂げるインメモリ・コンピューティング市場に参入。リアルタイム・データ処理、

データベース・スケーリング、アプリケーション・キャッシングおよびクラウド・サービスに対応。

■サンディスク エクストリーム microSDHC/microSDXC UHS-Iカード



1. 最大読取り速度90MB/秒、最大書込み速度70MB/秒の超高速データ転送を実現

2. ビデオスピードクラス30 (V30)、

UHSスピードクラス3 (U3)とCLASS10に対応

3. アプリケーション・パフォーマンス・クラス2 (A2)に対応

4. 32GB、64GB、128GB、256GB、400GBのラインナップ

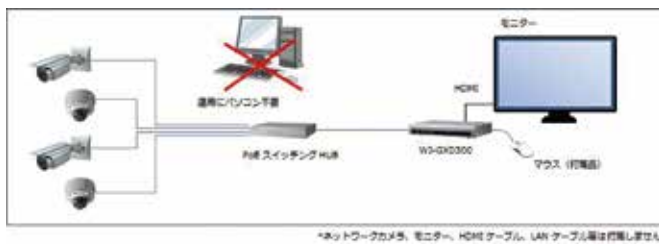
パナソニック、iPro EXTREAMシリーズNVR WJ-GXD300を発表

本製品は、ネットワークカメラの映像を、パソコンを介すること無くモニタに表示するための装置。通常、パソコンを介して表示する場合、パソコンの起動、シャットダウン処理やOSのアップデート、ウイルス対策などを行う必要がありますが、本製品ではその必要がないため、簡単操作、簡単運用が可能。



【主な特長】

■パソコンを介せずにネットワークの映像を表示



■最大64台までのカメラ映像を表示

●別売カメラ拡張キットWJ-GXDE30JWにより、標準の9台から最大64台まで増設

- 4K映像カメラの映像を最大4台まで同時デコードが可能。
- マルチキャスト配信にも対応
- H.265コーデックに対応し、4K HDMI出力の高画質映像で監視
- HDMIモニタ出力に対応し、カメラのライブ画像を高精細に表示
- アナログ・モニタにはHDMIと同じ映像を表示
- 多彩なレイアウト表示
 - 1画、3画(左大画面、右大画面)、4画、6画、9画、16画、25画、36画、64画
 - コリドール2画、3画、4画、5画、6画、7画

■コンパクトなサイズで省スペース化を実現

[幅]280mm [高さ]44mm [奥行き]212mm(ゴム足、突起部含まず)

■簡単運用・簡単設定

- 本機にマウス(付属品)を接続し、モニタ画面を見ながら簡単に設定。
- 簡単設定を実現した「らくらくスタート」により、PC無しで設定が可能。



ZMP、RoboVision® 3 PCI Express 対応版ユニットを販売開始

今回発売した製品は、最新のソニー製車載向け高感度イメージセンサIMX390を採用し、最大150m、水平100度の検出範囲の自動運転用ステレオカメラ「RoboVision®3」にPCI-Express(x4)に対応したフレーム・グラバ同梱ユニット。



有効245万画素

解像度 1920×1080ピクセル(30fps)

水平画角 広角部:100度/望遠部:40度

基線長 広角部:150mm/望遠部:230mm

■フレームグラバユニット

機能 同期撮像、歪補正、ステレオ平行化、HDRモードなど

インタフェース USB 3.0(x2)

■付属ソフトウェア

アプリケーション HDR RAW出力(24bit)・保存、視差画像出力、
ポイントクラウド(PCL対応)出力

動作環境 Windows 10(Core i7・AVX2装備)

【価格(税別)】

■自動運転用ステレオカメラRoboVision®3・・・220万円

■RoboVision®3セット用PC

(組み込み用PCタイプ、オプション)・・・60万円

【製品URL】・・・<https://www.zmp.co.jp/products/robovision3>

【特徴】

- 最大150m、水平100度の検出範囲の4眼ステレオカメラ
- ソニー製車載向け高感度CMOS イメージセンサIMX390採用。HDRとLED信号のフリッカー抑制の同時処理によるADAS・自動運転用として広範囲な照明条件に適用可能
- 距離画像やポイント・クラウドの出力に対応
- Linuxの開発環境に対応したソフトウェア開発環境(SDK)付属

【主な仕様】

■カメラモジュール

イメージセンサ ソニー製CMOSイメージセンサIMX390CQV*

ダファ社、顔認識型屋外用屋外ステーションVTO9341Dを発表

ダファ・テクノロジー社は最先端の顔認識技術を用いてフェンスとロビーの入口に新しいアクセス・コントロール・ソリューションを提供する、新しいマンション・アウトドア・ステーションVTO9341Dを発表した。



屋外のマンションは、常駐セキュリティシステムの安全性と利便性を、ファッショナブルなノンタッチの顔認識エントリーで新しいレベルに高める。一方、従来のロック解除方法は緊急時に保存される。製品の動作温度は-20℃～60℃で、様々な気象条件や地理的領域でスムーズに動作する。アルミ合金板製のシェルで、耐水性と防塵性のIP55規格、耐衝撃性のIK07規格に適合している。侵入防止システムによりさらに強化されたこの製品は、不動産所有者にとって理想的な侵入保護を提供し、セキュリティ・ガードの作業を容易にする。

アルミ合金板製のシェルで、耐水性と防塵性のIP55規格、耐衝撃性のIK07規格に適合している。侵入防止システムによりさらに強化されたこの製品は、不動産所有者にとって理想的な侵入保護を提供し、セキュリティ・ガードの作業を容易にする。

顔認識

VTO9341D内の0.5メートルの距離に近づいて誘導が始まると、2MP CMOSイメージセンサーは顔を高精細カラー画像で捕捉して識別する。0.5秒という短い時間で、認識を完了して住民のためのドアを開くことができる。最大20000人の顔を格納する強力な能力により、システムは大きな住宅地または商業用地の需要に十分である。オートゲインコントロールは、屋外の夜間視界を可能にする、弱い照明状況に対応するために白色光を補う。

複数のロック解除方法

VTO9341Dには、Mifareカード読取機、指紋認証(3000指紋のメモリ搭載)、タッチ・スクリーン・キーボードも装備されており、カード、指紋、パスワードによる複数のロック解除方法を提供します。VTS5240Bマスター・ステーションと一緒に画像をモバイル機器に転送することで、所有者は離れた場所でリモート・ロック解除機能を楽しむこともできます。さらに、オーディオ・システムは双方向通話をサポートしており、訪問者と所有者が顔認識の補助として双方向通信を支援する。

ルネサステクノロジー、IoT機器をセルラー回線で、簡単にクラウド接続できる Renesas Synergy™AE-CLOUD2キットを発売

今回発表した製品は、ハードウェアとソフトウェアを含むリファレンス・デザイン・パッケージRenesas Synergy™AE-CLOUD2キット。このキットにより、セルラー接続を容易に評価することができ、ユーザはLPWA(Low Power Wide Area)セルラーでのIoTアプリケーションの早期構築が可能となる。

【AE-CLOUD2キットの主な機能】

■Synergy S5D9 MCUベース・ボード

■Quectelの超低電力BG96セルラー・モジュール(4G/LTE Cat-M1、Cat-NB1および2G/EGPRS対応)



■データをサンプリングして計測データをクラウドに送信するための各種センサ類

- ・ルネサスの環境計測用デジタル赤外線/照度センサ (ISL29035)
- ・BOSCHの加速度計、ジャイロスコープ用MEMSセンサ (BMI160)
- ・BOSCHのコンパスナビゲーション用3軸地磁気MEMSセンサ (BMM150)
- ・BOSCHのガス、気温、湿度、気圧計測用MEMSセンサ (BME680)

・Knowles社製の音声キャプチャ用アナログ・マイク (SPM0687LR5H-1)

【SSP v.1.5.0の主な機能】

- カスタマイズ可能なプロダクション・グレードのソフトウェア
- ThreadX® RTOS(RealTime Operation System)
- クラウド・サービスとのセキュアなコミュニケーションを実現するNetX Duo™ MQTT(Message Queuing Telemetry Transport)およびNetX Secure™ TLS(Transport Layer Security)
- HTTPSクライアントとHTTP 1.1クライアントをサポート
- クラウド・サービス接続用の無線通信の実装を容易化するワイヤレス・フレームワーク群
- セルラー・フレームワークはデータ通信ネットワークの構成/設定/通信のためのAPIを提供
- AE-CLOUD2を各クラウド・サービス(Amazon、Microsoft、Google、Medium One)にイーサネット、Wi-Fi、LTE IoTセルラーを通して接続するためのリファレンス・コードとマニュアルを含むサンプル・プロジェクト

【価格】・推奨再販売価格199.00米ドル/個

【製品情報】

AE-CLOUD2キット・<http://renessasynergy.com/ae-cloud2>

SSP v1.5.0.(無償)・www.renessasynergy.com/software/ssp.

ADLINK社、新型CompactPCI® 2.0プロセッサ・ブレード2種を発表

今回発表した製品は、cPCI-3630とcPCI-6636。

■cPCI-3630の主な特長

64ビットのIntel Atom®プロセッサXシリーズのSoCおよび最大8GBのソルダードDDR3L-1600 MHz ECCメモリを採用した3UのCompactPCIプロセッサ・ブレード。

シングル・スロット(4HP)またはデュアル・スロット(8HP)幅のフォームファクタに対応し、様々なタータボードを使用して、広範なI/O機能を提供できる。デュアル・スロットの1つはレイヤ2のXMCサイトに対応している。

ストレージ・オプションには、オンボードの32GB SSD、CFastまたはmSATAソケット、レイヤ2ライザカード上の2.5" SATAドライブ・スペースが含まれている。

■cPCI-6636の主な特長

第6/7世代のIntel® Xeon® E3およびIntel® Core™ i3/i5/i7

プロセッサに加え、Intel® HM170またはCM236チップセットを採用した6UのCompactPCIプロセッサ・ブレード。

最大32GBのDDR4-2133メモリ(ソルダード・オンボードの16GBに加え、SODIMMソケット使用で最大16GB)に対応している。

また、シングル・スロット(4HP)およびデュアル・スロット(8HP)幅の両方のフォーム・ファクタに様々なフェース・プレートのI/Oインタフェースを実装できる。デュアル・スロット・バージョンのcPCI-6636DZは6つのRS-232シリアル・ポートに加え、高速通信を可能にする8つのUSB 3.0ポートを備えている。

ストレージオプションには、2.5型SATAドライブスペース、7ピンSATAコネクタ、CFastスロット(アダプタ・ボード使用時)が含まれている。もう一つデュアルスロット・バージョンのcPCI-6636Dでは、CFastの代わりに、PCIe x8アダプタ・ボードを使用して、XMCコネクタに対応している。

IDISコンパクト・ソリューション DR-1シリーズ/TR-1シリーズ/DC-D4212R、DC-E4212WR



【主な特長】

■幅広い市場に対応する新しいセキュリティカメラ・シリーズ

IDISコンパクト・ソリューションは、高品質な性能を維持しながら価格競争力を高めた、IDISの新しいセキュリティカメラ・シリーズ。ネットワークカメラ、NVR、HD-TVIレコーダのラインナップを揃え、幅広い市場に対応。IDIS製高機能クライアント・ソフトウェアに対応し、アナログとIP技術混在のシステム構築も可能。

■使い易さと耐久性

使い勝手が良く、高性能な機能を備えたラインナップには、壁掛け設置と従来の据え置き設置の両方に対応できるレコーダをラインナップ。高品質と信頼性を備え、小売店やレストランチェーンなど小規模から中規模の施設や企業に最適な監視カメラ・システム。

■小さいながらもパワフル

ドーム型カメラとバレット型カメラは限られたスペースに設置するのに最適。また、ライブ再生、モーション検知、アラート機能、

ゾーニング・プライバシー・マスキング機能そしてデイ/ナイト機能を内蔵したパワフルなフルHDカメラ。

■スピーディなインストールと設置コストの削減

4/8チャンネルのHD-TVIレコーダは、既存の同軸ケーブルを活用してスピーディにインストールすることが可能。またIPレコーダはスムーズでクリアなライブ監視が可能で、インテリジェント・コーデックを利用することで帯域幅とストレージの有効活用を実現。

【主な製品】

■IPカメラ

- DC-D4212R・・・フルHD IRドーム型カメラ、電動バリフォーカル(f=4mm)、IRカットフィルタ(焦点距離:20m/65.6ft).
- DC-E4212WR・・・フルHD IRバレット型カメラ、電動バリフォーカル(f=4.0mm)、IK10/IP66対応、IRカットフィルタ(焦点距離:20m)

■NVR(DR-1シリーズ)

- DR-1304P・・・4チャンネル・フルHDレコーダ、総受信スループット50Mbps、最大120ips 5MPリアルタイム・レコーディング
- DR-1308P・・・8チャンネル・フルHDレコーダ、総受信スループット80Mbps、最大240ips 5MPリアルタイム・レコーディング

■TVR (TR-1 シリーズ)

- TR-1204・・・4チャンネル・フルHDレコーダ、HD-TVI/960H/アナログカメラ、最大120ipsフル HDレコーディング
- TR-1208・・・8チャンネル・フルHDレコーダ、HD-TVI/960H/アナログカメラ、最大240ipsフルHDレコーディング

■株式会社セキュア

URL: secureinc.co.jp TEL: 03-6911-0660

TOA、AHDレコーダAH-R116-16を発売

本製品は容量16TBのHDD内蔵のH.264(mpeg-4 AVC)方式のDVR。NTSCカメラとAHDカメラと両方を接続でき、AHDカ

メラと組み合わせることで画像サイズ1920×1080による高画質な映像監視および録画が可能。

■主な仕様

- 映像入力16系統、音声入力16系統
- 最大総録画レート480ipsで録画
- 内蔵の2台のHDDに、ミラーリング機能を搭載
- マウスによる操作やコンビネーション・カメラの操作、ネットワーク経由による遠隔監視



GDPR時代の 映像監視データの保全



相互接続して情報を収集する機器数が増加するにつれて、世界はデータが重要な時代になってきた。

●a&s編集チーム(協力:シーゲイト・テクノロジー社)

遠隔地に保管し、アクセスが稀だった過去とは異なり、データは現在、人々の日々の生活において重要な役割を果たすアプリケーションの最適な機能の鍵となっている。シーゲイト・テクノロジー社が協賛するIDC社報告書「データ・エイジ2025」によると、2025年までの10年間で世界中で発生するデータ量は10倍に増加して163テラバイトになる。このデータのうち約20%が重要で、約10%は最重要だ。

しかし、世界中で生成されたデータと安全なデータとの間には驚くべきギャップがある。「データ・エイジ2025」によれば、2025年までに生産されるデータの90%近くが保護される必要があるが、実際にはその半分以下しか安全ではないと指摘している。

データ侵害と監視業界の高額な事件

データは、その重要度に基づいて様々なカテゴリに分類できる。侵害された場合に発生するコストは、データがどの程度重要なものであるかを決定する重要な要素だ。EUが最近公開したGDPR(一般データ保護規制)によると、データ漏洩のコストは、ますます高騰化するという。十分なセキュリティと技術的な防御と工程を会社内で実施していないことが判明した場合、企業は年間売上高の最大4%の罰金を科せられる可能性がある。

他の業界と同様に、データ・セキュリティは監視部門でも重要だ。シーゲイト・テクノロジー社セキュリティ製品主席責任者デイ

ヴ・シードルフ氏によると、監視データには、EUの個人データとみなされる顔認識データが含まれており、GDPRによる追加の保護が必要な場合がある。

セズドルフ氏によると、「政府および州また地方の管轄区域などには多くのハイエンド部門が存在し、そこには配慮すべき監視データがあり、法的手続きの証拠となる可能性がある。データは1台のドライブに存在し、潜在的に盗難または改竄される可能性があるため、使用していないデータも同様に非常に重要だ」と述べている。

シーゲイト・テクノロジー社国際信頼性&セキュリティ主管ブランドン・グレッグ氏は、「DVRとNVRのセキュリティ・システムは現在の低いセキュリティのためマルウェアおよびボットネットを主な対象となっていて、その他の懸念事項としてユーザ・プライバシーやブラック・メールそして個人情報などがある」と付け加えている。

映像監視がIoTを満たす場合のデータの保全

侵害の脅威に脆弱な他の産業と同様に、映像監視業界も一般電子機器上に構築されている。これは、IoT(Internet of Things:モノのインターネット)の一部である機器でマルウェアや侵入の試みが行われている現状では、ますます重要になりつつある。つまり、データ特に個人データは、GDPR時代の監視において非常に重要な要素となっている。



アクションソフト社
国際営業部長アラン・アタエグ氏



ジェネテック社
欧州事業開発部長
ジーン・フィリップ・デビ氏



シーゲイト・テクノロジー社
国際信頼性&セキュリティ主管
ブランドン・グレッグ氏



セキュア・ロジック社
営業部長ロビン・ヒューズ氏

機密情報を漏洩するような侵入は、企業に無駄な費用をかける可能性がある。これに関連して、データのセキュリティ強化は映像監視で重要な役割を果たす。「AIは映像を構造化データに変換しており、映像監視の価値は高まりつつあるが、安全性の保護の重要性も増している」とダファ・テクノロジー社サイバーセキュリティ製品群ツァン・ジュンチャン氏は語る。そして続けて「IoTは急速に進化している。データの安全性が企業や顧客にとって生命線となっている、相互接続世界を作り出している」と語っている。

この意見には他の業界の専門家も同意している。ジェネテック社欧州事業開発部長ジーン・フィリップ・デビ氏は、パスワード保護や、データのセキュリティを維持する上で重要なものにアクセスしているかなどの個人の記録が要因となっていることを指摘している。これら全ては、組織がGDPRの時代に大きな損害を被る可能性のあるデータの破損に終止符を打たないようにする上で重要な役割を果たす。

監視データの保護ソフトウェア・ベースのデータ保護システムは、セキュリティ管理者がデータの大部分を保護するのに役立ったが、より堅牢なアプローチが必要になった。シードルフ氏によると、データが暗号化されていないカメラやケーブルさらには配置されたドライブから、ハッカーがデータにアクセスすることができる多くのポイントがある。この点で、包括的な監視ソリューションには、カメラを暗号化するハードウェアとデータ信頼モデル、信頼できるカメラ・ハードウェア、暗号化ドライブを使用するNVR / DVRシステム、インスタント・セキュア・イレース (ISE)を使用する廃棄などが含まれる。

データ保全化での脅威を軽減する最良の技法

監視データに対する包括的なエンド・ツー・エンドの保護を確実にするためには、全ての工程を考慮する必要がある。シーゲイト・テクノロジー社国際監視営業&映像監視セグメント主管ダニー・リム氏は、シーゲイト・テクノロジー社のセグメントは、HDD

のファームウェアが改竄されていないこと、カメラとストレージメディアで暗号化を使用すること、新しいシステムにアップグレードする前にデータ退職戦略を持つことなどを指摘している。

「最良の技法は、NVRからそれに続くクラウドやサーバそして安心できる保存場所であるデータセンタまで、カメラで暗号化したデータを送信することだ。そして、データの不正なアクセスや改竄を防ぐため、パスワードのようなアクセス制御を使って安心してデータを暗号化することをお勧めする」とリム氏は述べている。

展開前

監視データのセキュリティは、設計から廃棄まで及ぶ。シーゲイト社は、ファームウェアをロックダウンして、ドライブへの不正アクセスを防止し、本物であり改竄されていない製品を保証している。さらに、セキュア・ブートなどの機能は、起動時に最新のファームウェアがドライブに確実に存在するようにしている。これは、SD&D(Seagate Secure Download&Diagnostics)によって提供している。SD&Dは全てのHDDに標準装備されている。SD&Dは、ドライブのファームウェアへの不正アクセスを防ぎ、ファームウェアの実行可能ファイルや重要なシステム・レベルのデータ改竄を防ぐ。

さらに、ISO 20243規格であるO-TTPS(オープン・トラステッド・テクノロジー・プロバイダ・スタンダード)に準拠することにより、設計を実装するために必要な構成機器が信頼できる企業から供給されていることを確認する。

展開中

シーゲイト・セキュア・エコシステムを導入した同社は、エッセンシャルとサーティファイドに分類された一連の機能を提供している。エッセンシャルには、ほとんどの要件に必要な重要なデータ保護機能が含まれているが、サーティファイドはFIPS140-2、Common Criteria(セキュリティ評価基準)、TAA (Trade

Agreement Act: 通商協定法)などの標準に準拠している。これらの規格を遵守しているシーゲイト社製品は政府やセキュリティの高いデータを扱う企業に最適だといえる。

シードルフ氏は、この段階での懸念事項は、不正なアクセスを防止し、暗号化によってデータを保護するという2つの問題に繋がると指摘している。同社の自己暗号化ドライブは、AES 256標準をハードウェア・ルートキーとともに使用する。展開後はデジタル署名されたファームウェアと不正なファームウェアの検出により、シーゲイト社がユーザにサポートを提供する。

ドライブの交換

必然的に、ライフサイクルの終わりに達したドライブを交換する必要がある。しかし、一旦それに格納されたデータを慎重に考慮することなくこれを行うと、情報への望ましくないアクセスにつながる可能性がある。シーゲイト社のISEにより、管理者はどの機器でも暗号鍵を簡単に置き換えることができるため、データを暗号的に削除することができる。この機能は、NIST 800-88およびISO 27040の国際的に承認されたメディアサニタイズ規格に準拠している。

GDPR法令順守の確保

ここでの重要な点は、映像監視はもはや映像をキャプチャすることではないことに注意することだ。人工知能(AI)ベースの解析とオブジェクト識別システムの導入により、当局は新しい規制のもとで保護される必要のある大量の情報にアクセスすることができる。「GDPRは個人情報の保護を中心としている」とシードルフ氏は説明する。

「私は、顔認識、ナンバープレート番号と登録、個人の正確な地理位置付け、データ・マイニングと集計などの新しいAI技術

が個人データのカテゴリに入ると考えている。EUIはGDPRを実施しているため、監視データには個人データが含まれており、それにに応じて保護する必要がある。データの暗号化は設計上プライバシー保護と考えられるため、監視データ保護の最良の技法となる可能性がある。



シーゲイト・テクノロジー社
国際監視営業&映像監視セグメント主管
ダニー・リム氏

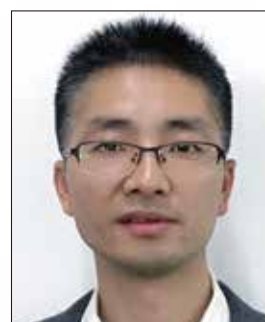
セキュリティ業界での対応状況

ダファ社ツァン氏は、ユーザが個人データの効果的で安全で規制に準拠した処理を実現するのを支援することに責任を持つと述べている。同社は、法律専門家、個人データ保護専門家、ネットワーク・セキュリティ専門家などからなる個人データ保護チームを設立した。本チームはGDPRの要件を満たし、顧客の要求に関する知識が豊富であり、そして、ダファ社は製品やサービスの個人データ保護能力を包括的に評価するシステムを導入している。

アクションソフト社国際営業部長アラン・アタエヴ氏は、顧客にマスキング技術と一般的な推奨事



シーゲイト・テクノロジー社
セキュリティ製品首席責任者
デイヴ・シードルフ氏



ダファ・テクノロジー社
サイバー・セキュリティ製品群
ツァン・ジュンチャン氏

システム構築者が監視データの保全で知っておくべきこと

現在世界中に設置されている監視施設について、シーゲイト・テクノロジー社国際監視営業&映像監視セグメント主管ダニー・リム氏は、機器がますます接続されるにつれて脅威が増加している。また、現在では映像監視はセキュリティにとどまらず、AIや深層学習、クラウド、ビッグデータ、既存のIT基盤との統合などにより、脅威とリスクのレベルは増加すると指摘している。

安全な都市、空港、交通機関、金融/銀行など、様々な技術が最高のリスクにある意思決定、洞察、収束を行うために、データを活用する業種を見ている。

ではシステム構築者(SI)にとって、これはどういう意味か?サイ

バー攻撃は、重要な基盤から財務およびその他の業界に至るまで、様々な業界で行われている。より多くの機器がインターネットに接続されるにつれて、脅威は今後数年で増加するだろう。このような状況の中で、SIは、データができるだけ保護され、設置が物理的および事実上改竄されないことを保証する適切な機器の選択において重要な役割を果たす。



項を提供している説明している。

セキュア・セキュア社営業部長ロビン・ヒューズ氏は、提供内容の一部としてサイバー・セキュリティ・スイートを挙げている。これは、同社内の自動化されたサイバー・セキュリティ管理により、世界中の顧客監視施設が常に安全で最適化し、完全に運用可能であることを保証していると述べている。

「ファイア・ウォール、ソフトウェア・セキュリティ・スイート、その他多くのソフトウェア・ベースのセキュリティ対策はフェール・セーフではなく、映像監視システム構築者はセキュリティ侵害が発生した場合に検出して対応するための追加ツールが必要となる」とヒューズ氏は説明している。

「直感的なインテリジェントなアルゴリズムがシステムの脆弱性を突き止め、サイバー攻撃を防ぐ方法をアドバイスし、マウスをクリックするだけでプロセスを自動化できる。脆弱性は、ネットワーク上の機器が使用する異なるネットワーク・プロトコルをデコードし、人間が判読可能な形式で結果を提示することによって識別される。信頼できるソースの事業用構成機器のみを利用し、暗号化されたHDDを含む全てのレベルで暗号化を提供し、紛失したか盗難されたかまたは引退した製品のデータを外部のいかなる目的にも使用できないようにしている」。

あなたが知るべきこと

個人データの暗号化は、GDPRやその他のデータ保護とサイバー・セキュリティの規制が発効する中で最も重要だ。ジエネテック社デビ氏氏は、暗号化、適切なファームウェア、機器の認証、ユーザの認証などは別として、データのエンド・ツー・エンドのセキュリティを確保するための手順について詳述している。

リム氏は、映像監視業界はまだ学習中で、GDPRに準拠する方法を欧州で展開する際に解決策を見つけることを試みているようだとしている。そして、次のように続ける。

「しかし、現在明らかになっていることの1つは、あらゆる展開の目的で正当化される必要があり、GDPRは、映像を取得し、必要に応じて映像を消去するよう要求することに関して、ユーザに対してより多くの力を与えている。全ての映像監視担当者はこの新しい要求に従う必要があり、映像監視ソリューション・プロバイダは、プライバシー・マスキング、映像の安全な消去などの前進する要件をサポートし、対応するために機能を見直す必要がある」。

最終的に、シードルフ氏が指摘したように、GDPRに関連する映像監視データは、生体認証技術を利用した解析によって生成されたものとなる。これに同意するヒューズ氏は、今日、多くのソフトウェア・ソリューションが、年齢、性別、体重、体重を正確



に特定し、既知の犯罪者や容疑者の顔の特徴を特定できることを付け加えている。

ストレージの保全化の開始

このように、システム構築者はインストールが生成するデータが保護されていることを覚えておく必要がある。このセキュリティは、ハードウェア・ベースの暗号化技術を利用できるHDDから始まり、安全なサプライチェーンを通じて製造され、安全なデータリタイアオプションを提供し、セキュリティ評価基準(Common Criteria Certification)などの認定された国際規格に準拠している。

GDPRとシステム構築者

GDPRが効力を発揮するにつれて、システム構築者には、顧客が監視データ漏洩に脆弱でないことを確実にする責任が増大するだろう。

シーゲイト・テクノロジー社ブランドン・グレッグ氏は、暗号化はこの点で重要な鍵となると指摘する。映像に記録されている顧客や人々は、自分の画像、顔の詳細、時間と場所を間違った人々と共有したくないだろう。他の業界の専門家は、監視データのセキュリティとGDPRの重要性は、潜在的に顧客とのSIの役割に影響を及ぼすことを示している。

セキュア・ロジック社営業部長ロビン・ヒューズ氏は次のように述べている。「映像監視は常に犯罪を検出して解決するための有効なツールとなり、IP分野でしっかりと定着している。システム構築者とIT責任者の関係はこれまで以上に緊密になり、先進的なCCTV企業の機能ではサイバー・セキュリティのスキルが高くなるはずだ。そして製品セットの一部製品を紹介するのに役立つメーカーを探すべきだ」。



監視カメラ用SDカードの選択



監視カメラ用最良のSDカードを選択することは、映像監視ソリューションにおいて信頼性を確保するための重要な要素だ。エッジストレージとしての監視カメラを最優先ストレージ製品にすることで、SDカードに求めることが見えてくる。

●エイフェ・ストロム、フリー記者

エッジ・ストレージとしての監視カメラは、より柔軟で手頃な監視ソリューションの構築を実現している。しかし、過去にエッジ・ストレージの信頼性が疑問視されていた。これらの懸念の大きな部分は、一般用途向けSDカードの能力不足によるものだった。その結果、監視カメラ向けの適切なセキュアのデジタル・メモ리카ード(SDカード)を効果的な監視ソリューションの重要な要素として選択した。映像データの保存と書き込みに適したSDまたはmicroSDカードがないと、監視システムの信頼性が著しく低下する可能性がある。

パーシステンス・マーケット・リサーチ社の報告書によると、SDカードの世界市場規模は2022年までに89億米ドル超になると予測されている。NAND技術の進歩により、SDメモ리카ードのアプリケーションが進歩することが期待されている。これらの進歩は、メーカーが映像監視の要望に適したSDカードを開発する上でも役立っている。筆者は、有力なSDカード・メーカー監視カメラ用の優れたSDカードの製造について尋ねた。

監視カメラの必要性

他のタイプのカメラと異なり、監視カメラには様々なストレージ要件がある。監視カメラが導入されている数多くの環境や、24時間365日連続でデータを書き込む必要性など、監視カメラでは一般用途のSDカードよりもさらに何かが必要だ。

「今日市販されている大部分のmicroSDカードは、デジタル・スチル・カメラ(DSC)、車載カメラ、家庭用カメラなど消費者向けに設計されている。IP映像監視カメラの産業用に設計されたものではない」とマイクロン・テクノロジー社セグメント・マーケティング上級責任者ジョーイ・リン氏は説明している。その結果、エッジ・ストレージは、多くのシステム構築者や設置業者から「信頼できない」と看做されている。

ユーザの大半は、エッジ記録に使用されるSDカードの寿命と品質が、選択したカードの品質で大きく異なることを理解していない。そのため、品質を誤ってSDカードを選択すると、設置から数ヶ月以内にコストがかかるフィールド障害が発生する可能性がある。

リン氏は、「最近よくある間違いは、映像監視システムで一

般用途向けmicroSDカードを使用することだ。一般用途向け64GBカードは、連続した8 Mbpsのビットレートで、典型的な映像監視システムですぐに消耗してしまう。一般用途向けmicroSDカードに記録する場合、1日12時間以上では、数ヶ月の使用で障害が発生する可能性が高い」と語っている。

同氏は現在、市場で入手できるSDカードの主な違いとして、カードに使用されているNANDフラッシュ技術、どのようにファームウェアが24時間365日の映像録画に最適化されているか、NANDがどのようにテストされ、スクリーニングされ、全体的な製品の信頼性が向上するかを示している。

監視カメラの記録保存要件を満たすには耐久性が高く、環境上の危険を伴うカード、例えば温度や湿度を確認して選択することを推奨する。監視カメラは気象条件を問わず24時間365日を記録することができ、持続的な性能維持と失敗に危険性があるため、間違いなく記録できるカードが必要だ。つまりSDカードを正しく選択することが重要だ」とキングストーン・デジタル社 EMEA地域技術サービス・マーケティング担当部長ロバート・アレン氏は述べている。

もう一つの重要な仕様は、監視カメラの録画解像度とフレーム・レート(fps)だ。SDカードのデータ転送速度がカメラの要求と一致しない場合、記録に影響を及ぼす。監視カメラのエッジ・ストレージと他のカメラとの最大の違いの1つは、エッジ・ストレージ機器への負荷が大きいことだ。監視カメラは、24時間365日の高品質映像録画の要求を満たすために、高い耐久性と記録性能を必要としている。

「耐久性の観点からは、IPカメラのエッジ記録はメモリの最も大きな負荷の1つであり、一般用途向けmicroSDカードですぐに



“映像データの保存と書き込みに適したSD/microSDカードがなければ、監視システムの信頼性は非常に低下する可能性がある。”

消耗させることになる。カードを交換するまで映像記録は保管できない。24時間365日連続録画が必要なアプリケーションでは、全てのフレームが記録されることを保証するために、ファームウェアを最小定常状態のパフォーマンスをサポートするように調整する必要がある。

課題の克服

2017年にマイクロン社とウェスタン・デジタル社そしてサムスン社は、監視カメラの要求の高まりに応えるため、特にセキュリティ監視用途で監視等級のメモ리카ードを開発した。一般用途向けSDカードとは異なり、天候(-25°Cから85度°Cまで)、最長2年から3年の連続記録に耐えられるように、監視機能を備え



キングストン・デジタル社
EMEA地域マーケティング&
技術サービス部長
ロバート・アレン氏



マイクロン・テクノロジー社
セグメント・マーケティング
上級責任者
ジョーイ・リン氏

たSDカードが開発されている。

これらのカードは、製造元により32GB~128GBの記憶容量がある。これらの仕様は全て24時間365日のビデオ監視の要求を満たすものだ。

マイクロン社は2017年、超高密度の監視等級のエッジ・ストレージ・ソリューションを発表した。

このソリューションは、64層のMicron 3D TLC NAND技術を

エッジ・ストレージ・ソリューションで考慮すべき4つの項目

マイクロン・テクノロジー社セグメント・マーケティング上級責任者ジョーイ・リン氏は、監視カメラ用のエッジ・ストレージ・ソリューションにおいて考慮すべき4つの点を挙げた。

監視カメラ用エッジ・ストレージは、バックアップ・ソリューションからプライマリ・ストレージとして使用するよう進化してきた。しかし、右端のストレージ・ソリューションを選択することには困難が伴う。リン氏は、ソリューションを選択する際に考慮すべき点を以下に概説しました。

- 1. サービス・レベル・アグリーメント(SLA)・システム構築者(SI)またはシステム設計者にとっての最初の考慮事項は、サービス契約または契約期間が終了することが保証されている製品から選択することだ。これは環境や用途により変動するが、通常3年以上の保証となる。トラック・ローリングを招くことは少なく、現場でカードを交換するには非常に高い費用がかかる。**
- 2. 記憶容量**・第2の考慮点は、十分な映像保存記録を提供するカード容量を選択することだ。エッジ・ストレージ・ソリューションでは、選択した圧縮手法を使用して、目標解像度で映像保存記録を最大2週間あるいは1か月間保存できるかだ。

現在の映像監視業界では、1080pの解像度はIPカメラの基本要件であり、今後は4Kへと移行するだろう。高品

質の監視映像を継続的に記録することで、基本的なデータ・ストレージと保存記録要件を満たす高密度のストレージ機器が必要になる。



- 3. パフォーマンスの記録**・第3の検討事項は、データ品質のためにSLAを満たすことができるエッジ・ストレージ・ソリューションを選択することだ。

ストレージ機器への連続映像録画は、フレーム・ドロップの問題を引き起こす可能性がある。エッジ・ストレージ機器は、データ損失のリスクを低減するために監視使用のために記録パフォーマンスを最適化する必要がある。

- 4. 状態モニタリング**・第4の考慮事項は、カードの寿命状況を報告できるエッジ・ストレージ・ソリューションを選択することだ。カードがその製品寿命を使い切ると、カードが正常に動作しない間にシステム障害(記録停止)またはデータ損失の危険性が生じる。リスクを最小限に抑え、点検保守費用をさらに削減するために、エッジ・ストレージ・ソリューションには状態モニタリング機能が搭載されている必要がある。

“セキュリティカメラは、高耐久性と1週間24時間連続で高品質の映像録画の要求を満たすための録画性能を必要とする。”

ベースにしている。「新しくリリースされた高密度メモリ機器は、より小さなスペースでより大きな容量を可能にし、より効率的な電力使用を可能にし、カメラ自体に依存して最大30日間の監視映像記録を可能にするビットレートを有している」とリン氏は説明している。

マイクロン社の監視用等級のmicroSDカードの他の機能として、200万時間のMTTF(mean-time-to-failure)、または0.44%の年間故障率(AFR)があり、これはほとんどの監視用HDDと同等またはそれ以上だ。さらにフレーム・ドロップを最小限に抑える連続映像録画用に設計された特別なファームウェアを搭載している。これにより技術情報を自己監視し、利用情報と予想される耐用年数を提供している。

ウェスタン・デジタル社やサムスン社も、監視等級のSDカードを開発している。ウェスタン・デジタル社製紫色のmicroSDカードは、特に監視カメラ用に作られている。2018年初頭、サ



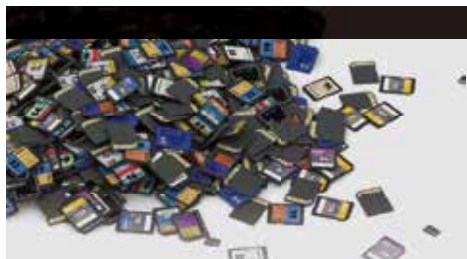
監視等級のSDカードは、最高2~3年にわたり極端な温度や連続記録に耐えることができる。

ムスン・エレクトロニクス社は、最大43,000時間の連続録画を誇るPRO Endurance microSDカードを発表した。

更なるメモリカードの品質向上

映像監視の必要性が高まるにつれて、SDカード・メーカーは、監視等級のメモリカードの必要性に対応する必要がある。

カメラの解像度は向上し続ける一方で、高いセキュリティレベルを保証するには、このような高解像度と重いデータフローを処理できるSDカードが必要になる。



SDとSDHCの違いとSDXCの違い

SDカードは全てを「SDカード」と呼ぶが、SDカードの種類には大きな違いがある。ここではそれらの違いを簡単に説明する。

全てのSDカードが同一になるわけではなく、全てのSDカードが交換可能ではない。カード全般を全てSDカードと呼んでいるが、Secure Digital(SD)、SD High Capacity(SDHC)、SD Extended Capacity(SDXC)メモリカードには大きな違いがある。

今や一般用途向けSDカードが監視カメラには十分であるとは考えられていない。通常の一般用途向けSDカードがSD、

SDHC、SDXCカード全てをサポートするという考えは、混乱を招く可能性がある。

現在、マイクロン・テクノロジー社、サムスン・エレクトロニクス社、ウェスタン・デジタル社が製造している監視用途のSDカードは、最小容量が32 GBのSDHCカード、64 GBと128 GBの容量のSDXCカードだ。下記に3種類のカードの基本を比較している。

カード種別	ストレージ容量	既存フォーマットの互換性
SD	128MBから2GBまで	FAT16・ SD、SDHC、SDXCのいずれか
SDHC	4GBから32GBまで	FAT32・ SDカード対応機器との互換性なし。 2008年以降の主要機器にはSDHCと互換性あり。
SDXC	64GBから2TBまで	exFAT・ SD/SDHCカード対応機器との互換性なし。 2010年以降の主要機器にはSDXCと互換性あり。

(情報提供: サンディスク社)

ショッピング街の 安全を確保する上で 不可欠な統合とは

近年の幾つかの出来事は、店舗街での堅牢な安全対策の重要性を象徴している。

本稿では、店舗街でのセキュリティの要件と、それを保証するための統合ソリューションの必要性を探る。

●バラサンス・アビィ・トーマス フリー記者

2017年7月、米国ニューオーリンズでショッピング街の外で2人が発砲して3人が死亡し、7人が怪我をした。地元報道によると、長銃と拳銃で武装した襲撃者は群衆に無差別に発砲した。同月、テキサス州のある店舗街では盗難未遂が発生した。そして8月後半には、ナイフを持った万引犯がフロリダのあるショッピング街で買物客を恐怖状況に陥れた。

これらは、ショッピング街での安全対策の重要性を具現化した事件だ。この問題は、米国や特定地域に限定したものではないということだ。繁華街では毎日多くの人々が訪れ、資産価値が高い状況を考慮すると、平常の活動を確実にするためには堅牢なセキュリティ・システムが必要だ。

IDIS米国社営業&マーケティング上級部長キース・ドルモンド氏によると、米国のショッピング街にとって最大の脅威は、テロ攻撃や頻発する銃撃だ。公共の場での銃撃回数が増えている。店舗街は他の集会場と同様に、テロ攻撃の恰好の対象と考える必要がある。

ヘルタ・セキュリティ社CMOローラ・ブランク・ペドレガル氏は、テロの脅威を強調した。彼女は、多くのショッピング街はテロ攻撃に対して脆弱だと指摘しているが、店舗スタッフが常に万引に対処しなければならないという問題もある。セキュリティ・ソリューションを個別で利用しているだけでは何の役にも立たない。さらに、日常的に注意しなければならない懸念がある。

「ほとんど全てのショッピング街に共通するもう一つのセキュリティ上の問題は、窃盗や強盗などのいわゆる『よくある犯罪』だ」とペドレガル氏は語っている。「これらの犯罪は人に怪我を負わせることは無いが、店舗経営者に直接の脅威となる収益の損失をもたらし、別の損失も引き起こす。これらの犯罪は回避する上で役に立つ適切なセキュリティ・ソリューションがないため、相変わらず発生している。つまり映像監視カメラや警備員だけでは不十分だ。監視カメラが正しく設定されていないことや、警備員が監視によって欺かれることがある。これは、泥棒が数週間から数カ月間も前から事前に下調べを行い準備している。

CAUTION CRIME SCENE DO NOT ENTER

ショッピング街の脆弱性の克服

アリコント・ヴィジョン・コスター社マーケティング担当副社長ジェフ・ホイットニー氏によると、ショッピング街には、コンコースやアトリウム、駐車場や建造物、緑地や積み込み用基地などの大型オープン・スペースと、複数のアクセス・ポイントがある。

「残念なことに、これらの有益な場所のショッピング街が犯罪活動拠点となり、従業員による株式売買から詐欺への転落、詐欺行為や組織犯罪、強盗や暴行に至る可能性がある。極端な事例では、ショッピング街が活発な銃撃や爆弾の脅威などで、テロの潜在的な標的になる可能性がある。

確かに、それは最も危険と接しているショッピング街の特徴でもある。ハンファ・テックウィン欧州社事業開発責任者ウッドゲイト・リン氏は、ショッピング街は多くの出入口があり簡単に入退出することができるように設計されていると語っている。そのため、混雑した環境が最大限の被害を受ける可能性のあるテロリストの対象となりやすい。経済的不安が高まると他のリスクも発生してくる。

同氏はまた、「厳しい経済環境の中で、ショッピング街のテナントは、組織化された犯罪集団による窃盗の増加に備える必要がある。また、アルコールや薬物乱用者による反社会的行動の発生は、ショッピング街にとって絶え間ない課題だ」と指摘している。

Hikvisionデジタル・テクノロジー社個別ソリューション責任者フェン・ツァイ氏は別の問題点を挙げている。ショッピング街の広い領域を考えると、かなりの電力を消費し、引火性物質により資産の喪失や人身傷害につながる懸念のある火災発生の危険度が高い。もちろん、これらはより幅広いビジネス状況で観測する必要がある。

IDIS欧州社上級技術主任ビリー・ホプキンス氏によると、全ての小売業がオンライン競争と消費者の習慣の変化から圧力を受けている。同氏は続けて、「結果的に、彼らは競争に勝ち抜いて顧客を獲得する新しい方法を見つけようと努力している。ショッピング街は進化しており、多くはレジャー目的の役割も担い、ショッピング街での娯楽性などの顧客体験を提供している。このような背景から、セキュリティと安全性はますます重要になっている」と話している。

ショッピング街はどのように緊急事態に対処するか

ショッピング街のセキュリティ部門は、損失防止からコンコースや駐車場の構造、その他の公共区域の監督に至るまで、一般的に小売セキュリティの課題を担当してきた。しかし、近年では火災や攻撃的な銃撃、武装強盗やテロリスト問題などの緊急



Hikvisionデジタル・テクノロジー社
個別ソリューション責任者
フェン・ツァイ氏



IDIS米国社
営業&マーケティング上級部長
キース・ドルモンド氏

事態への対応が含まれている。

ホイットニー氏は、緊急事態への対応を強化し、顧客や店舗街の労働者の安全を確実にするためには、セキュリティの可視化が重要だと述べている。これには、出入口や公共区域での一目で分かる制服着用の警備員数の増加や、その同一場所に存在を目立たせた監視カメラの増設などが含まれている。どちら



“建物が美観として評価される必要があるため、これがセキュリティ・システムの設計上での障害となることがある。”

もセキュリティ効果と顧客やテナントの快適さを高める。他の地域での慎重な監視は全体を俯瞰するように配置されて、状況認識を高めるのに役に立つ。公衆と従業員の許可なしに移動できる場所を制限するアクセス・コントロールの改善も助けになると指摘している。

同氏は、経験豊富なセキュリティ・コンサルタントを雇い、施設とそのセキュリティ計画を見直すことが改善の第一歩と挙げている。地方の法執行機関、消防署、地元の救急車のサービスを活用して、緊急時および災害時の計画を更新し、事故発生時に双方向の通信が確実に行われるようにすることも重要だと付け加えている。

しかし、特定のセキュリティ管理システムを導入しているにもかかわらず、ショッピング街に非常事態に対処するための技術的能力が不足している可能性があるという。例えば、映像監視、警報、アクセス・コントロール、火災制御の分散サブシステムを1つの監視センターに統合し、緊急コマンドの統一された管理システムを確立する必要がある。テナント側には、もはや互いに独立して動作するセキュリティ・ソリューションを持つ余裕はない。

統合ソリューションの重要性

ショッピング街に統合されたセキュリティ・ソリューションが必要であることは間違いないが、実装する際に考慮すべき幾つかの要素がある。ボッシュ・セキュリティ&セーフティ・システムズ社個別市場担当部長ダン・リーズ氏によると、小売セキュリティ戦略では、損失防止、物理的セキュリティ、資産保護、リスク管理、ITなどの要素を考慮する必要がある。

「既存のセキュリティ基盤を評価し、将来の計画を策定すると、責任チームは次の質問を考慮する必要がある」とリード氏は述べている。「より安全な店舗がありますか? 人員の効率と買物客の安全性を向上させるための通知やその他の技術はありますか? セキュリティ技術によって集められたデータの恩恵を受けることができる組織内の他の部門はありますか?」

店舗内の現在の不備な点を理解し、統合されたセキュリティ・ソリューションがどのようにこれらの問題に対処できるかを理解することが、最良のソリューションを実装する鍵だ。典型的な小売店の中には、POS端末、デジタル・サイネージ、銀行ATM、



ヘンス・セキュリティ社CMO
ローラ・ブランク・ペドレガル氏



ボッシュ・セキュリティ&セーフティ・システムズ社
個別市場担当部長ダン・リーズ氏

出入用ドア、空調機、冷凍庫などの統合ソリューションの力を簡単に実証する「ホットスポット」が幾つも存在する。

ホプキンス氏は、顔認識や高度解析などの他のソリューションにも統合を盛り込むと付け加えた。予防は治療より優れており、顔認識技術は罪を犯す機会を得る前に、出入りを禁止された人物の検出を可能にすると述べている。先進の解析エンジンは、迷子の身に着けている衣服で検索するなど、重要な課題にも役に立つ。

ヘンス・セキュリティ社CMOローラ・ブランク・ペドレガル氏は、この技術は主に小売業界における盗難防止に使用されていると述べている。続けて「この種の犯罪は、通常犯罪を何度も繰り返している人々と同じだということが特徴だ。そのため、最も脆弱な場所でこの種の被験者を識別することができるシステムを自由に使い分けることは、頻繁な盗難を避けるためには根本的なものになる」と述べている。



カメラからのデータはクラウド内のアルゴリズムにより処理され、店舗経営者が商品陳列と店舗レイアウトの成功を評価するのに役に立て、顧客の動線に関する情報を提供することができる。

反復犯罪者の顔のデータベースの存在は、この問題を解決するのに有効だ。

セキュリティを超えた統合

ほとんどのセキュリティ専門家が今認識しているように、解析の目的はセキュリティのみに限定されない。ペドレガル氏は、特定の事業における顧客の類型の特定に関心が高まっていると指摘している。顔認識機能を持つシステムは、訪問者の顔の分析を可能にし、習慣的なクライアントの経歴や他の関連統計を確立することを可能にする人数統計データを提供する。

小売業者は、カメラからのメタデータを使用して、入店人数などのビジネス統計を収集することもできる。リーズ氏によると、このデータは、人材配置に関する意思決定のピーク日時を理解する上で役に立つ。

「精算場所の監視を提供していれば、精算待ち人数が予め定義した閾値を超えた場合に、カメラの映像解析を使用してアラートをトリガーすることもできる。現時点では、ショッピング体験を強化するためにBGMを演奏するのに使用された同じパブリック・アドレス・システムとスピーカーを起動して、別のキャッシュ・



アリセント・ヴィジョン・コスター社
マーケティング担当副社長
ジェフ・ホイットニー氏



ハンファ・テックウィン欧州社
事業開発責任者
ウッドゲイト・リン氏

レジスタを開くようにメッセージを送信し、店舗運営を改善することができる」。

カメラによって生成されたメタデータは、クラウド内の洗練されたアルゴリズムで処理されるため、買物客の店内を移動する際の動線軌跡や歩行と停止が分かり、また個々の買物客のプライバシーを保護する。この情報は、マーケティング担当者が、顧客の関与と販売に直接影響を及ぼす陳列と店舗レイアウトの成功を評価するために使用できます。

ショッピング街用の理想的なシステム設計

IDIS米国社営業&マーケティングシニ上級部長キース・ドルモンド氏によれば、映像監視ソリューションとアクセス・コントロール・システムの統合が、ショッピング街にとって理想的なセキュリティ・システムを設計するための第一歩だと言う。

「コンサルタントおよびシステム構築者によるサイト調査要件はユニークではなく、多くのセキュリティ・アプリケーションに利用されているが、ショッピング店舗街にとっては不可欠な資源だ。そしてショッピング街のセキュリティシステムを設計することは非常に困難だ。サイトの歩みと建築図は、顧客のために最も安全な環境を作り出すための鍵だ」とドルモンド氏は述べている。

ヘルタ・セキュリティ社CMOローラ・ブランク・ペドレガル氏は、実際に分析されている全ての情報をコンパイルするために、高品質なVMSであるイメージストリームを有効にする高品質のカメラを使用して、ショッピング街の理想的なセキュリティ・システムを構築すべきだと提案している。ブラックリストに記載された人物が構内や屋外で検出されるたびに瞬間的な警報を送信する顔認識システムなどがある。

IDIS欧州社技術上級責任者ビリー・ホプキンス氏は、技術的側面についてさらに詳しく説明している。システムは管制室の運用を中心に設計し、必要な全ての情報供給を一元管理する必要があると述べている。人工知能(AI)のような技術は、既に情報の評価と提

供には優れたツールだが、最終的には電話をかける必要がある経験豊かで直感的な専門家と置き換えることはできない。

これは、人々の生活が危険にさらされている場合に特に当てはまる。ショッピング街は運営上の違いがあり、コンサルタントや経験豊富なSIの現地の専門知識と知識が極めて重要だ。

ホプキンス氏は「理想的なセキュリティ・システムは、到着の瞬間からの訪問者の肯定的な体験を確実にするように設計する必要がある。例えば、ALPR技術を駆使して、駐車場の合理化と秩序あるサービスが可能になる。技術的な機能のチェックリストから始めて、それらをどうするかを決めるのではなく、常にユーザの利便性と積極的な経験則を重視したこのアプローチが出発点になるはずだ」と述べている。

ショッピング街ではロボットとドローンを実験しようとしています。これははまだ広く採用されていない。ナイトスコープ社は、その拡大を制限する可能性のあるいくつかの挫折にもかかわらず、最前線企業だ。おそらく、人が自律走行するのに慣れるまでには時間がかかるが、セキュリティの面では効果的な選択肢となる。

ショッピング街でのシステム統合事業

システム構築者は、ショッピング街にセキュリティ・ソリューションを提供する際に様々な課題に直面している。大部分は、これは導入側の事業している市場に依存している。

ツアイ氏は、既存のアナログ監視システムをIPベースのシステムに切り替える時に、全ての機器とデータを一元管理する分散システムに統合するという大きな障壁があると指摘している。

「ソリューション供給業者とエンドユーザ間の中心的役割として、システム構築者と設置業者は、エンドユーザに集中管理の重要性と、操作と応答効率そしてサイト・セキュリティを向上させることを、ソリューション供給業者とともに実施することの重要性を教える必要がある」とツアイ氏は付け加える。

ドルモンド氏の意見では、ショッピング街用システムを設計する上での最大の課題はアーキテクチャだと言う。多くの場合、これらの建物は美観的に満足できるように設計されており、それにより隠れ場所が生じ、コンサルタントやシステム構築者はこれに対応したセキュリティ・システムを設計することが難しいと言う。

ホブキンスも、アナログからデジタルシステムへの移行の難しさを強調し、シンプルでユーザ・フレンドリなフロント・エンドを提供することは難しいと付け加えている。

「カメラから送信そして業種用ソフトウェアまで、全ての構成

“ショッピング街は移動が容易で、客寄せができるように設計されており、混雑した環境で最大限の被害を受ける可能性のあるテロリストの標的になっている。”



機器が完全に調和して動作することが保証された、エンド・ツー・エンドの製造ソリューションを使用する明確な事例がある。重要なことは、最高のエンド・ツー・エンド・ソリューションは、サードパーティの専門家による統合が、大規模な小売環境の様々な脅威や要件に対応できることだ。

顔認識のようなソリューションを実装する場合、セキュリティ担当者のために適切な知識が不足していることも、システム構築者の課題になるとペドレガル氏は述べている。これに対する解決策はもちろん、適切な技術の訓練と意識向上だ。

確実なセキュリティの確保

世界中で安全性に対する懸念が高まるにつれ、セキュリティ・ソリューションはもはや必要悪とはみなされない。ショッピング街のような商業用サイトは、積極的なショッピングとエンターテインメントの経験を維持しつつ、セキュリティを強化することによりますます関心を集めている。

監視カメラ、防火システム、アクセス・コントロールなどの機器を統一する統合ソリューションは、店舗街で最高のセキュリティを確保するための鍵となる。これらは、自律的なマシンのような新しいソリューションと共に、買物客に不便を与えることなく、より厳しいセキュリティのための道を開くことができる。しかし、これに決定打はなく、適切な技術を組み合わせることが最善の方法だ。



国土交通省、無人航空機（ドローン・ラジコン機等）の飛行ルールの周知を強化

近年特にドローンの普及に伴い、様々なトラブルや事故が発生している。これを受けて国土交通省航空局では、無人航空機（ドローン・ラジコン機等）に関する法規制を広く周知することを強化している。セキュリティ産業従事者は、下記の規定を遵守することが求められている。

1. 航空法における無人航空機

1-1. 無人航空機の定義

「人が乗ることができない飛行機、回転翼航空機、滑空機、飛行船であって、遠隔操作又は自動操縦により飛行させることができるもの」と定義されており、いわゆるドローン（マルチコプター）、ラジコン機、農薬散布用ヘリコプター等が該当する。ただし、マルチコプターやラジコン機等であっても、重量（機体本体の重量とバッテリーの重量の合計）200グラム未満のものは、無人航空機ではなく「模型航空機」に分類される。

また、航空機から改造されたもの等、無人機であっても航空機に近い構造、性能・能力を有している場合、航空法上の航空機に該当する可能性がある。そのような場合には個別に相談する。

1-2. 模型航空機の定義

ゴム動力模型機、重量（機体本体の重量とバッテリーの重量の合計）200グラム未満のマルチコプター・ラジコン機等は航空法上「模型航空機」として扱われ、無人航空機の飛行に関するルールは適用されず、空港周辺や一定の高度以上の飛行について国土交通大臣の許可等を必要とする規定（第99条の2）のみが適用される。

2. 無人航空機の飛行ルールに関する航空法の規定

2-1. 飛行の禁止空域

有人の航空機に衝突するおそれや、落下した場合に地上の人などに危害を及ぼすおそれが高い空域として、以下の空域で無人航空機を飛行させることは、原則として禁止されている。これらの空域で無人航空機を飛行させようとする場合には、安全面の措置をした上で、国土交通大臣の許可を受ける必要がある。ただし、屋内で飛行させる場合は不要。

なお、自身の私有地であっても、以下の(A)～(C)の空域に該当する場合には、国土交通大臣の許可を受ける必要がある。

(A) 地表又は水面から150m以上の高さの空域

(B) 空港等周辺の空域

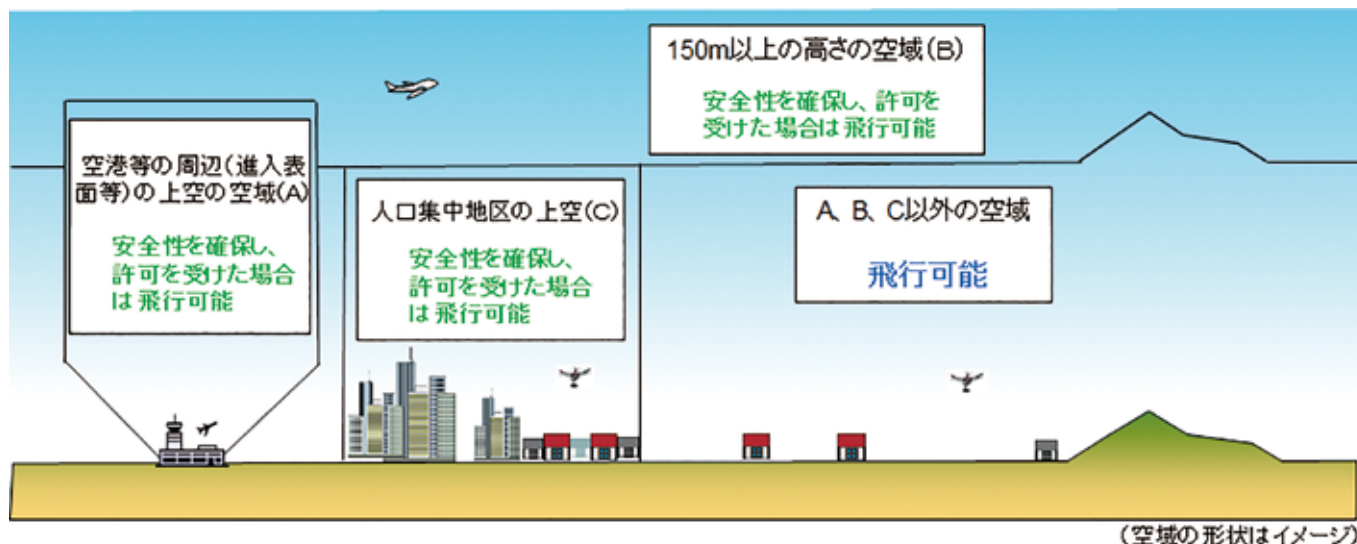
空港等の周辺の空域は、空港やヘリポート等の周辺に設定されている進入表面、転移表面若しくは水平表面または延長進入表面、円錐表面若しくは外側水平表面の上空の空域。

また、実際に飛行させたい場所が「空港等の周辺の空域」に該当するか否かは、以下を利用して確認する。

○ 進入表面等の設定状況（広域図・詳細図）

○ 国土地理院「地理院地図」

(i) 全ての空港やヘリポート等における進入表面等の例





(夜間飛行)



(目視外飛行)



(30m未満の飛行)



(イベント上空飛行)



(危険物輸送)



(物件投下)

全ての空港やヘリポート等において、空港等から概ね6km以内の範囲で進入表面、転移表面および水平表面が別途設定されている。

(ii) 東京・成田・中部・関西国際空港及び政令空港における進入表面等の例

東京・成田・中部・関西国際空港及び政令空港においては、(i)の表面(進入表面、転移表面及び水平表面)に加え、空港から24km以内の範囲で延長進入表面、円錐表面及び外側水平表面が設定されている。

(C) 人口集中地区の上空

平成27年の国勢調査の結果による人口集中地区の上空。飛行させたい場所が人口集中地区に該当するか否かは、以下を利用して確認する。

○ 国土地理院「地理院地図」

○ e-Stat 政府統計の総合窓口「地図による小地域分析(j STAT MAP)」

【参考】j STAT MAPによる人口集中地区の確認方法

または以下の航空局HPを通じて確認することができる。

http://www.mlit.go.jp/koku/koku_tk10_000003.html

2-2. 飛行方法

飛行させる場所に関わらず、無人航空機を飛行させる場合には、以下のルールを守ることが必要である。

● 日中(日出から日没まで)に飛行させること

● 目視(直接肉眼による)範囲内で無人航空機とその周囲を常時監視して飛行させること(

目視外飛行の例:FPV(First Person's View)、モニター監視)

● 第三者又は第三者の建物、第三者の車両などの物件との間に距離(30m)を保って飛行させること

● 祭礼、縁日など多数の人が集まる催し場所の上空で飛行させないこと

● 爆発物など危険物を輸送しないこと

● 無人航空機から物を投下しないこと

※承認が必要となる飛行方法

3. 注意事項

無人航空機を安全に飛行させるためには、航空法を遵守することはもちろん、周囲の状況などに応じて、さらに安全への配慮が求められる。具体的には以下の事項にも注意して飛行させる。

3-1. 飛行場所

● 空港等の周辺では、飛行禁止空域が詳細に設定されている。誤って急上昇させるなどにより飛行の禁止空域に飛行させることがないように、原則として空港等の周辺では無人航空機を飛行させない。

● 空港等以外の場所でも、ヘリコプターなどの離着陸が行われる可能性があります。航行中の航空機に衝突する可能性のあ

るようなところでは、無人航空機を飛行させないでください。

- 操縦ミスなどで無人航空機が落下した際に、下に第三者がいれば大きな危害を及ぼすおそれがある。第三者の上空では飛行させない。また、学校、病院等の不特定多数の人が集まる場所の上空では飛行させない。
- 高速道路や新幹線等に、万が一無人航空機が落下したりすると、交通に重大な影響が及び、非常に危険な事態に陥ることも想定される。それらの上空およびその周辺では無人航空機を飛行させない。
- 鉄道車両や自動車等は、トンネル等目視の範囲外から突然高速で現れることがあります。そのため、それらの速度と方向も予期して、常に必要な距離(30m)を保てるよう飛行させる。
- 高圧線、変電所、電波塔及び無線施設等の施設の付近では、電波障害等により操縦不能になることが懸念されるため、十分な距離を保って無人航空機を飛行させる。

3-2. 飛行操作時の注意事項

- アルコール等を摂取した状態では、正常な操縦ができなくなる恐れがあるので、無人航空機を飛行させない。
- 無人航空機は風の影響等を受けやすいことから、飛行前に安全な飛行ができる状態であるか下記事項を確認する。
 - ・安全に飛行できる気象状態であるか
 - ・機体に損傷や故障はないか
 - ・バッテリーの充電や燃料は十分か
- 周辺に障害物のない十分な空間を確保して飛行させるよう心がける。特に無人航空機の飛行速度が出ている際には、法令で定められている距離(30m)以上に余裕を持った距離を人や物件から取る。
- 航空機との接近または衝突を回避するため、航空機を確認した場合には、無人航空機を飛行させない。
- 他の無人航空機との接近または衝突を回避するため、他の無人航空機を確認した場合には、飛行日時、飛行経路、飛行高度等について、他の無人航空機を飛行させる者と調整する。
- 国土交通省から、災害等による被災地周辺での捜索救難機の安全を確保するための飛行自粛等の要請があった際には、無人航空機の不要不急の飛行は控える。
- 無人航空機の種類にもよるが、補助者に周囲の監視等してもらいながら飛行させて、安全確保に注意する。

3-3. 日常での留意事項

- メーカーの取扱説明書に従った定期的な機体の点検・整備の実施
- 飛行中、突風等により操縦が困難になること、または予期せ

ぬ機体故障等が発生する場合がある。このため、不測の事態を想定した操縦練習を行うなど、日頃から技量保持に努める。

- 安全に留意して無人航空機を飛行させても、不測の事態等により人の身体や財産に損害を与えてしまう可能性がある。このような事態に備え、保険に加入しておくことを推奨する。

3-4. 無人航空機による事故等の情報提供

- 万が一、無人航空機の飛行による人の死傷、第三者の物件の損傷、飛行時における機体の紛失もしくは航空機との衝突または接近事案が発生した場合には、国土交通省(空港事務所)への情報提供に協力する。なお、安全に関する情報は、今後の無人航空機に関する制度の検討を行う上で参考となることから、航空法等法令違反の有無にかかわらず、報告する。
- 情報提供の方法は、「無人航空機(ドローン・ラジコン機等)の飛行ルール」掲載している。

http://www.mlit.go.jp/koku/koku_tk10_000003.html

3-5. その他関係法令の遵守等

- 河川(ダムやその貯水池を含む)において、無人航空機を飛行させようとする場合、許可申請が必要な場合や、河川管理者や周辺自治体が河川利用のルールを定めている場合があるので、事前に飛行可能な区域が確認する。詳細は、河川管理者まで問い合わせる。
※国土交通省ホームページ「日本の川」
http://www.mlit.go.jp/river/toukei_chousa/kasen/jiten/nihon_kawa/index.html
- 電波を利用して無人航空機を飛行させる場合、電波法を遵守する。
- 自治体が、その管理する公園等の上空におけるドローンの飛行を禁止していることがある。また、重要文化財を含む神社仏閣等の管理者が、敷地上空での無人航空機の飛行を禁止する看板を掲示している場合もある。土地の所有者等が、その土地の上空での無人航空機の飛行を禁止する旨の表示等を行っている場合には、その土地の上空では無人航空機を飛行させない。第三者の所有する土地の上空で無人航空機を飛行させる場合、所有権の侵害とされる可能性がある。
- 無人航空機を利用して映像を撮影し、インターネット上で公開する場合は、「『ドローン』による撮影映像等のインターネット上での取扱いに係るガイドライン」(総務省)に従って、第三者のプライバシー等に注意する。
- 無人航空機により他人の身体や財産に危害を加えることは、処罰対象になる可能性がある。

出典・http://www.mlit.go.jp/koku/koku_tk10_000003.html





ASISインターナショナル日本支部、 「東京セキュリティカンファレンス2019」の開催を決定

ASISインターナショナルは、セキュリティ専門家を会員とする世界最大のセキュリティ団体で、自らの企業・団体を守るセキュリティ専門家が会員の中核を占めている。そして、ASISインターナショナル日本支部は、ASISインターナショナルの日本を拠点して活動する一般社団法人である。

ASISインターナショナル日本支部はSECURITH SHOW2019において「東京セキュリティカンファレンス2019」を開催することになった。

■本イベントのメインテーマ

「新しいフレームワークESRMとは<副題>～セキュリティはコストではなく重要な経営課題です～」をメインテーマとして掲げ、その具体的な内容は下記の通りである。

- 国内外のリスク・セキュリティ情報の共有
- ESRM(企業セキュリティ・リスク管理)の考え方の紹介
- セキュリティ・マネジャ(企業内セキュリティ管理者)育成の

推進

- 国内外セキュリティ関係者の交流の促進

■企業内セキュリティ管理者の管理業務範囲例

企業により異なるが、管理業務範囲として次のように考えられている。

- 物理セキュリティ(監視カメラ、入退室管理、警備員による警備等)
- 危機管理(自然災害、業務災害、テロ、火災、ストライキ等)
- 雇用前身元調査、インテリジェンス
- 事業継続及びレジリエンス
- 情報資産保護およびサイバー・セキュリティ
- サプライチェーン・リスク・マネジメント
- 法的セキュリティ・コンプライアンス(パワハラ、セクハラ、企業内倫理等)

ASISインターナショナル日本支部

東京セキュリティカンファレンス2019

ASIS TOKYO CONFERENCE 2019

主な講演者



「ASISインターナショナル本部からのメッセージ」

財務担当理事 2020年会長(内定)
ゴッドフリード・ヘンドリックス氏



基調講演 「ESRMの概念および組織にもたらす価値」

元ASIS本部長
エドワルド・エムデ氏



「2020夏のオリンピックに適用可能な過去のセキュリティ事例」

ハイネケン・グローバル・セキュリティ顧問
チャーリー・スレン氏



「ESRMの観点から見た公的機関と民間の協力体制の必要性」

オランダ中央銀行セキュリティ責任者
ベルント・リフ氏



「ESRMと大規模な国際イベント」

ボードルーム@クライシス社長
グレン・ショーン氏

他5名の講師が
登壇する。

開催概要

■日 時

3月4日(月) 19:00~21:00	インターナショナル・ミキサー・ナイト 参加費:8,000円(税込)
3月5日(火) 9:30~17:00	セミナー講演 参加費(税込):5,000円(一般)、1,000円(学生)
3月5日(火) 18:00~19:30	懇親会 参加費:3,000円(税込)
3月6日(水) 10:00~12:00	SECURITH SHOW2019海外参加者向け会場ツアー 参加費無料

- 会 場 東京ビッグサイト会議棟6階605+606(3月5日セミナー講演)
- 対 象 者 企業・官公庁・団体の経営層、総務・経理・人事幹部、セキュリティ・リスク担当、学生
- 定 員 200名
- 主 催 一般社団法人ASISインターナショナル日本支部
- 共 催 日本経済新聞社
- スポンサー HEINEKEN、Chesapeake Strategies Group
- 後 援 日本ファシリティマネジメント協会、日本防犯設備協会、東京都セキュリティ促進協力会、日本ロックセキュリティ協同組合等
- メディア協賛 a&s JAPAN、セキュリティ産業新聞社、セキュリティスペシャリスト協会、日本実務出版
- 使用言語 英語および日本語(同時通訳サービス付き)
- (isc)2 CPE 7ポイント

【問い合わせ先】一般社団法人ASISインターナショナル日本支部
〒221-0022 横浜市神奈川区守屋町3-9-13 TVPビルディング306 TEL:045-450-2131 FAX:045-461-2610

info@asis-japan.org

http://www.asis-japan.org/

VIVOTEK JAPAN、VIVOTEKパートナー・イベント2018を開催

台湾大手の映像監視メーカーVIVOTEK社は、2018年11月9日に東京都港区のヴェルサール田町においてVIVOTEKパートナー・イベント2018を開催した。同社としては日本で初開催となる本イベントには、VIVOTEK日本正規代理店であるグリーン・フラッシュ・ジャパン、システム・ケイ、フォースメディアの3社をはじめ、パートナー企業などから合計約100名が参加した。



イベントの内容は、技術トレーニングVDT(VIVOTEK Discovery Training)および技術トレーニングVTT(VIVOTEK Technical Training)そしてVIVOTEK事業戦略の三部構成だった。

■技術トレーニングVDTの3つのテーマ

1. 監視システム・プロジェクトのデザイン
2. プロジェクトの重要な情報を収集
3. 最適なVIVOTEKのカメラの選択

本セッションでは、プロジェクトの設計の第一歩としてリスクとニーズの評価を挙げ、セキュリティ&リスク調査、情報収集、機能解析、地方法律の確認、防犯のためのビデオ画質の決定要因を解説した。

プロジェクト設計第二歩としてカメラの選択を挙げ、その不可欠な要素として焦点距離、視野角(FOV)、アイリス調整機能による違い、被写界深度(DoF)、解像度とピクセル密度について解説した。さらに、VIVOTEK社独自のカメラのフォームタイプ・ソリューションを紹介した。

本セッションは、映像監視システムを基礎から理解する上で不可欠な情報を盛り込んだ内容だった。

■技術トレーニングVTTの5つのテーマ

1. VIVOTEK IPカメラ構成の最適化

2. 環境に応じて高画質を得る

3. VIVOTEK独自の機能を利用してパフォーマンスを向上させる

4. 帯域幅の計算

5. IP camera Design toolsの使い方

本セッションでは、オフィスおよび交通監視における画像の最適化、帯域幅の計算、VIVOTEK IP Design Toolなどを具体的な例を挙げて解説した。また、本セッションは、VIVOTEK社製品による映像監視システムの設計と構築に関する専門的な情報で構成されており、実務ですぐに役立つ技法や手法を紹介していた。



■VIVOTEK事業戦略

VIVOTEK JAPAN事業部長佐藤稔浩氏が、VIVOTEK JAPAN 2018-2019年の営業戦略と製品情報について説明した。同氏は、VIVOTEK JAPANが2018年11月中旬に株式会社化し、これまで以上に積極的に営業展開することを明らかにした。今後は、テクニカル・サポートをはじめとするスタッフを増強して、日本市場での事業展開を推進する意欲を表明した。

続いてフォースメディア社ビジネス開発部長本田龍氏がVIVOTEK社の注目製品と技術を紹介した。そして、システム・ケイ社がネットワークカメラによる人数カウント・ソリューションについて解説した。

■アワード表彰

VIVOTEK/パートナー・イベント2018には、台湾本社ブランドビジネス部門副社長ウィリアム・クウ氏が来日して、同社の日本

市場に対する高い関心をもった積極的な事業計画を宣言した。

その後、2018年日本市場における事業貢献に寄与した有力企業に対して、VIVOTEK社としてアワード表彰を行い、パーティ懇談会で参加者との親睦を深めた。



GeoVision社、映像監視ソリューション新製品内覧会2018(東京)を開催

デジタル映像監視システム・プロバイダのGeoVision社は2018年11月13日と14日の両日、東京本社において映像監視ソリューション新製品内覧会2018(東京)を開催した。同社は近年、ハードウェア主体の製品提供からワンストップ・ソリューションの提供に比重を移行している。

顔認証技術をベースにした様々なシステムを展示

今回特に力を入れていた技術が様々な顔認識および認証ソリューションだった。例えば、予め登録した顔情報を内蔵しているJVS-AVD01と専用モジュールがあればハンズフリー顔認証アクセス・コントロールが、顔認証用サーバやPC無しで構築することができ、鍵なしで開錠することができる。



さらに上記技術のアプリケーションのうち、出入口の管理における混雑緩和ソリューションでは、最大8名までの顔認証を行なう機能により円滑な入退管理を可能にする。また店舗における顧客対応ソリューションでは、最大10,000名登録の顔情報から顧客情報を認識することができる。

複数のカメラと専用ソフトウェアによる入退室・滞在管理

また、店舗支援ソリューションは、GeoVision社製専用ソフトウェアとネットワークカメラの組み合わせによる構成だ。入口でキャプチャした顔情報を追尾することで退出するまでの滞在情報、性別や推定年齢などの情報をログ化することもできる。さらに、集計



データを活用することで、店舗の効率的な運用を支援する。



汎用性の高いGV-OPAL E1

GV-OPAL E1は、幅広い使い方に対応することができるネットワークカメラだ。Wi-Fi通信/SD録画に対応し、USB給電あるいはバッテリー駆動対応(オプション)により手軽な設置と運用を実現することができる。さらに4-5時間の運用条件であれば充電バッテリーを使用することでコードレス設置も可能となる。モニタリングはスマートフォンやタブレット端末上でカメラ映像を表示、録画再生することができ、インターネット経由での遠隔監視に対応している。



USB給電による設置例

特筆なのが、付属マグネット・スタンドによる取り付けで、これにより誰もが画角調整を簡単にその場で行なうことができる。このようにGV-OPAL E1は簡便性に富んだ映像ソリューションの実現を可能にする。



充電バッテリーによる設置例とマグネット・スタンド(右端)



2018年11月

SECUTECH THAILAND

会期:2018年11月8日～10日

開場:10:00 - 17:00

会場:バンコク国際トレード&展示会場(BITEC)

88 Bangna-Trad Road (Km.1),
Bangna, Bangkok 10260, Thailand

主催:Messe Frankfurt New Era

Business Media Ltd, Taiwan Branch

URL: <https://secutechthailand.tw.messefrankfurt.com/bangkok/en/exhibitors/welcome.html>

本イベントに関するお問い合わせは、
ASJ合同会社までお願いいたします。
TEL・03-6206-0448
E-MAIL・komori@asj-corp.jp

Embedded Technology 2018 /
IoT Technology 2018

会期:2018年11月14日～16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/>

12月

社会インフラテック2018

会期:2018年12月6日～8日

開場:10:00 - 17:00

会場:東京ビックサイト

主催:インフラメンテナンス国民会議、
日本経済新聞社URL: <https://messe.nikkei.co.jp/in/>国際画像機器展2018/ビジュアルメディア
EXPO2018

会期:2018年12月10日～12日

開場:10:00 - 17:00

会場:パシフィコ横浜

主催:アドコム・メディア

URL: <https://www.adcom-media.co.jp/ite/>

2019年1月

CES 2019 (Consumer Electronics Show)

会期:2019年1月8日～11日

会場:Las Vegas Convention and World
Trade Center (LVCC)

米国ネバダ州ラスベガス

主催:the Consumer Technology
Association (CTA)URL: <https://www.ces.tech/>

INTERSEC

会期:2019年1月20日～22日

会場:ドバイ・ワールド・トレード・センター

P.O. Box 9229, Dubai, United

Arab Emirates

アラブ首長国連邦 ドバイ

主催:Messe Frankfurt

URL: <https://www.intersecexpo.com/frankfurt/51/for-exhibitors/for-exhibitors.aspx>

2月

国際ホテル・レストラン・ショー
(HOTERES JAPAN)

会期:2019年2月19日～22日

開場:10:00 - 17:00

会場:東京ビックサイト

主催:日本能率協会/一般社団法人日本
ホテル協会/一般社団法人日本旅
館協会/一般社団法人国際観光日
本レストラン協会/公益社団法人国
際観光施設協会URL: <https://www.jma.or.jp/hcj/>

3月

SECURITY SHOW 2019

会期:2019年3月5日～8日

開場:10:00 - 17:00

会場:東京ビックサイト

主催:日本経済新聞社

URL: <https://messe.nikkei.co.jp/ss/>

リテールテックJAPAN 2019

会期:2019年3月5日～8日

開場:10:00 - 17:00

会場:東京ビックサイト

主催:日本経済新聞社

URL: <https://messe.nikkei.co.jp/rt/>

ライティング・フェア2019

会期:2019年3月5日～8日

開場:10:00 - 17:00

会場:東京ビックサイト

主催:日本経済新聞社

URL: <https://messe.nikkei.co.jp/rt/>

上記3つのイベントへの出展は、
ASJ合同会社も取り扱っております。
TEL・03-6206-0448
E-MAIL・komori@asj-corp.jp

4月

第22回 組込みシステム 開発技術展

会期:2019年4月10日～12日

開場:10:00 - 17:00

会場:東京ビックサイト 西1-4

主催:リードエグジビション ジャパン

URL: <https://www.japan-it.jp/ja-jp/about/ese.html>

ISC WEST

会期:2019年4月10日～12日

開場:10:00 - 17:00

会場:Sands Expo Center

米国ネバダ州ラスベガス

主催:Reed Exhibitions

URL: <http://www.iscwest.com>

5月

SECUTECH

会期:2019年5月8日～10日

会場:台北市南港国際展覽館

〒11568 台北市南港区經貿二路

主催:Messe Frankfurt New Era

Business Media Ltd, Taiwan Branch

(香港商法蘭克福新時代傳媒有限公司 台湾分公司)

8F, No. 288, Sec. 6, Civic Boulevard

Xinyi District, Taipei 110, Taiwan

(〒110 台湾台北市信義区市民大道6路228号8階)

TEL: +886 2 8729 1099

URL: <https://secutech.tw.messefrankfurt.com/taipei/en.html>

本イベントに関するお問い合わせは、
ASJ合同会社までお願いいたします。
TEL・03-6206-0448
E-MAIL・komori@asj-corp.jp

クラウド コンピューティング EXPO【春】

会期:2019年5月8日～10日

開場:10:00 - 17:00

会場:東京ビックサイト 西1-4

主催:リードエグジビション ジャパン

URL: <https://spring.japan-it.jp/ja-jp/about/cloud.html>

データストレージ EXPO

会期:2019年5月8日～10日

開場:10:00 - 17:00

会場:東京ビックサイト 西1-4

主催:リードエグジビション ジャパン

URL: <https://spring.japan-it.jp/ja-jp/about/dse.html>

ネットワーク監視機器を海外からOEM調達する際に確認すべきセキュリティ

今やネットワーク監視機器に日本企業の現状は、海外企業のOEMに頼らなければならない状況に追い込まれている。日本を代表するトップブランド数社もコスト面で対抗できずに、海外大手企業の軍門に下っている。これは、あらゆる分野で見られる減少であるため、OEM調達そのものを単に悲観しても意味は無いだろう。

しかし、米国市場で大きな問題となっているネットワーク機器上の懸念については、調達先の説明するセキュリティ内容を鵜呑みにすることなく、精細に検証することを強く求める。日本のあるブランドは、海外製品をOEM調達しているが、ファームウェアだけは自前のもをを搭載して、セキュリティ面に拝領していると聞く。

OEMを採用している日本企業は、近年よく耳にするバックドアや組み込みOS、それ以外のセキュリティ対策について必ず検証を済ませてから出荷しているのだろうか。さらに、その販売パートナーも、さらに確認をして取り扱っているのだろうか。もちろんパスワード設定も含めたセキュリティに対する取り組みが確立されていることを求めたい。

万が一、ハードウェア上ハッキングされる状態のまま販売し設置した場合、一切の責任の負うという姿勢とその実践を強く求めたい。

(東京 コンサルタント)

企業内セキュリティは物理セキュリティも重要な要素

今やセキュリティという言葉と接しない日がないくらい、セキュリティは社会や企業で不可欠となっている。社会においては、地域の安全確保や犯罪防止の用途で、映像監視カメラの設置が盛んだ。一方企業においては、情報セキュリティが喫緊の課題として認識されている。そして、情報セキュリティとしては外部からのネットワークへの侵入と社内情報の窃取や破壊が主要テーマになっている。

では、企業における物理セキュリティの取り組みを見てみると、まず外部からの侵入防止と発見を最優先して、映像監視と入退管理や各種のアクセス・コントロールなどの運用で対応しているのが一般的ではなかろうか。

しかし、忘れてならないのは企業内部における物理セキュリティの整備だろう。ネットワークからの侵入は履歴を辿ることで把握できると聞かすが、証拠の残ることの少ない内部者によるモノやデータの窃取も真剣に取り組むべきだろう。サーバ室への入室や機密文書の保管などには既にアクセス・コントロールを導入しているが、それ以外のスペースへの出入りやそこでの行為にも細心の注意を払うべきだろう。これは、既にフード・ディフェンスで経験済みだと思う。

(大阪 システム構築者)

「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をご遠慮ください。

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。メーカー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、個人情報や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.jp

secutech

2019年5月8 - 10日 台湾台北市
www.secutech.com

IoT&AIエコ・システムなど、 アジアのセキュリティが 一堂に集まる

7つのスマート・ソリューション展示

- スマート小売、スマート健康管理
- スマート・ホテル、スマート情報交換
- スマート工場、スマート輸送
- スマート駐車

7つのテーマ・ゾーン

1. AI + ソフトウェア・ゾーン
2. RFID応用ゾーン
3. LPWAN応用ゾーン
4. スマート施設ゾーン
5. サイバーセキュリティ・ゾーン
6. 警備設備ゾーン
7. スマート工場 & 産業用安全ゾーン



MOBILITY
powered by Secutech

- インテリジェント輸送システム向けアジアでの主要イベント
- スマート道路、スマート鉄道、スマート駐車から船団の管理まで幅広いソリューションの紹介

SM BIoT SOLUTION
powered by Secutech

- アジア初のスマート・ビルIoT市場分野のイベント
- 住宅、情報交換、介護、看護施設、商業ビルディング向けの代表的なソリューション


fire & safety
powered by Secutech

- 自然災害監視、安全都市、産業安全から個人安全までの様々な代表的なソリューション
- スマートな防災応用事例

info security
powered by Secutech

- IoT向け最新サイバー・セキュリティ・ソリューションの公開

日本での問い合わせ先
ASJ合同会社
TEL : 03-6206-0448
E-mail : komori@asj-corp.jp

 messe frankfurt