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　Sep/Oct. 2020 no.78

特　集：リモートワークでサイバー・セキュリティと物理的セキュリティのリスクを減らす方法

EAGLE EYE NETWORKS

セキュリティカメラシステムの導入時に必要な 10のチェックリスト

☑ 現在使用しているカメラの買い替えが必要ですか?

セキュリティカメラシステム、特にモバイルアクセスやアラートなどのいくつかの先進的な新機能を提供するクラウドシステムには、そのシステム会社の専用カメラを使用しなければならないという但し書きがついている場合が多く見られます。

カメラのハードウェアや配線にはすでに大きなコストがかかります。さらに、既存のカメラを捨てて新しいカメラを購入すれば、コストは簡単に2倍にもなってしまいます。

Eagle Eye Cloud VMSは3000機種以上のIPカメラ、アナログカメラに広く対応しています。

チェックリストの続きはこちらのページよりダウンロードしてお読みください。

お問合せ:
イーグルアイネットワークス株式会社
TEL:03-6868-5527(代表)
Email: APACsales@een.com

www.idisglobal.com

最大98% の精度とパフォーマス
信頼が高いAnalytics

IDIS Deep Learning Analytics (IDLA)

Powered by
IDIS Deep Learning Engine

誤作動による負荷を防ぐことで、コントロールルームに変化をもたらし、セキュリティチームの意識を高め、
チームワークが向上します。強力な検出と認識、そして容易な検証と迅速な調査を可能にします。

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.

SECURE

目　次

広告索引

広告主名（ABC順）	掲載ページ
ASMAG.COM	21
イーグルアイネットワークス	表二
IDIS	1
リテールテックJAPAN 2021	表三
SECURITY SHOW 2021	表四

次号案内　2020年 11/12月号（12月5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

a&s JAPAN ©ASJ合同会社　2020年 9-10月号　No.78
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1-24-21 加瀬ビル8階

■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
E-mail：komori@asj-corp.jp

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。

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。

チリ市、Hikvision社製熱感知カメラを危険に使用

ロバー·レン·ゴードン　著

https://ipvm.com/reports/hikvision-chile-truck

発熱感知カメラを屋外に設置することは明らかに危険だ。それにもかかわらず、チリのある都市では、寄贈されたHikvision社製システムを祝って、コロナウイルスに感染している人を見つけるために街中を稼働させている。

市は根本的に欠陥のある使用方法に依存することでは感染を拡大させる危険があるにもかかわらず、Hikvisionは沈黙している。

本稿は、ラテンアメリカでの欠陥のある発熱カメラの配備に関する記事シリーズの第4回目で、以前の記事については下記をお読みいただきたい。

●**Faulty Hikvision Cali Colombia Fever Camera Implementation**

https://ipvm.com/reports/hikvision-cali

●**Dahua Buenos Aires Bus Screening Violates IEC Standards and Dahua's Own Instructions**

https://ipvm.com/reports/buenos-aires-bus

●**Colombia's President Promotes Bad Hikvision Fever Camera Setup.**

https://ipvm.com/reports/hikvision-colombia-fever

Hanwha社とHikvision社、HEVCライセンスなしでH.265を販売

ザッハ·セガール　著

https://ipvm.com/reports/han-hik-hvec

IPVMは、Hanwha社とHikvision社はH.265製品を4年間販売しているにもかかわらず、HEVC AdvanceのH.265ライセンスを持っていないことを確認した。

本稿では、HEVC Advance、Hanwha社、Hikvision社からの回答を得て、年間数千万ドルのライセンス支払いなどの問題点を検証している。

概要

Avigilon、Axis、Bosch、Dahua、Genetec、Milestoneなどの主要な映像監視企業がHEVC Advance特許のライセンスを契約しているのに対し(HEVCライセンシーリストを参照)、H.265を使用した製品を販売し、MPEGLAプールのH.265特許をライセンスしているにもかかわらず、Hanwha社とHikvision社は契約していない。

IPVMに対して、Hikvisionはコメントを拒否したが、Hanwha社は技術のライセンス化に取り組んでいると語った。

米政府説明責任局、顔認証の規制を要請

ザッハ・セガール　著

https://ipvm.com/reports/gao-face-rec

GAO（米政府説明責任局）は、65ページに及ぶ報告書で顔認証の規制を促している。IPVMは、この報告書を評論および分析し、これを実現するための推奨されている3つの主要なステップを紹介している。

事業計画書の要約

GAOは、商業的な顔認証はオープンで透明性があり、特定の用途に限定され、倫理的に収集された質の高いデータに限定され、最も正確で偏りの少ないアルゴリズムのみで構築され、偏りとデータ保護のためにレビューされるべきであると述べている。同書では、2013年の報告書の勧告である、新しい技術に対処するために議会が消費者保護法を強化することを繰り返し述べている。GAOは7年前にこの勧告を初めて行ったものの効果はなかったが、顔認識とプライバシーは最近炎上しており、今後の規制の可能性が高くなっている。

GAOとは

GAOは、議会が問題を分析するのを支援する米国議会の超党派組織。GAOは議会の番犬と呼ばれている。彼らはしばしば、納税者の税金が効率的に使われていることを確認することを任務としている。

ハネウェル社、Huawei社に警告を発し、将来の防御策を提唱

コーナー・ヒアリィ　著

https://ipvm.com/reports/honeywell-ndaa-huawei

長年、ハネウェル社はDahua社からOEM供給を受けたり、Huawei社製 Hisilicon半導体を使ったりして利益を得てきた。現在、同社は、Huawei社製 Hisilicon半導体を使用した製品がNDAAに違反していると警告し、米国政府が中国に対してさらに強力な行動を取った場合に備えて、将来的な防御策を提唱している。

本稿では、2020年8月28日に開催されたハネウェル社のウェビナーで「NDAA準拠ビデオ・ソリューション」の内容を紹介している。その一部は下記の通り。

- ●NDAAコンプライアンスに向けた当社のこれまでの歩みと今後の取り組み
- ●ブラックリストに載らないようにするためにサプライヤーはどう考えるべきか
- ●NDAA準拠のハネウェル製品

システム構築者はVSaaSで苦しんでいる

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/vsaas-int

VSaaSはこれからもシステム構築者を苦しめるだろう。システム構築者がどれだけ打撃を受けるかは、重要な問題である。

本稿では、システム構築者の役割、その役割が過去20年間でどのように変化してきたか、そして今後5年間でVSaaSがシステム構築者にどのような影響を与えるかを検証する。

英国の裁判所は警察の顔認識に改革が必要と判断

ザッハ・セガール　著

https://ipvm.com/reports/south-wales-pd-lose-face-rec

英国の裁判所は、サウスウェールズ警察の顔認証の使用は違法であるとの判決を下し、同署は簡単に改革できると述べている。しかし、これをきっかけにさらなる訴訟が起こるかもしれない。

今回の判決は、英国の法執行機関による顔認証の使用にとって何を意味するのかを探る。

Verkada社、セキュリティ販売チャネルの破壊について語る

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/verkada-sales-speaks

Verkada社の急成長は業界を席巻しており、業界には「恐竜」が多いと評した同社の企業向け営業責任者ライアン・ヤング氏は、同社がどのようにセキュリティ販売チャネルを破壊してきたのか、貴重な洞察を得たプレゼンテーションを行った。

本稿で下記を検証している。

●Verkada社はAxis社やAvigilon社またBosch社および各社のシステム構築者・パートナーとどのように異なる販売をしているか

●Verkada社で考えている販売とはどういうことか、競合他社との対比は？

●最高の営業組織が重要な理由は？

●カメラを売ることが他のシリコンバレーのスタートアップよりも刺激的な理由は？

●Verkada社営業担当者に求められることは？

●同社の営業研修の内容は？営業担当者はどのように営業開拓するのか？

●同社顧客でシステム構築者を使用していない割合は何%か？

●同社で成功するのは何歳から何歳までか？

●同社が長期的に目指すものとは？

Huawei社製 HiSilicon半導体不足、監視カメラメーカへの影響大

イザベラ・チャン　著

https://ipvm.com/reports/huawei-hisilicon-shortage

Huawei社は、HiSilicon半導体事業の問題点と課題を認め、来月には主力のKirinチップを廃止する。IPVMは、これが映像監視業界にも影響を与えることを多数の中国ハイシリコンの顧客に確認している。本稿では下記の項目について検証している。

●5月の米国エンティティリストの規則改正

●HiSilicon SoCの生産と供給の問題

●これらの制作上の問題がビデオ監視業界にどのような影響を与えるか

●リスクと影響

アクシス社とAvigilon社の特許訴訟、3件の無効特許で終結

ジョエイ・ウォルター　著

キヤノンとアクシスの両社がAvigilon社に対する何年もの複数の特許訴訟が終結し、その過程で3件のAvigilon社の映像解析特許が無効となった。

要旨

キヤノンの支援を受けて、アクシス社はAvigilon社の特許ライセンスに積極的に対抗し、大部分の無効化訴訟に勝利しました。Avigilon社は、映像解析の基本となる ObjectVideo など特許 3 件を維持するための控訴に敗れた。両社は現在、訴訟を終わらせることで合意に達している。

FLIR社CEO、新規参入企業が科学的裏付けの無い主張をしていることを指摘

IPVM Team著

https://ipvm.com/reports/flir-ceo-science

フリアーシステムズ社CEOは、発熱スクリーニング・システムのリスクを訴える声が増えていることに賛同している。

先月、IPVMは、米国と英国、カナダとイスラエルそしてアイルランドの健康専門家が、発熱スクリーニングは効果がないと述べたことを紹介した。

現在、20年近く前からスクリーニング・システムを提供しているフリアーシステムズ社CEOは、新規参入のライバル企業を非難している。

映像監視カメラ用メタレンズの将来
マサチューセツ工科大学、UMass社、Immervision社

ザッハ・セガル　著

https://ipvm.com/reports/mit-flat-wide-metalens

魚眼レンズを使ったパノラミックカメラは、過去10年の間に映像監視では当たり前のものになった。現在、研究者たちは、より薄く、より安価な「メタレンズ」の開発に取り組んでいる。最近では、MIT(マサチューセツ工科大学)が「完全に平らな魚眼レンズ」を発表したことで注目を集めている。

この技術の可能性をより深く理解するために、MITの科学者たちと、現行のパノラマレンズを提供している大手のImmervision社、そしてメタレンズに取り組んでいるヘブライ大学の研究者ヤコブ・エングレベルグ氏に話を聞いた。

概要

MIT/UMASSのチームは、メタレンズと呼ばれる波長よりも薄い回折レンズ（ガラスやプラスチックを介して曲がるのではなく、障害物との衝突によって光が制御される）を使用した。

メタレンズは現在、色の単一の帯域でしか動作しないことから、一緒に可視光の全ての色をキャプチャすることはできず、現在まで監視業界に幅広い影響をもたらす可能性は低い。しかし、メタレンズにはそのような単一のタイプのLEDによって照らされたIRシーンや携帯電話のための深さ知覚などのニッチな用途を持っている可能性がある。

アムネスティ・インターナショナル、アクシス社の中国警察への輸出を批判

IPVM Team　著

https://ipvm.com/reports/axis-prc

アクシス・コミュニケーションズ社をはじめとする EU の監視機器企業は、中国の「無差別大量監視」に貢献しているとアムネスティ・インターナショナルから非難を受けている。

中国の広大な警察ビデオ監視市場は、国内大手のHikvision社とDahua社によって支配されていますが、アクシス社は北京と上海に事業所を構えており、その再販業者が複数の中国の警察プロジェクトに供給していることが、アムネスティ・インターナショナルの新しい報告書で明らかになった。

同報告書は、中国での存在感が小さいアクシス社の場合でも、中国の人権記録が粗悪なため、欧米の監視メーカが中国で事業展開している事実とコンプライアンス上のリスクを紹介している。

アムネスティ報告書

アムネスティ・インターナショナルは、「アウト・オブ・コントロール」と題した報告書を発表し、欧州企業3社による中国への監視技術の販売に焦点を当て、この行為に対する輸出規制を求めた。

URL・・

https://www.amnesty.org/download/Documents/EUR01255620 20ENGLISH.PDF

温度タブレットの競争
Dahua社、Hikvision社、ZKTeco社、TVT社、他5社

デレク・ワード　著

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

温度タブレット端末/ステーションは、2,000ドル以下の低価格発熱カメラの代替品として登場して、同等の競合製品として見られている。

しかし、9種類のタブレット端末のIPVMテストでは、特に広範囲に及ぶ厳格な温度測定に大きな問題があることが示されている。

このレポートの中で、我々はすでに個別にテストした以下のデバイスを撃ち抜きます。

Aratek社製品、Bems社製品、Dahua社製品、Hikvision社製品、Injes社製品、Sperry West/Alibaba社製品、Telpo China製品、TVT社製品、ZKTeco社製体温&マスク検出機器

中国SMIC社への米国の貿易制限の攻撃、映像監視業界に影響

イザベル・チェン　著

https://ipvm.com/reports/smic-restrictions

米国による貿易制限が、中国最大かつ最先端受託製造企業SMIC 社(Semiconductor Manufacturing International Corporation)を直撃した。制限の真の影響はまだわからないが、業界筋はIPVMに、これは中国の半導体産業の発展と映像監視製品の提供にとって大きな危機だと伝えている。

これは、映像監視製品の最大のチップメーカHuawei社HiSilicon半導体に対する米国の影響を受けている。本稿ではIPVMが検証する。

SMICの背景

- 米国の貿易規制で打撃を受けたSMIC社
- SMIC社の計画

SMIC社とHuawei社との関係

- 規制の影響は現時点では不明だが、業界は不安視
- 映像監視業界への潜在的な影響
- 規制に対する市場の反応
- SMIC社の将来は不透明

マイルストーン社製XProtectのAWS版をテスト

ジーン・パットン　著

https://ipvm.com/reports/xprotect-aws-20

マイルストーン社は2020年、ついにAmazonとの提携という方法で複数のクラウド・ソリューションを発表した。XProtectはAmazon AWSで無料のエッセンシャル版プラスのデモと、BYOL(Bring Your Own License：所有しているライセンスの持ち込み)XProtectに提供している。

どのくらいの効果があるのか?AWS上でセットアップとテストを行い、その結果を公開する。

- セットアップは簡単?
- ビデオストリーミングの性能は?
- システムのセキュリティは?
- 費用はどのくらいか?
- Genetec社やAvigilon社のクラウドとの比較は?
- どのような顧客がAWS上のXProtectを検討すべきか?

さらに、その仕組みを7分間のビデオでご紹介する。

Avigilon社製温度上昇検知カメラをテスト

ロブ・キルパトリック　著

https://ipvm.com/reports/avigilon-etd

Avigilon社はH4 温度上昇検知カメラを発表し、温度スクリーニング市場に参入した。ではこれまでに市場に出回っている他の製品と比較してどうか?

ETDカメラ(640S-H4A-THD-BO50)について下記項目について検証した。

- Avigilon社の測定方法は他社と比較してどうか
- 高温のカメラを「叩く/騙す」のがどれだけ簡単か、難しいか
- 帽子、マスク、メガネが温度測定に与える影響
- セットアップと構成が他と比較してどうか

ボッシュ社、皮膚温度検出カメラを発表

ジーン・パットン　著

https://ipvm.com/reports/bosch-temp

製品の詳細は2020年IPVM秋の新製品ショー2020 IPVM Fall New Products showを参照。

製品概要

- 皮膚温度を測定する部位は?
- 他社検温カメラとの比較　●価格

NEC、マスク着用時でも高い精度を実現する顔認証製品を販売開始

NECは、生体認証「Bio-IDiom」の中核技術であり、世界No.1の認証精度を有する顔認証技術を強化し、マスク着用時でも高精度な認証を実現する新たな顔認証エンジンを開発した。また本エンジンを、顔認証や様々な映像分析機能を組み合せて複合的なソリューションを実現する「NEC 映像分析基盤」や、複数の生体情報を活用してマルチモーダル生体認証を実現するサービス「Bio-IDiom Services(バイオイディオム サービシーズ)」などの製品として、販売開始した。

本エンジンを用いた顔認証工程は、まず、カメラで撮影し検出した顔画像からマスク着用の有無を判定する。次に、それぞれの場合で使用する顔認証アルゴリズムを切り替えて、特徴点の抽出と照合を行う。これによりマスク着用者と非着用者が混在しても、高精度な認証を実現する。

本エンジンを用いた社内評価では、マスク着用時の1:1認証での認証率は99.9%以上と、高い認証精度を実現したことを確認した。また様々な色や柄のマスクに対応しており、高い実用性を有している。

低コストでプレミアムなサービスを約束するセキュリティ・ロボット

https://www.asmag.com/showpost/31955.aspx?name=news

セキュリティ・ロボットについては幾つかの懸念事項があるが、その多くは機能、機能、実用性に限定されている。また言及されていないが、人間の警備員を増強したり、代替したりできるロボットを検討する際には、価格が顧客にとって大きな決め手となるということだ。セキュリティ・ロボットに投資費用が人間の警備員を維持するよりも高いのであれば、何の意味もない。

この点は、インドのハイデラバードに拠点を置くロボット新興企業が、asmag.comの取材に応じたH-Bots社創業者兼CEOキッシュハン氏は、自社のロボットをより多くの顧客に利用してもらえるようにすることを目指していると説明した。

ワークスペースでの監視

このロボットは、LiDAR、同時定位、マッピングなどの技術を活用した自律型ナビゲーション・システム上で動作する。これらの技術は、ロボットが機能しなければならない地域の環境を包括的に把握するのに役立つ。また、これらの技術は、ロボットが進むべき道や障害物を特定し、担当者がロボットの位置を特定するのにも役立つ。同社は、全てのロボットをROS（Robotic Operating System）で動作するように製造している。

「当社のセキュリティ・ロボットは、ゲート付きコミュニティや産業用などに設計されている。昼夜を問わず指定区域を動き回りデータを収集し、捕捉することで、経営者は侵入者の有無、産業界の場合は従業員が適切に仕事をしているかどうかを見極めることができる。」

具体的には、製造業などの現場に向けて、H-Botのセキュリティロボットはもう一つの機能を持っている。顔認識機能で従業員の出勤状況を把握できるのだ。顔認識機能は、ロボットに内蔵されたAIを使って動作する。顔認識機能は、ロボットに内蔵のAIを使って動作し、認識できない人を検知した場合には、即座に担当者に警告を出す。これらのロボットに使われているカメラはIntel社製WebカメラReal Sense、マザーボードはNVIDIA製だ。

顧客が魅力を感じるもの

セキュリティ・ロボットに取り組んでいる企業の自律型マシンの多くは、既存のセキュリティ基盤を支援するために、既にモールなどに設置されている。しかし、市場の中で他とは一線を画すようなソリューションを作ることが課題となっている。

「我々の最大の強みはコストだ。世界中の他のロボットと比較しても、当社のモデルは最も経済的だ。例えば、当社の消毒ロボットの価格は約4,770米ドルだ。これは、可能な限り低価格で提供することを第一義としているからだ」とキッシュハン氏は説明する。

同氏によると、H-Botのもう一つの利点は、ロボットの大半が自社製造だという。マザーボードやカメラなどの部品を除い

て、AI、外装、電気部品など、全てハイデラバードにある同社で製造されている。

インドのロボット企業の世界市場での可能性

キッシュハン氏は、今欧州やUAEなどの地域では、インドのロボット企業に対する強い需要があると見ている。しかし、過去にはインド製の品質について懸念があった。

しかし、COVID-19と中国メーカに対する最近の懸念により、顧客に変化が見られる。キッシュハン氏は、顧客が製造協力企業を中国以外に求めるようになり、インド製品への関心が高まっていると述べている。同氏は、海外進出を目指すインドのロボット新興企業は、今後1、2年で高い成功率を得るだろうと予測している。

システム構築者がセキュリティでAIスタートアップから得るものは?

https://www.asmag.com/showpost/31915.aspx?name=news

この記事のために取材した映像解析の新規企業ほとんどは、システム構築者と連携している。実際、SIは彼らの販売チャネルに欠かせない存在だ。これは特に、最終的には解析は他のソリューションと連携する必要があり、SIを経由することで、これらの企業は既存のエコシステムに参入することができるからだ。

Viisights社CEOアザフ·ビレンツィエグ氏は、同社はほとんどの販売をシステム構築者経由行っており、積極的に販路を拡大しようとしていると説明している。

同氏は「モトローラ·ソリューションズやNECなどの大手システム構築者との協力関係を持っているが、小規模システム構築者とも提携している。当社は、主に米国と欧州でシステム構築者のネットワークを拡大したいと考えている。当社製品については、現在は監視采井会社や警備会社に直接販売しているが、今後は現地の代理店への販売方法を拡大していきたい」と述べている。

システム構築者をサポート

ほとんどの企業は、協力会社と組むことで、顧客に提供するサービスにさらなる付加価値をもたらすことを提案している。Davista社CSO兼CMOスコット·シエラスキ氏は、協力関係を構築することで、販売会社は、現在利用可能な最も価値のある技術の1つを顧客ベースに提供できるようになると説明している。

そして、「当社がこれまでに面談したエンドユーザはみな、AIをセキュリティ·プログラムに拡張したいと考えている。AIがどこに適合するかを正確に把握していないが、セキュリティでの運用をより多く行う必要があることは理解している。今、物理セキュリティ販売会社は、顧客ベースにプロアクティブや処方型の技術的解決策を提供し、既に提供している他のサービスや技術価値を拡大することができる」と話している。

Rhombusシステムズ社CEOギャレット·ラーソン氏も同様の考えを持ち、協力会社であるシステム構築者の成長は同社にとって重要であると付け加えている。

「当社は全て販売会社経由で販売しており、すべての販売会社との関係を非常に大切にしている。私たちは販売会社が当社事業にとって非常に重要な存在であり、顧客との関係を可能な限り成功させたいと考えている。当社の販売会社は、当社と一緒に仕事をすれば、彼らの成功に全面的に支援してくれる技術提供企業が背後にいることを知っているので、販路経由販売で大きな成功を収めている」と付け加えている。

システム構築者が付加価値を高める方法

Netra社CEOアミット·ファンサルカ氏は、システム構築者が当社と提携することで、シンプルさ、洗練されたもの、そして価格の3つの要素が、システム構築の提供価値を高めると述べている。

同氏は提供側の観点から見たシンプルさについて、「当社が単一のAPIを使用して、物体検出、行動検出、さらには車のメーカやモデルの検出など、全ての機能を提供している」とPhansalkar氏は説明している。洗練さについては、「他のソリューションとのシームレスな統合を実現する能力のことを指す。非常に早く統合できる。システム構築者や販売代理店は、数時間以内に当社のソリューションと統合することができる。最終的には、システム構築者の主要ソリューションに価格を追加するだけで、エンドユーザが簡単に利用できるようにしている」と解説している。

MOBOTIX社、同社映像技術は100% NDAAに準拠を宣言

NDAA第889条には、スパイやハッカーの攻撃からの保護を強化するためのガイドラインが新たに盛り込まれている。さらに、通信目的で使用される部品（セキュリティ製品を含む）を製造する中国企業の名前が挙がっているが、これはもはや受け入れられない。

MOBOTIX社は、上記を明確にするために、中国企業のSoC（システム・オン・チップ）やソフトウェアを処理することができるその他のコンポーネントを使用していない。さらに、同社のOEMパートナー（相手先ブランドの機器メーカ）から供給された製品は、100% NDAAに準拠している。

MOBOTIX社は、同社製品とシステムに中国製の部品が含まれていないことを3段階の自己認証プロセスで明確に証明している。NDAA適合証明書は、MOBOTIX社製品を購入して設置する米国の複数の機関や主要な統合パートナーに既通知されている。

MOBOTIXの技術は、品質だけでなく、データとサイバー・セキュリティの観点からも世界に先駆けている。リスクのある供給企業からの部品を使用しないことは、常に非常に重要なことであり、独自の設計によって顧客やパートナーのセキュリティを保護している。

グローバル化の時代にあっても、国家の安全保障上の利益が国際貿易政策を支配し続けている。個々の国や国のグループが投資を管理し、防衛・安全保障調達のためのルールを確立しています。コンプライアンスガイドラインは、グローバルなサプライチェーンに沿ったリスクを効果的に特定し、最小化するように設計されている。

■関連URL・・https://www.mobotix.com/en/node/16372

イーグルアイネットワークス社、ベンチャーキャピタルから4000万ドルを調達

イーグルアイネットワーク社は、今回ベンチャーキャピタルのアクセル社からのシリーズ調達した4000万ドル（約40億円）の資金を、成長を継続し技術的リーダーシップを拡大するために投入する。

具体的には、真のクラウド・プラットフォーム上で人工知能（AI）を活用し、映像監視を劇的に再構築して、世界中の企業の安全性、セキュリティ、オペレーション、顧客サービスを向上させ、ビジネスインテリジェンスとセキュリティを提供する。

■URL・・https://www.een.com/ja/eagle-eye-networks-raises-40-million-to-transform-video-surveillance-by-combining-cloud-and-ai/

■アクセル社について

同社はグローバルなベンチャーキャピタル。これまでにAtlassian、Braintree、Cloudera、Crowdstrike、DJI、DocuSign、Dropbox、Etsy、Facebook、Flipkart、Freshworks、Jet、Pillpack、Qualtrics、Slack、Spotify、Supercell、Tenable、UiPath、Venmoなどに、過去35年以上にわたって支援をしている。

オフィス移転

株式会社ADL

〒166-0002 東京都杉並区高円寺北1-17-5　上野ビル

TEL　03-5318-1420　FAX.03-5318-1421

URL・・http://www.adlinc.co.jp/

ビボテックジャパン株式会社

〒 105-0012 東京都港区芝大門2-1-14 デルタ芝大門ビル

TEL・・03-5733-1280

https://www.vivotek.com/website/jp/

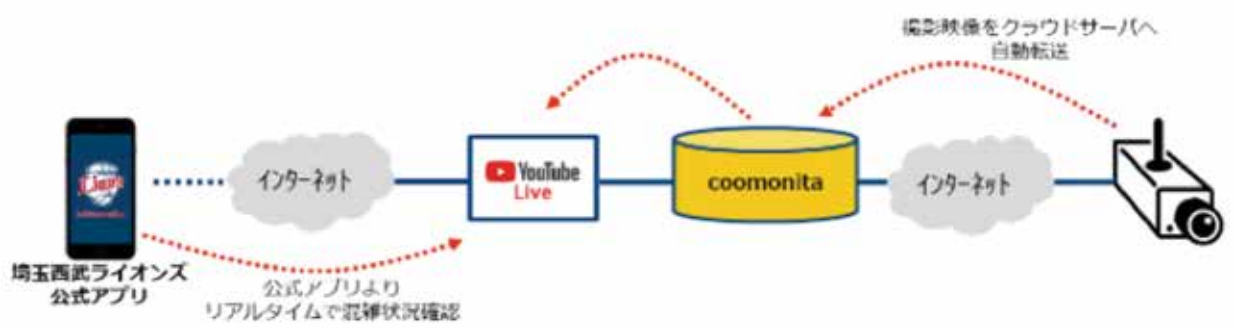
カリーナシステム株式会社

〒650-0034 神戸市中央区京町69 三宮第一生命ビルディング7F

TEL：078-335-7601　FAX：078-335-7602

URL・・https://www.carinasystem.co.jp/

NTTコミュニケーションズ、埼玉西武ライオンズでクラウド録画カメラサービス「coomonita」を活用



NTTコミュニケーションズが提供する、スマートフォンやパソコンからカメラのライブおよび録画映像を視聴できるクラウド録画カメラサービス「coomonita (コーモニタ)」が、埼玉西武ライオンズのスタジアムにおけるデジタルトランスフォーメーション(DX)実証実験に採用された。

同社は映像を活用したDXの取り組みの一つとして、メットライフドームにおいて、ネットワークカメラで撮影したリアルタイム映像の配信により、来場者がスタジアム内のグッズショップや飲食売店の混雑状況を確認できるサービスを提供している。

■背景

埼玉西武ライオンズではメットライフドームにおける新型コロナウイルス対策の「密」を避けるための取り組みとして、一部店舗での入場整理券配布や、待機列での立ち位置の目安マーク表示などを行っている。

NTTコミュニケーションズは、今後も安全安心かつ快適に来場者が野球観戦を楽しむため、手軽に導入することができる本サービスを活用した混雑回避ソリューションを提供し、その効果測定や価値検証を行う。

■概要

混雑が予想される箇所をネットワークカメラで撮影し、その映像を本サービスの「YouTube Live連携」機能を用いてリアルタイム映像として配信。

■メットライフドーム内撮影場所

①公式グッズショップ「ライオンズ チームストア フラッグス」
②「西武球場前駅」改札付近
③「クラフトビアーズ オブ トレインパーク」

■特長

①「YouTube Live」と連携し、大人数への映像配信を実現

本サービスの「YouTube Live連携」機能により、ハイビジョン画質のリアルタイム映像を大人数へ配信することができる。

②配信映像は公式アプリから確認可能

来場者は自分のスマートフォンにインストールした「埼玉西武ライオンズ公式アプリ」を通じて「YouTube Live」にアクセス可能。観客席にいながらネットワークカメラ設置先の混雑状況を確認できる。

③来場の利便性を増加させ、スタジアムを活性化に貢献

イニング終了間際の混雑集中など、リアルタイムで混雑状況を確認することができ、待ち時間の削減や混雑回避に繋がる。その結果、公式アプリの使用者数の増加、店舗混雑による機会損失の解消など、メットライフドーム活性化に貢献する。

■今後の展開

NTTコミュニケーションズは本サービスの本格導入に向け、埼玉西武ライオンズのカメラ設置場所拡大を支援する。将来的には、IoTプラットフォーム「Things Cloud(R)」と各種センサを組み合わせたイベント検知の仕組みや、AI映像解析ソリューション「COTOHA Takumi Eyes(R)」による画像解析結果に基づくマーケティングや業務改善活用など、埼玉西武ライオンズおよび来場者の利便性向上に貢献する新たな価値を提供していく。

■coomonita(コーモニタ)

設置したネットワークカメラの24時間365日の映像をクラウドに保存できるサービス。カメラで撮影した映像は、過去映像もリアルタイム映像も、テレビ放送並みの高画質での視聴が可能。従来の防犯カメラシステムに必要であったカメラと紐づくレコーダやモニタが不要なため、費用を抑えた導入が可能となる。

また、月々の費用も、保存期間に応じて選択が可能で、予算に応じて柔軟に導入することができる。

ADLINK社とSageRAN社、5Gオープン無線アクセスネットワーク（RAN）向けエッジソリューションの開発拡大で、提携

ADLINK社は、エンド･ツー･エンドの5Gオープン無線アクセスネットワーク（RAN）ソリューションの開発での提携強化のため、SageRANネットワーク･テクノロジ社と契約を締結した。パートナーは、パブリックおよびプライベートネットワーク向けのオープン･アーキテクチャに基づく統合5Gエッジソリューションを開発するための共同ラボを設立し、通信サービスプロバイダが業者間の相互運用性を向上させ、イノベーションを強化し、継続的なコスト削減を実現するのを支援する。

このパートナーシップの拡大で、プライベート5Gネットワークに求められるコンパクトなエッジ･ソリューションの開発に加え、車と車との間/道路と車との間（V2X）通信や産業用IoT（IIoT）などの特殊用途向けの5G対応ソリューションの開発が加速される。

既に両社は、ADLINK社製最新マルチアクセス･エッジ･コンピューティング･サーバのMECS-7210/MECS-6110とSageRAN社製ベース･バンド･ユニット（BBU）のプロトコル･スタックを統合した、業界初の超コンパクトの統合5Gスモールセルセットの開発に成功している。

この5Gスモールセルセットは、便利で費用対高価に優れた5G統合ソリューションを構築して、OTIIに準拠し、NGC-Readyに認証されたハードウェアに完全な5Gネットワーク機能を提供するのに役立つ。

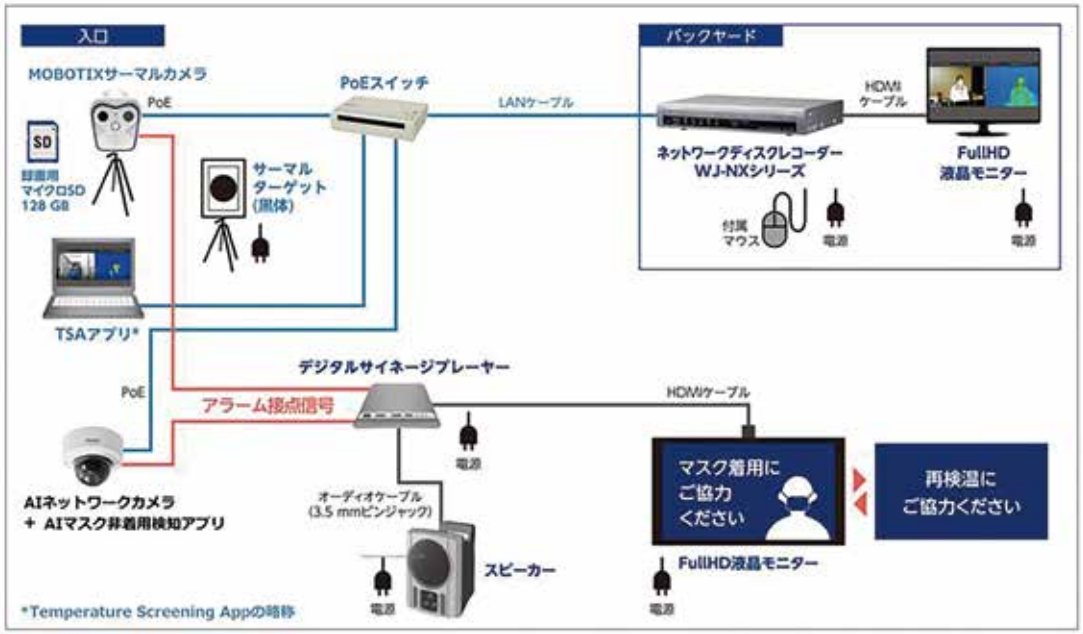
■関連URL

ニュース　https://www.adlinktech.com/jp/CompanyNews_20102113215582383

ADLINK　https://www.adlinktech.com/jp/

SAGERAN　http://www.sageran.com/en/

パナソニックi-PROセンシングソリューションズとコニカミノルタ、感染症の拡大防止対策を支援する映像監視システムを開発し販売



本システムは、「発熱者の検知」(2020年11月発売)および「マスク非着用者の検知」(2020年12月発売)の2つの用途から構成されている。

■発熱者の検知 (2020年11月発売)

i-PRO製NVRを、MOBOTIXサーマルカメラとコニカミノルタ開発のMOBOTIXサーマルカメラアプリケーション「Temperature Screening App（テンパーチャー スクリーニング アプリ）」に連携させ、非接触で人間の体表面温度を計測するとともに、MOBOTIXサーマルカメラで撮影した可視映像とサーマル映像をネットワークディスクレコーダーに記録する。

発熱者を検知した場合、管理担当者へ通知、もしくはデジタル･サイネージの画面案内を行う。また遠距離からの体表面温度測定が可能で、スループット性能が高く、人の流れを妨げることなく測定でき、測定する側･される側双方の負担を軽減できる。

さらに、NVRに記録された映像は、発熱者を検知した場合、Temperature Screening Appが発信するアラーム情報をもとに確認することができる。

■「マスク非着用者の検知」(2020年12月発売)

i-PROが開発した「AIマスク非着用検知アプリケーション」をAIプロセッサ搭載ネットワークカメラで稼働させ、カメラ単体で映像内の人物を特定し、その人物の顔にマスクが装着されているかどうかをAIテクノロジにより判定する。

■特長

- AIネットワークカメラで稼働し、マスク非着用者を映像から自動検知し、アラーム通知
- 既存の監視システムに追加組み込みが可能で、設定レスで簡単導入が可能
- 現在流通している主要なマスクに対応し、複数マスク非着用者を同時に検知

■関連URL

https://news.panasonic.com/jp/press/data/2020/10/jn201006-3/jn201006-3.html

https://www.konicaminolta.com/jp-ja/newsroom/2020/1006-01-01.html

---

日本万引防止システム協会、認定個人情報保護団体となる。

工業会 日本万引防止システム協会は、2020年9月30日に一般財団法人日本情報経済社会推進協会の制定する認定個人情報保護団体の認定を受けた。同協会は40番目の認定団体となった。

認定個人情報保護団体

一般財団法人日本情報経済社会推進協会（英文名称：JIPDEC）の制定する個人情報保護法の適用を受ける事業者（個人情報取扱事業者）は、個人情報の適正な取扱いを確保するための取組を自発的に確立しなければならない。そのため個人情報保護法では、事業者の自発的な取組を促進させ、法の趣旨を踏まえた個人情報の保護を推進する目的で、「認定個人情報保護団体」制度を設けている。

認定個人情報保護団体は「個人情報保護指針」を定め、対象事業者に保護指針を遵守させるための措置をとることが義務付けられている。

対象事業者

認定個人情報保護団体の個人情報取扱事業者は以下のいずれかに該当する。

1. 当協会が運営する個人情報保護にかかる認証制度（プライバシーマーク制度）において認証を受けた事業者
2. 電子情報の保護と利活用の推進のため、当協会が認める事業者

工業会 日本万引防止システム協会（英文名称：JEAS）

万引防止システムを製造、販売、サポートする企業の業界団体であり、流通業界の 健全な経営、また青少年の非行防止という産業的、社会的役割を果たすべく、行政 機関、関連業界団体とも連携をとり活動している。

■協会URL･･https://www.jeas.gr.jp/

モスウェル、製品ラインナップを拡充

同社は、CMOSカメラ、周辺映像機器を中心に製品開発している企業で、このたび多様化する需要に応えるため、製品ラインナップを拡充した。

アナログ/アナログHDでは、MS-M47HTおよびMS-M104HDAの組込用カメラとアナログ→USB変換ボードMS-TR104AUDの新製品をはじめ、他10数機種をそろえている。アナログHDモニタ/電源/DVRでは、モニタとしてML-7AHおよびML-7AHRの7型を含めて8機種、IH電源ユニットとしてMS-PV25、4チャネルDVとしてMR-1004Mを用意している。また、USBタイプで11機種14品目、HD-SDIタイプで6機種、Wi-Fiタイプで3機種をラインナップしている。

上記例外にハイブリッド型、ステレオ･外部同期型、車載システム（HD-SDI･アナログ･アナログHD）などを開発販売している。

■URL･･https://moswell.co.jp/

リモートワークで サイバー・セキュリティと 物理的セキュリティの リスクを減らす方法

COVID-19の大流行により、世界中の何百万人もの人々が在宅勤務を余儀なくされている。企業の中にはリモートワークのシナリオに備えているところもあるが、多くの企業はそうではなく、備えている企業でもパンデミックのような長期化に備えていない場合がある。

現在の状況がどのくらいの期間続くのか、あるいは在宅勤務や社会的距離を置く命令がどのくらいの期間続くのかが見当もつかない中で、企業はリモートワークの計画を試している。

残念ながら、多くの企業はリモートワークには多くの準備が必要であり、サイバー犯罪者が現在の状況を悪用していることを体感している。自宅のネットワーク、企業所有の機器やデータのサイバー・セキュリティを確保し、物理的な場所の遠隔監視を行うための最善策を実施することで、企業は従業員が自宅で仕事をしている間も安心して仕事をすることができる環境を提供することになる。

●アイフェ・ストロム　フリーランサー　著

家庭内ネットワークは企業所有機器に対応できるか？

新型コロナウイルスは、リモートワークに関して多くの疑問を投げかけている。一部の企業にとっては、遠隔での運用すら可能かどうかという疑問が生じている。また、在宅勤務が企業の機密データのセキュリティにどのような意味を持つのか疑問に思う企業もある。

また、在宅勤務は、データのプライバシー、サイバー攻撃、詐欺などの問題も浮上している。侵入は、安全性の低い家庭内ネットワークで顕著になっている。

通常、オフィス環境の物理的な制約の中で操作される機器は、企業のファイアウォールの外で使用するように構成されていない。現在の状況では、これらの機器や家庭内ネットワークが試されている。

「ネットワーク・ディスカバリ、ワイヤレス印刷、RPC/SMBなどのサービスが無効化されておらず、家庭内ネットワークにセキュリティ対策が施されていないことを考えると、これらの機器がより大きな脅威にさらされている」と米国に拠点を置く大手システム構築企業コンヴァーギント・テクノロジィズ社戦略・サイバー担当副社長ケビン・ドネガン氏は述べている。

従業員に基本的なセキュリティ知識を身につけさせることが重要となる。自宅の Wi-Fi ルータが安全であることを確認し、フィッシング・メールを開かないようにするなどの簡単なことが、大きな効果をもたらす。

プロトコルの変更

接続機器が一般的ではなかった時代を思い出すのは難しい。今日では、全てのものが接続されているため、ネットワーク・セキュリティにはそれほど注意を払っていないのではないだろうか。残念ながら、これはネットワーク通信を盗聴されやすい状態にしている可能性があることになる。

「当社では、所有する機器が安全なネットワーク内でファイル・サーバやデータベース、その他の企業アプリケーションに接続できることを当然のことと考えているため、家庭内ネットワークでの取引は暗号化されていないことが多い。一部の組織では、IT 部門が自宅からのオペレータへのアクセスを開放しているが、通信プロトコルは変更されておらず、チャネルの安全性を確保するための措置も取られてない」とドネガン氏は述べている。

家庭内ネットワーク接続が暗号化されていることを確認することで、データや機器の安全性を保つことができる。Wi-Fiの暗号化規格はいくつかあるが、WPA2またはWPA3を使用することをお勧めする。また、強力なパスワードを選択することも忘れないことだ。

セキュリティ向上のための新技術の導入

世界経済がCOVID-19への対応に苦慮している中、予算が削減され、人員が解雇される一方で、攻撃対象が指数関数的に拡大しているとドネガン氏は説明している。

「ほとんどの組織では、BCP（事業継続計画）の中で、従業員を在宅勤務モデルに移行する計画がなかった。これを実現するためには、企業は新技術を導入して機器を安全に管理し、リモートで機器を管理・更新する手順を作成し、セキュリティ・ツールから物理的に分離された機器上の脅威を軽減するプロセスを管理する必要がある。できるだけ迅速に新技術を選択して展開し、工程と手順を作成する必要があり、技術や手順についてのトレーニングを受ける必要がある」とドネガン氏はアドバイスする。

将来に向けての準備

現在のパンデミックがいつまで続くのか、いつまで存在し続けるかは誰にもわからない。そのため秩序やソーシャル・ディスタンス(社会的な距離感)を保つことになる。当面はリモートワークが標準、つまり在宅勤務に関連した全てのセキュリティ・リスクに対処することが重要となる。

サイバー・セキュリティの脅威からリモートワーク機器を保護する方法

オフィスでも自宅でも、IT部門にとってサイバー・セキュリティは年々大きな関心事となっている。COVID-19の環境下で、リモートワーカーの数は劇的に増加している。残念ながら、多くの人が業務の自宅への移行の準備をしていなかったため、ネットワークや機器、データが脆弱なままになっている。

しかし、全てが失われたわけではない。自宅待機命令が世界中で発令され始めてから、

多くの企業がリモートワークの最善策を発表している。VPNからクラウド・サービスのソフトウェア・アップデートまで、ネットワークへの侵入を防ぐためには幾つかのステップがある。

システムを直接インターネットに晒さないこと

可能であれば、アプリケーションやシステムを直接インターネットに公開しないようにするよう、コンヴァーギント・テクノロジィズ社戦略・サイバー担当副社長ケヴィン・ドネガン氏はアドバイスしている。

コンヴァーギント・テクノロジィズ社
戦略・サイバー担当
副社長ケヴィン・ドネガン氏

必要であれば、セッションの安全性を確保するためにHTTPS/TLS やその他の標準規格を使用していることを確認し、基礎となるシステムがパッチ適用されていることを確認し、ユーザが確実な認証情報を持っていることを確認し、多要素認証の使用を要求する。

「物理的または論理的な分離を使用して、インターネットに晒されているシステムを隔離し、以下のことを行う。脆弱性を制限し、攻撃が発生した際に自動的にリスクを軽減するMDR（マネージド・ディテクション&レスポンス）機能を導入する」と同氏は述べている。また、

VPN（仮想プライベート・ネットワーク）を利用してWi-Fiネットワークにアクセスし、暗号化することでオープン・インターネットを経由する全ての通信は、データを保護するための別の方法となる。

パスワードのリセット

企業は従業員のパスワードを監査し、アクセスに使用されるパスコードをリセットする必要がある。新しいパスワードは、厳格なセキュリティ基準の範囲内に収まるようにする必要がある。英数字コードや多要素認証を勧める。

また、家庭用ルータのパスワードをリセットすることも重要となる。家庭用Wi-Fiルータは、デフォルトのパスワードが変更されていないだけで、ハッキングの被害に遭うことがよくある。リモートワークを行うことで、サイバー攻撃からデータとネットワークを保護するためのシンプルかつ重要なステップとなる。

不要なサービスやアプリケーションを無効にする

今は、必要なサービスやアプリケーションだけアクセスする時代だ。ドネガン氏は、従業員が自宅に持ち帰る機器で絶対に必要ではないサービスやアプリケーションをすべて無効にすることを推奨する。

「エンドポイント・ベースのセキュリティ・アプリケーションを有効にするかインストールして、機器を監視して保護する。機器を使用している間は、ソフトウェアの更新とオペレーティング・システムへのパッチ適用を継続することだ」とアドバイスする。

機器とソフトウェアの更新を維持する

新たに作成され、発見されるウイルスやマルウェアの数は増え続けている。特にサイバー犯罪者が危機的な時期を悪用することはよくあることで、機器、ソフトウェア、オペレーティング・システム、アプリケーションなどを常に最新の状態に保つことが重要となる。

ハッカーは、ソフトウェアのアップデートを怠る人々の怠惰さを利用している。これでは、簡単に侵入口を開けてしまうことになる。ソフトウェアを定期的にアップデートすることで、脆弱性にパッチを当てることができる。

機器紛失に備える

従業員がオフィスで仕事をしている時は、IT部門では機器が盗まれることを心配することが少ない。しかし今では、機器が外に持ち出されることで、そのセキュリティ／ネットがなくなった。つまり、企業は機器が行方不明になった時や、もしものときのための計画を立てておく必要がある。

英国に拠点を置くナショナル・サイバー・セキュリティ・センターでは、リモート・ワーカは 機器を紛失したり盗まれたりした場合の対処法を知っておく必要があり、データへのリスクを最小限に抑えるために、従業員は可能な限り早く紛失や盗難の報告を徹底している。

常に注視する

上記の対策は、ネットワークや機器を保護するための基本的な手段に過ぎない。業務上の企業サービスにこだわり、警戒心を持ち続けることで、サイバー・セキュリティへの懸念をさらに緩和することができる。

リモートワーク中の空席オフィスの確保

COVID-19の在宅勤務やソーシャル・ディスタンス確保の指令により、物理的なオフィス空間が生じ、脆弱性を残した

ままになっている。

サイバー・セキュリティはリモートワークに関連して人々が考える第一の問題かもしれないが、COVID-19のために空になったオフィスの物理的なセキュリティはどうするか?オフィス内の資産と、出入りする必要がある従業員を保護することは、やはり最優先事項でなければならない。

リモート監視とアクセス

セキュリティ担当者や経営者は、空きスペースや使用されていないオフィス空間を遠隔監視するアクセス権を持っている必要がある。モバイル機器やデスクトップを介した遠隔監視機能は、現代のほとんどの映像監視供給企業が提供している。セキュリティ運営担当者は、このパンデミックの前にそれを完全に活用していない可能性がある。今は、システムの遠隔監視機能を見直す良い機会だ。

オフィスビルから従業員を完全にロックダウンし、ロックアウトする必要はないかもしれないが、監視およびアクセス・コントロール・システムへのアクセス権を持つことは、空の施設内およびその周辺の全ての活動を監視するのに役立つ。遠隔監視により、セキュリティ担当者は、誰がいつ、どのくらいの時間、敷地内にアクセスしているのかを確認することができる。また、アクセス・コントロール・システムは、許可されていないエリアを維持するように設定することもできる。

また、コンヴァーギント・テクノロジィズ社戦略・サイバー担当副社長ケヴィン・ドネガン氏は、デバイスやシステムの遠隔監視の必要性を強調している。同氏は、機器やシステムは安全でなければならないが、メンテナンスも必要であることを指摘している。

「機器の状態や性能そしてセキュリティだけでなく、遠隔で機器を監視するための機能を導入する必要がある。セキュリティ担当者は、自宅から機器を更新したりパッチを当てたりすることができ、機器が故障した際にそれを知ることができる必要がある。機器は、セキュリティを確保し、監視し、脅威が発生したときにそれを緩和する機能を持つ必要がある」。

サイバー・セキュリティは今も重要

ドネガン氏によると、セキュリティ・システムを遠隔で監視するという行為そのものが、システムに新たな脆弱性を開く懸念があるという。

「これは新しい接続を開き、より多くの通信をインターネットに晒し、通信を盗聴したり、ネットワークに侵入したりする攻撃者を誘います」と同氏は述べている。

また、同氏は、セキュリティ専門家が自宅からアクセスして管理できるように、物理的なセキュリティ機器ネットワークやビル・オートメーション・システムなどの重要なシステムのログイン・ポータルがインターネット上に直接公開されている一方で、これらのシステムはしばしば使用済みのシステムであると説明している。これは、メーカのパッチでサポートされなくなったか、単に定期的にパッチを当てていないため、攻撃者が容易に発見できる新たな脆弱性が発生している。

「当社では、業界標準を満たす、あるいはそれ以上の安全な通信モデルが証明されているクラウド・ベースのMDR(マネージドディテクション&レスポンス)およびヘルス・モニタリング(HM)機能を導入している。これらのシステムにより、チームは遠隔で環境を監視、更新、安全を確保することが可能になり、セキュリティ担当者の負担を軽減することができる」とドネガン氏は述べている。

セキュリティ・プランの再評価

オフィスが空っぽになった今は、新規および既存のセキュリティ・ポリシーや手順を見直し、実施する良い機会かもしれない。オフィスが空いている間にセキュリティ評価を実施することで、評価者は通常の業務を中断することなくテストを実施することができる。また、以下のような場合のセキュリティ手順やコンティンジェンシー・プラン(緊急時対応計画)を考えるのにも良い時期だろう。

COVID-19のパンデミックは、映像監視やアクセス・コントロール、侵入検知や照明などを含む全ての物理的なセキュリティ・システムがいかに重要であるかを証明し、最新の情報を入手し、改善していく必要があることを示している。

a&S

サイバーセキュリティとクラウド映像監視

イーグルアイネットワーク社

ネットワーク化された昨今の映像監視システムは、様々な点において脆弱が指摘されています。とりわけ監視カメラはハッカーにより大量のDDoS（Distributed Denial of Service）攻撃の踏み台にされます。

ネットワーク映像システムのセキュア化は複雑かつ技術的に困難な場合があります。しかし、中小規模のビジネスにおいては、必ずしも複雑な問題ではありません。映像システムおよび関連機器は、既に導入されている既存のネットワーク映像技術とは対照的に、事前にセキュリティ強化済みかつ容易にセキュリティ保護が可能な専用品を用いることができるからです。

映像システムにおけるサイバーセキュリティ

コンピュータとネットワーク・セキュリティは、ネットワーク・システムおよびそのデータにおける機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の保護に重点が置かれています。映像システムにおいてカメラの記録映像は重大な法的証拠になり得るため、この3つの要件は、極めて重要です。さらに、昨今多くの企業では、映像システムに瞬時に監視できる機能や様々な映像解析などの運用面も重視されています。モバイルデバイスにより、映像へいつでもどこでもアクセスできることが、昨今のビジネスにおいては、期待されます。

しかしながら、多くの映像システムではサイバー攻撃に対するセキュリティ機能が組み込まれておらず、インターネット接続は機密性、完全性、可用性の点でリスクがあると考えられています。このように、多くの映像システムはサイバー攻撃に対して無防備であり、サイバー攻撃の増加により対策を行うことが、これまで以上に重要になってきています。

従来型と専用型（General-Purpose vs. Purpose-Build Equipment）

従来型のネットワーク映像管理システムでは、セキュリティを確保するためにコンピュータ、ネットワーク・スイッチ、ルータ、ファイアウォールについての高いスキルが必要でした。製品開発元からは、適切なセキュリティ設定を行うためのシステムやガイドが提供されていました。それでさえ、製品の改善や新たなサイバー脅威の出現に伴い、セキュリティの強化の為には、継続的な注意とアップデートが必要となります。

ネットワークに繋がっている機器からセキュアなVMSの設定をすることは、映像システムの設置業者や顧客にとっては、特に重要なことではないかもしれません。専用的な映像監視プロダクトを提供する開発元は、あらかじめ機器の設計時にソフトウェアのセキュリティ強化を行い、セキュリティの事前設定がなされたシステムを提供することが求められます。

一方、サービスとして提供されるクラウドベースの映像監視システムは、サイバーセキュリティに対して継続的なアップデートを行われます。

クラウド映像監視システムにおけるサイバーセキュリティの利点

十分に設計されたクラウドベースの映像管理システムは、完全オンプレミス型のシステムには搭載されていないセキュリティ上の利点を持っています。

●強いセキュリティ・プロファイル

小規模オフィスや店舗、サービスセンターや製造設備にとって、完全なオンプレミス型で映像監視システムの実装は、とても困難でコストがかかります。一方、クラウドベースのシステムでは、顧客はライブまたは記録映像へのセキュアなアクセスを、オンプレミス型よりも安価に利用することができます。

●管理システム

例えば、Eagle Eyeのオンプレミスの映像アプライアンス製品は、Eagle Eye Cloud Data Centerで管理され、セキュリティと機能を自動的に最新状態に保ちます。したがって、設置業者と顧客はアップデートの手間を削減することができます。

●システムとデータ冗長性

Eagle Eyeの複数のデータセンターで管理されているサーバとデータベースは、個々のサーバやデータストレージ機器のステータスに関係なく、システムを維持します。Eagle Eyeのローカル映像ストレージは冗長性も兼ね備えています。

ここからは、Eagle Eyeネットワークス社Eagle Eye Cloud VMSが有する様々な特長や利点について、前号で紹介していない項目についてご紹介します。

システムアーキテクチャ

Eagle Eye Cloud VMS はセキュアなクラウドベースのシステムで、従来のDVRやNVRと異なる点は以下の通りです。

●オンプレミスのEagle Eyeカスタムビルド・アプライアンス

ブリッジ(Bridge)は、カメラ・ビデオエンコーダから映像や音声、アラームやイベンドデータを受信およびバッファリングし、

Eagle Eyeのクラウド･データセンターに送信します。

Cloud Managed Video Recorder（CMVR）は、Bridgeの機能にプラスして、オンプレミスの機器のローカルストレージに映像を保存する機能を有します。必要なネットワーク、ルーティング、ファイアウォール機能は、オンプレミス･コンポーネントの整合性を確保するために、アプライアンス内部に搭載されています。

●Eagle Eyeカスタムビルド･データセンター機器

Eagle Eye Cloud VMS プラットフォームとVideo API プラットフォームアプリケーションサーバ、システムデータストレージ、映像データストレージなどすべてEagle Eye Cloud Data Center で管理されています。

Eagle Eyeシステムは、最新の冗長クラウドアーキテクチャで構成されており、Web ブラウザのインタフェイス、iOS、Android スマートフォン･タブレット機器で包括的に管理が可能です。システムアーキテクチャは、下図の通りです。

記録は通常、オフサイトであるEagle Eye Cloud Data Center で行われます。ユーザの希望によっては、カメラのロケーションにあるオンプレミスでの記録、またはカメラにあわせてクラウドとオンプレミスのコンビネーションを選択することができます。オフプレミスでの記録では、Eagle Eyeオンプレミス装置は、データをローカルでバッファリングすることで、インターネット接続が不安定な環境でも、映像データが途切れることはありません。

Eagle Eye Cloud Data Center

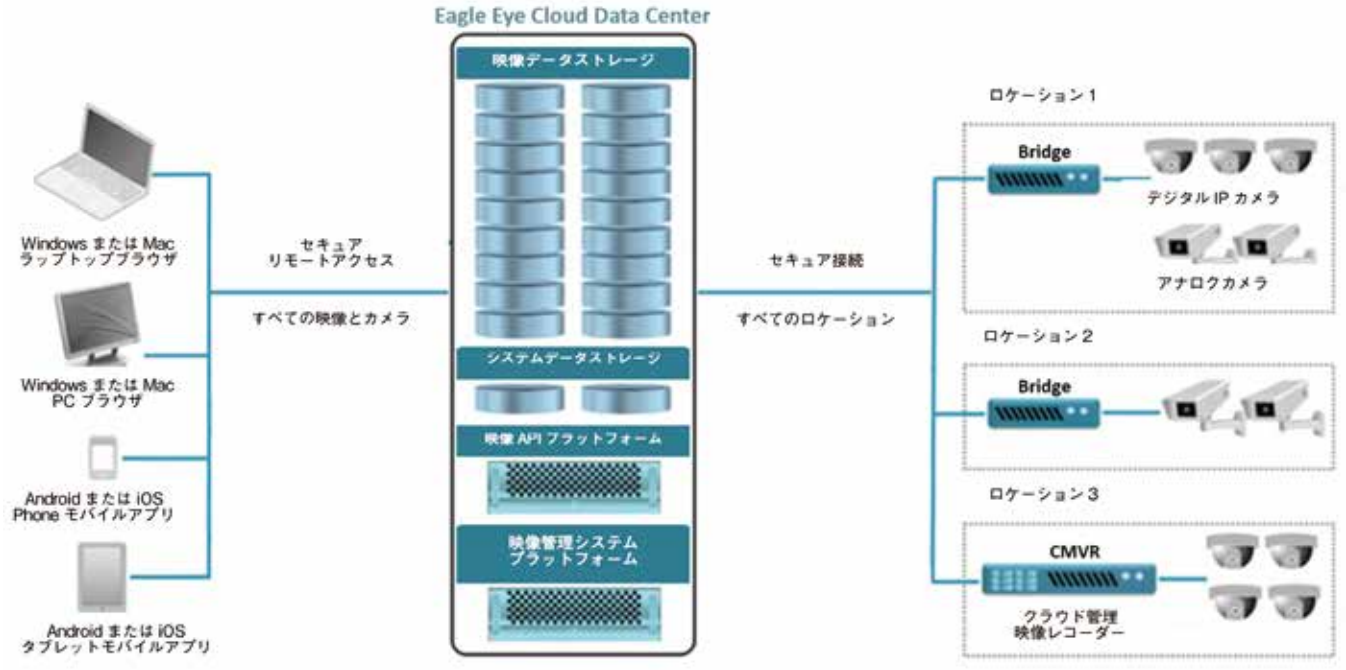
システムアーキテクチャの中心は、顧客のオンプレミス環境のアプライアンスと互いに連携することで、セキュアな接続を維持し、高いセキュリティを確保したデータセンターです。

データセンターは、3種類のアーカイブで顧客の映像データに保存するために、冗長データ保存方式を採用することで、記録映像のデータロスを防ぎます。このデータセンターは、Eagle Eye Cloud Data Center と呼ばれています。

Eagle Eye Cloud Data Centerの設計にはバイオメトリック･アクセス･コントールをもつ区画化されたセキュリティゾーンがあります。全てのデータセンター･コンポーネントは完全にフォールト･トレラントで設計されており、冗長ネットワーク･アップリンク、アプリケーション･サーバ、データストレージ、冷却装置、HVAC 空調設備、電源パネル、電源分電盤などで構成されています。ネットワーク構成もサーバのデュアル･ネットワークカードを含め、冗長化されています。電源は2つの異なる変電所から供給された電力によって供給され、なおかつ各電源に1つずつバックアップ発電が備え付けられています。これらの要件は、99.999%のハードウェア可用性を確立することで、単一障害ポイントを防ぐように設計されています。

Eagle Eye Cloud VMSアーキテクチャ

Eagle Eye Cloud Data Center は、バイオメトリックス･スキャナとセキュアなカードアクセスにより、コロケーション･サービス区域への入室が許可されています。オンサイト･セキュ



Eagle Eye Cloud VMSアーキテクチャ

リティ担当者は、ホスティング設備を屋内外の映像監視を介して24時間365日監視しています。データセンターへのアクセスにはセキュリティ·デスクによるチェックインが必要で、24時間365日管理されています。

Eagle Eye Cloud Data Center によるマルチレイヤのアプローチは、境界ファイアウォール、ネットワーク侵入検知システム、ネットワークアドレス変換(NAT)、およびデータベース·サーバがパブリックにさらされないようなネットワーク·セグメントが含まれています。またデータセンターは、地理的にも物理的にもEagle Eye社オフィスから離れた場所に所在しています。インターネットアクセスは冗長インターネット·バックボーンによって供給されています。Eagle Eyeでは、Eagle Eye Cloud Data Centerプラットフォームへ物理的なアクセスまたはログイン·アクセス権限を持つ社員については、徹底的なスクリーニングとバックグラウンドチェックを行っています。

Eagle Eyeのオンプレミス·アプライアンス

Eagle Eyeのアプライアンスはローカルで映像をバッファし、限られた帯域でも制御を可能とするIntelligent Bandwidth Management™テクノロジによって、Eagle Eyeクラウドに転送されます。Intelligent Bandwidth Management™はデータ転送と帯域の利用を動的に調整し、既存のインターネット接続を最適に利用できるようにプライオリティ付けを行います。

サイバーセキュリティ機能については、次号でご紹介します。

サイバーセキュリティ機能

Eagle Eye Cloud VMSではサイバーセキュリティについて暗号化とデジタル証明書を利用しています。下記に掲げたキーワードについて解説します。

●イーグルアイのデータ暗号化
●公開鍵と秘密鍵の管理　●デジタル証明書
●Eagle Eye Cloud Data Centerの認証
●イーグルアイアプライアンスの認証
●送信データの暗号化　●記録データの暗号化
●ユーザ認証の方法　●Apple Touch ID による指紋認証
●First Responder Real-Time Video Access
●アプリケーションセキュリティ　●顧客データ保護
●高度なネットワークリクエスト
●イーグルアイのセキュリティプラクティス

【問い合わせ先】イーグルアイネットワークス　03-6868-5527

パナソニックi-PROセンシングソリューションズ、耐重塩害仕様の赤外線照明搭載PTZネットワークカメラ 2機種を発売

本製品は、重塩害地域に設置可能な赤外線照明搭載PTZネットワークカメラ2機種（WV-X6533LNSJ/WV-S6532LNSJ）で、潮風が吹く沿岸部などの重塩害地域においても設置可能なことに加え、明るい昼間だけでなく、夜間、照明の一切ないゼロルクスの場所でも、赤外線照明（LED）を用いたPTZ（パン/チルト/ズーム）機能による映像監視を行うことができる。

【主な特長】

●重塩害地域といった厳しい屋外環境における塩害腐食への耐久性

カメラ筐体に耐食処理を施し、さらに耐食･耐候性の高い塗料を粉体塗装することで表面を保護し、塩害による腐食に強い耐重塩害塗装を実現している。さらに塩害対策の処理を施したねじを採用することにより、メンテナンスが困難となる塩害トラブルを低減している。また、耐食性を評価する試験規格である国際規格 ISO14993に準拠し、塩水噴霧、乾燥、湿潤の耐久試験を繰り返すことで高品質な製品として、遠征を伴うネットワークカメラのメンテナンス業務低減を実現する。

●夜間視認性の向上と、光学40倍ズームレンズと仰角30度で広範囲を監視

高性能赤外線照明と可視光カットフィルタを搭載し、夜間における光源の影響を抑える。またWV-X6533LNSJは350m離れた先でも被写体に赤外線光を照射でき、昼間と遜色なく被写体に焦点を合わせることができる。光学40倍ズームレンズを搭載し、遠方はもちろん、左右方向は360度、仰角30度によりチルト可動範囲は-30度から210度までと、広範囲にわたり監視することが可能になる。

●ズーム揺れ補正機能による、高倍率ズーム使用時の揺れによる映像への影響の削減

WV-X6533LNSJはズーム揺れ補正機能を搭載しており、カメラ内部のジャイロによる揺れの検出に加え、画像ベクトル検出を併用してより高精度な補正を行い、映像への影響を最小限にとどめ、安定した監視映像を提供する。

●アドバンスド親水コーティングによる、雨天などの気象条件でも鮮明な映像を実現

レンズカバー部分に特殊なコーティングにより粒状の水滴となりにくくなり、鮮明な視界を確保する。さらに、レンズカバー表面に汚れがつきにくく、雨水が当たることで表面の汚れを洗い流す効果もあり、メンテナンスにかかる手間やコストを削減することもできる。

●その他

- H.265とスマートコーディングによるデータ高圧縮でネットワークへの負荷を軽減
- ギアドライブ式パン･チルト機構の採用し高耐久性を実現
- 「データセキュリティ･高信頼性」：認証局が承認したデバイス証明書をカメラ標準搭載
- 梱包箱を開けずにカメラの設定が可能な「かんたんキッティング梱包」を採用
- iA機能により、変化する周辺環境に合わせて自動で最適な画質に調整

※iA(インテリジェントオート)機能‥パナソニック独自機能で、視認が厳しい環境での識別性を向上させる。スーパーダイナミック機能の改善とシャッタースピード最適化で、移動する人や車の輪郭、ヘッドライトに照らされて光っているナンバープレートの識別性と、顔の位置を自動判別し明るさを調整することで背景の明るさが変化した時の顔の判別性を向上させる。

- IP66対応で、屋外の風雨が直接当たる場所にも設置可能
- IK10（IEC 62262）の高い耐衝撃性を実現
- 暗号通信、改ざん検知機能を搭載することでセキュア性を向上

データやSDメモリカードを持ち去られても漏洩をブロック（データの暗号化･改ざん検知）し、カメラからの映像を暗号化と電子署名に対応。

また、覗き見をシャットアウト(通信の暗号化)し、認証機関発行の証明書を使用したSSL通信を実現。

■製品URL‥

https://sol.panasonic.biz/security/camera/ipro_extreme/wv-x6533lnsj-s6532lnsj/

ウエスタンデジタル新製品情報

WD Purple 18TB HDD

本製品は、NVRと映像分析アプライアンス、およびリアルタイム分析とポスト分析アプリケーションの両方を提供するGPU対応デバイス向けに設計されている。現行世代より容量が28%増加した18TBドライブは、AIをより効果的にサポートするために、映像、リファレンス画像、メタデータをエッジに保存する容量を備えている。

8TBから18TBまでのWD Purpleドライブは、最大64台の高解像度カメラの録画を可能にし、ディープ･ラーニング分析用に追加の32台のストリームに対応するAllFrame AIテクノロジーを搭載している。

■製品URL･･

https://www.westerndigital.com/products/internal-drives/wd-purple-hdd

ハードウエアに対応するソフトウエア最適化

ウエスタンデジタルのWD Purpleドライブ向けHDDファームウエアの最適化とデータ管理機能は、システム能力の向上とAI対応スマートビデオソリューション全体のデバイス管理において極めて重要な役割を果たす。この組み合わせにより、性能、信頼性、耐久性が向上し、全体的に一層優れた運用効率とTCOが得られる。WD Purple HDD向けのAllFrame™テクノロジーは、データ損失を防ぎ、継続的なストリーム管理に対応するための広範なキャッシングとストリーミング管理技術を提供する。ウエスタンデジタルのHDD用ソフトウエアベース･ソリューションであるWestern Digital Device Analytics™は、ユーザに監視とドライブ解析機能を提供し、ドライブ上で問題となり得る状態を検出と、問題が発生する前に修復するための方法を提示する。

■製品URL･･

https://www.westerndigital.com/ja-jp/solutions/device-analytics

---

WD Purple SC QD101 1TB microSDカード

本製品は、AI対応カメラ、監視カメラ、およびエッジデバイス向けに設計されており、プライマリまたはバックアップ用データストレージとして機能する。ウエスタンデジタルの先進の96層3D NANDテクノロジーを採用しており、最大500 P/Eサイクルの超高耐久性を実現し、1TB、512GB、256GB、128GB、64GB、および32GBの各容量モデルを提供する。

堅牢で耐久性のあるWD Purple microSDカードは、耐候性、耐湿性に優れ、-25°Cから85°Cまでの温度に耐えることができる。対応カメラに搭載されたカードのヘルスモニターにより、設置業者やシステム構築者に対して、必要に応じて耐用時間や予備的な交換サービス情報を提供する。

■製品URL･･

https://www.westerndigital.com/ja-jp/products/embedded-removable-flash/surveillance-sd-microsd-cards

---

サンディスク ウルトラ microSDXC™ UHS-I カード　1TB

サンディスク ウルトラ microSDXC™ UHS-I カードシリーズに、今回1TBの大容量モデルが追加され、32GBから1TBの容量ラインナップとなった。

【主な特長】

1.最大100MB/秒の高速データ転送
2.UHSスピードクラス1（U1）とCLASS 10に対応し、フルHD動画の撮影に最適
3.アプリのパフォーマンスを快適にするアプリケーションパフォーマンスクラス1（A1）に対応
4.高い耐久性：防水、耐温度、耐衝撃、耐X線
5.10年間限定保証

■製品URL

https://shop.westerndigital.com/ja-jp/products/memory-cards/sandisk-ultra-microsd

ロジック・アンド・デザイン、画像解析補正ソフトウェアの販売を開始

本製品は、パソコン上で画像/映像の容易な高精細補正を可能にする解析補正ソフトウェア「LISr Image Filter(リサ･イメージ･フィルタ)。

LISr Image Filterは静止画に対する歪み補正や輪郭補正、明るさ補正、鮮明化補正、および動画に対する鮮明化処理を実施し、画像や映像の不明瞭な状態を改善して、詳細な判別を可能にする。

また、LISr Image Filterは、より高精細な画像補正のニーズに応えるため、画像解析補正や画像鮮明化のアルゴリズムを採用し、逆光や雨･霧等の悪条件下で撮影された画像や映像の鮮明化処理を可能にした。また使いやすいユーザ･インタフェイスにより、誰もがパソコン上の容易な操作で高度な補正を行うことができる。

■本製品の特長

･画像解析補正アルゴリズムに加え、画像鮮明化アルゴリズムの追加により、逆光や暗所、雨･霧等の悪条件で撮影された画像や映像の鮮明化処理が可能
･簡便な操作性(ユーザ･インタフェイス)で、パソコン上で画像や映像を簡単補正

■主な仕様

･OS･･Windows10 64bit版
･メモリ･･8Gバイト以上
･USB･･USB2.0 1ポート必須(コピーガード用)
･ディスプレイ･･(解像度)1280×720以上 (色深度)32bit True color
･CPU･･(最小規模)Intel(R) Pentium(R) 1.6GHz
(推奨規模)Intel(R) Core i5(R) 3.6GHz
･空き容量･･500Mバイト
･GPU･･NVIDIA(R) CUDA(R) 9.1対応のグラフィックスカード
*GPUは無くても動作可能
･必須ライブラリ･･CodeMeter ランタイム、
Microsoft Visual C++ 2015再頒布可能パッケージ、
上項GPUの最新ドライバ(GPU利用の場合のみ)

■販売価格･･オープン価格(取扱販売会社経由)

■LISr(リサ)について

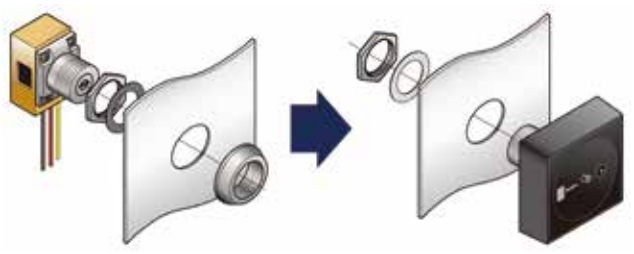
ロジック･アンド･デザインが開発したLISrは、画像加工技術ではなく、監視カメラ向けに特化した画像改善フィルタとして開発された画像鮮明化技術。

LISrは暗く沈んだ領域や白くとんだ領域、うっすらとコントラストが落ちた領域などダイナミックレンジが低い領域を検索し、その部分を特殊なアルゴリズムを用いて解析しています。領域の判断は画素ごとに行うため、逆光などの極端に明るい部分と暗い部分が混在していても画像全体のバランスを維持する。

LISrは、この原理をもとにノイズ対策やコントラスト対策をさらに強化した最新の画像鮮明化アルゴリズムを使用している。明るい場所は明るいなりに、暗い場所は暗いなりに処理を行えるので、24時間監視において悪天候や逆光、夜間と、刻々と環境が変化しても全自動で対応することを可能にした。

■URL･･http://www.lad.co.jp

KEIDEN、NFCカードリーダ SS-Reader2 キースイッチ取替型を発売



本製品は非接触ICカードやおサイフケータイをかざすことで、RFID技術で情報を照合し自動ドアや電気錠の解錠を行うNFCカードリーダSS-Reader2の新製品であるSS-Reader2キースイッチ取替型。既存のインターホンのキースイッチから加工を必要とせずカンタンに設置ができる。

■特長

･既存のインターホン(集合玄関機)のキースイッチを交換するだけで設置が可能
･既存のカギから簡単に交換可能
･本体だけで抹消、登録等の操作が可能
･Fe-Lockシリーズと共通のインターフェイスで簡単操作
･おサイフケータイ、FeliCa、MIFARE規格のカードがカードキーとして登録可能

■価格(税別)･･162,000円

■URL･･https://www.keiden-jp.com/index.html

NIKKEI MESSE
街づくり・店づくり総合展

IMAGINATION & CREATION

ニューノーマルの
デジタル戦略

リアル展示会とハイブリットで初のオンライン開催！

リテールテック JAPAN Online 2021

2021. 3.9(火)→12(金) ［主催］日本経済新聞社

オンライン展示場「NIKKEI NEON」上で開催

リテールテック OSAKA 2021

2021. 6.10(木)→11(金)
インテックス大阪 6号館 Aゾーン

http://www.retailtech.jp/

大阪展も出展者募集中

出展者募集中
申込締切日
2020年
12月25日(金)

［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　Eメール：info@retailtech.jp

第29回 セキュリティ・安全管理総合展

SECURITY SHOW Online 2021

出展者募集中

申込締切日：2020年12月25日（金）

リアルな展示会とハイブリッドで初のオンライン開催！

社会の安全・安心を守るテクノロジー





本資料に掲載の写真は2019年のリアル会場のものです。

展示分野

総合セキュリティ　防犯建物部品　センサー・アラーム　テロ対策　ホームセキュリティ　ネットワークカメラ&クラウド　AI・映像解析　災害対策　IoT・情報セキュリティ　店舗・オフィスセキュリティ　感染症対策マテリアル　感染症対策テック

2021年3月9日(火)-3月12日(金)

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

主催　日本経済新聞社

http://www.securityshow.jp/

Tel;03-6256-7355　info@securityshow.jp

NIKKEI MESSE 街づくり・店づくり総合展