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. 2019 no.72

特　　集：製薬業界のセキュリティは、業界保護に不可欠

secutech

2020年4月22日 – 24
台北南港國際展示館　ホール2
www.secutech.com

セキュリティ、IoT＆AIに関する アジアの先進的プラットフォーム

- Secutechは、アジア太平洋諸国からの多数の訪問者が来場し、新たなビジネスパートナーシップを生み、促進することができるハブ的役割を担います。
- メーカ各社が、販売代理店やシステム構築企業と連携し、またテクノロジー企業がOEM / ODMパートナーを見つける機会となる理想的なプラットフォームです。

同時開催イベント

SMAbuilding powered by Secutech
MOBILITY powered by Secutech
fire&safety powered by Secutech
info security powered by Secutech

messe frankfurt

比類なき映像技術で優れたパフォーマンスを実現

IDISのビデオソリューションは高級ジュエリーショップからデザイナーズ・ファッションブティック、そして世界中の高級ショップにおいて信頼あるセキュリティを提供します。
IDISは、サイバーセキュリティの最先端の技術を使用して 信頼性の高いたエンドツーエンド(E2E)ソリューションを提供します。
新製品の2MPマイクロドームカメラや受賞歴のあるSuper Fisheyeカメラによる画像分析、NVRそしてVMSソリューションに至りあらゆるニーズにお応えします。

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.

SÉCURE

www.idisglobal.com

目　次

広告索引

広告主名（ABC順）	掲載ページ
Fire & Safety	23
HIKVISION	5
IDIS	3
SECUTECH TAIPEI	表二
SECHTECH THAILAND	表三
日本経済新聞社	表四

次号案内　2019年 11/12月号（12月10日発行予定）

（誌面の都合上、変更になることがあります）

特　集
ナンバー･プレート認証

連　載
クラウドの利点と活用

a&s JAPAN ©ASJ合同会社　2019年 9-10月号　No.72
The Professional Magazine Providing Total Security Solutions

発行人　小森堅司　　DTP　サンフィール

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

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

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

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

顔認識によりインテリジェントな入退室管理

Hikvisionは、暗い環境であっても、迅速かつ信頼性の高いID検証を提供しています。世界的に有名なセキュリティーテクノロジーと強いR&Dチームに基づいて開発されたHikvisionのディープラーニング顔認識システムは、入退室管理業界の新たな標準を定めました。顔認識、IDカード、指紋など多様な組み合わせを選択し、独自の応用環境に応じて安全レベルを自由にカスタマイズできます。顔認識技術によって、ユーザー認証はより安全で信頼性が高くなり、検証済みのユーザーのみ入室を許可し、それ以外の不正行為を排除します。シンプルかつ直感的な操作とスリムなデザインを揃え、あらゆるプロフェッショナル環境で最も便利なIDスキャナーです。

日本代理店

Security DESIGN	D’s Security Tel	Jsecurity inc.
Tel 03-6230-3021	03-6661-6116	Tel 03-6806-0343
www.security-d.com	www.dss.co.jp	www.jsecurity.jp

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。

映像監視のための新GDPRガイドラインの検討

チャールズ・ロレット　著

https://ipvm.com/reports/gdpr-edbp

最高水準を誇るEUデータ保護機関のGDPRは、暫定的な映像監視のガイドラインの新編を発行した。DPRは発足後1年以上経つが、GDPRが設定した映像監視ガイドラインが映像監視システムにどのように適用されるかは不明確だ。

現在、この新しいガイドラインは最終的なものではなく、今後2か月間のパブリックコメントの対象となり、映像監視GDPRコンプライアンスに関する一般的な質問に対する優れた洞察を明らかする。

本稿では、新しいガイドラインについて説明し分析する。

●EDPBの背景
●ガイドラインの法的影響
●パブリック・サイネージ例の提供
●サインの配置
●大規模な生体認証に必要なDPIA
●ストレージ：3日間以上の記録期間を必要とする理由
●生体認証とは見なされない分析
●VIP認定：VIPだけでなく、全員からの同意が必要
●顔認識：サイネージによる通知が十分でない可能性がある理由
●データ要求/匿名化
●暗号化の種類に関する明確さの不要化
●保証対象外
●GDPRの対象外となるダミーカメラ

登録受付中-2019年10月IPネットワーキング・コース

https://ipvm.com/reports/ip-networking-course

業界をリードするIPネットワーキングブックを使用した12のセッションで、映像監視に影響するIPネットワーキングの基礎を解説する。

(1)帯域幅
(2)アドレス指定
(3)ネットワーク・ハードウェア
(4)PoE、VLAN、QoS
(5)プロトコル
(6)ネットワーク配線
(7)インストール
(8)リモート・アクセス
(9)サイバー・セキュリティ
(10)ハッキング
(11)ワイヤレス
(12)ネットワーク管理

ファーウェイ・ハイシリコン社製半導体を搭載しているかを知る方法

イーサン・エース　著

https://ipvm.com/reports/hisilicon-check

IoT機器の中核であるにもかかわらず、メーカが使用するSoC（チップ上のシステム）を公開することはほとんどない。これに対する関心は、一般にサプライチェーン・リスクと、米国NDAA禁止を含むファーウェイ社製品使用に関するより具体的な議論が高まっている。本稿では、ユーザが自分自身を調査できるように、一般的なカメラ内のSoCを見つけてアクセスする方法を示す。

●カメラ内でチップが見つかる場所
●カメラにより異なる分解と再組み立て
●カメラを分解するリスク
●サンプルカメラで使用されるSoC

チップの場所

カメラのSoCの正確な場所はモデルごとに異なります。IPVM本文にリンクしたビデオでは、アクシス社、HIKVISION社、UNIVIEW社のカメラを見て、SoCの場所とアクセス場所、およびそれぞれが使用しているものを示している。

分解と再組立の違い

上に示したように、幾つかのチップは数本のネジを外すだけで簡単に取り出すことができるが、小さなセキュリティ・ドライバーと複数のデリケートなケーブルの切断が必要なチップもある。ここで例として使用されているカメラのうち、アクシス社製カメラはアクセスが最も簡単で、カメラ・モジュールを取り外すのに数本のネジの取り外しが必要で、SoCの下部に目立つラベルが付いている。

ただし、HIKVISION社およびUNIVIEW社モデルでは、複数のマルチピン・コネクタを取り外す必要があった。これには、非常に細いワイヤを使用するメインボードに撮像素子を接続するコネクタが含まれている。これらを取り外した後、SoCを下に置いて、カメラのメインボードを裏返すために、いくつかの小さなネジを取り外す必要があります。

分解リスク

カメラを分解する前に、ユーザはその際に2つの重要なリスクを考慮する必要がある。

●**無効の保証**・・カメラを分解すると、ほとんどが漠然と定義された「誤用」をカバーしないため、保証が無効になる場合がある。修理中にデバイスに損傷を与えた場合、ユーザは将来の修理のために現金を支払う必要がある。
●**壊れたカメラ**・・一部のカメラを分解するのは面倒なプロセスだ。コンポーネントを相互接続するために使用される小さなゲージ・ワイヤは、マルチピン・コネクタから外れてしまい、センサが誤動作したり、IRが機能しなかったり、フィルタが1つの位置に留まったままになる傾向がある。

HIKVISION社製4Kカメラを突撃テスト

イーサン・エース　著

https://ipvm.com/reports/hikvision-4k-shootout

HIKVISION社は、最新のスマート・シリーズの5つのカメラを使用して、「高性能および業務用アプリケーション向けの最新技術」が「完全に搭載された」カメラであると主張している。しかし、これは、同様の機能セットをはるかに低価格で主張している低価格のパフォーマンス・シリーズや、4K/8MP固定レンズの銃撃戦で勝利した低価格のバリュー・シリーズと比較した場合どうか?

性能を比較するために、スマート・シリーズDS-2CD5585G0-IZHSとパフォーマンス・シリーズDS-2CD2785G0-IZS 4Kカメラの両方を購入して、旧世代のDS-2CD4585FWD-Iとバリュー・シリーズDS-2CD2383G0-Iをテストした。比較項目は以下の通り。

●これらの新しいモデルは、旧世代およびバリュー・シリーズ・モデルと比較して違いは何か?
●スマート・シリーズとパフォーマンス・シリーズの比較
●フルライト（～400lx）、ローライト（～2lx）、ダーク（～0.02lx）シーンでの機能は?
●H.265 +の帯域幅を比較すると?
●インストールは他のドーム型モデルと比較してどうか?

これは、ボッシュ社製Starlight 8000iおよびHanwhaテックウィン社製Wisenet Pに続く、一連の更新された4Kカメラテストの最新版で、AVIGILON社やAXIS社、DAHUA社やVIVOTEK社などが間もなく発表する。もし他にどの4Kカメラをテストすべきかご存知であれば教えていただきたい。

ペルコ社CEOが退任、新CEOを模索中

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/pelco-ceo-19

2019年5月にペルコ社が売却されてからわずか数ヵ月後、同社CEOは退任し、新たに業界内から新しいCEOを探しているとペルコ社オーナーはIPVMに語った。本稿では、次のシュナイダー・ペルコの変更点、利点、および新しい同社CEOになるべき人物について説明している。

ジーン・マーク・セオリオ氏は、ペルコ社CEOをわずか2年経験しただけだったが、20年以上にわたりシュナイダー・エレクトリック社で勤務していた。様々な情報源によると、業界門外漢だがシュナイダー出身である彼はペルコ社内で尊敬されていた。そして彼は、2017年にペルコ社CEOに就任した時に多くの人が目標として考えていたことを確実に達成した。

ペルコ社の新社長はブライアン・マクレーン氏である。同氏は、ペルコ社新オーナーのトランソン・キャピタル社が送り込んだ。トランソン・キャピタル社が買収して以来、マクレーン氏はCOOだったが、セオリオ氏が退任した現在はCEOに就任している。ここで最も重要なことは、マクレーン氏は以前トランソム社のポートフォリオ会社であるラウド・オーディオ社CFOだったため、トランソム社に自信を持っていることだ。

シュナイダーからの独立

独立したペルコ社は独自のシステムとプロセスを構築する必要があるため、シュナイダー社から分離するには、それ自体で多くの作業が必要となる。

独立のプラス面は、ペルコ社が独自の決定を行えるようになることだ。これまで長年にわたってシュナイダー社が指示していたのだろうが、ペルコ社の判断と行動を遅延させていた大きな問題だった。もちろん、これは巨大なコングロマリットのアプローチになる傾向があるため、シュナイダー社固有の問題ではない。例としてハネウェル社とUTC社の関係を参照していただきたい。ただし、シュナイダー社のペルコ社への影響ほど悪くはない。

VIVOTEK社の収益が急増

ジョン・ホノヴィッチ　著

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

VIVOTEK社の収益は2019年に急増して、45%も増加している。本稿では企業収支記録を調べ、同社の成長を促進を支えている要因と、同社最新の顧客がオンラインであることを見つけた。また、VIVOTEK社の成長を台湾の映像監視メーカと比較し、注目すべき違いを明らかにした。

事業計画書の要約

VIVOTEK社の売り上げは2018年に1億6500万ドルを達成し、2019年には2億4,000万ドルを達成するペースで進んでいる。興味深いことに、同社の2つの上位ODM顧客は、閉鎖型システム構築者のMeraki社とVerkada社だ。Meraki社とVerkada社の両社とも独自のファームウェアとソフトウェアを開発しているため、真のODMである。

VIVOTEK社はまた、新しいOEM顧客であるハネウェル社によって業績増加が後押しされ、とりわけ「30シリーズ」が追加されるため、米国企業であるハネウェル社は、米国政府が禁止していないIPカメラを一部だがそろえることができた。しかし、他の製品シリーズはDahua社からOEM調達している。

輸入業者の内訳

以下は、決算収支書から収集した、過去12か月間（2019年8月から2019年7月まで）のVIVOTEK社の米国の主要輸入業者の内訳だ。

Customer	SUM of GROSS
AIR TIGER EXPRESS (USA), INC.	4,234
Avigilon	62,315
CLOUD NETWORK TECHNOLOGY USA	2,917
DCL	4,442
Meraki	114,055
Pelco	1,195
PRIORITY WORLDWIDE SERVICES	6,802
TRENTON TECHNOLOGY INC	52,219
TVCenlinea.com	14,209
VERINT SYSTEMS INC.	15,149
Verkada	137,190
Vivotek USA	265,329
Grand Total	**680,056**

DAHUA社、自社ソフトウェアを米国ペッパー社製品に置き換え

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/dahua-pepper

米国政府が取引禁止にした企業は、米国セキュリティ業界の立場位を改善するために何をしたか?

DAHUA社は米国に拠点を置くペッパー社提携して、新しいソリューションを発表した。プレスリリースの内容だけでは誤解を招く恐れがあるので、本稿では、DAHUA社とペッパー社の両社と個別に話し合った後、アプローチが何であるか、その主な利点とその主要な制限について解説する。

リリース内容

ペッパー社製プラットフォームと統合することにより、DAHUA社製ハードウェアは、包括的で安全な機能に基づいたサービス・フレームワークの一部になる。米国で提供されるDAHUA社製品の場合、全てのデータおよび映像通信は米国内で処理されて、ペッパー社の厳格なサイバー・セキュリティおよびデータ・プライバシー基準に準拠する。DAHUA社の法人顧客向けに、ペッパー社のパートナーシップは、エンドユーザに映像および非映像IoTサービスを配信するように設計され、市場に提供されるプラットフォームとソフトウェア機能のセットへのアクセスを提供する。

消費者向けは?

DAAHUA社とペッパー社両社は、リリースでDahua製品全般、具体的には「法人顧客」について語っているが、少なくとも現段階ではそうではないことを明らかにした。DAHUA社の説明は以下の通りだった。

パートナーシップの公式および最終決定により、最初の焦点である消費者製品ラインに目を向けると、今後の市場投入戦略については、両当事者間の追加の議論を通じて決定される。特に、ペッパー社は、DAHUA消費者向けブランドのImuuライン(以前はLeChange)は「ペッパー社入り」になると指摘している。しかし、両社ともDAHUA社で最も広く販売されている米国市場向けLorexについて、過去1年間で米国に輸入された量について明確にしていなかった。

ペッパー社の概略

同社は2017年3月に850万ドルのシリーズB資金を元手に米国カンザスシティに設立された従業員25名を擁する新興企業。企業規模は小規模だが、この分野に特化しており、他の多くの非公開IoTカメラプロバイダーを顧客としている。

ボッシュ社、ソニーの映像セキュリティ販売とマーケティング・チームを統合

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/bosch-sony-int

ソニーの映像監視事業の将来はどうなる?2016年、ボッシュとソニーは非定型的な「パートナーシップ」を発表した。現在、ボッシュはIPVMに、ソニーの販売チームとマーケティングチームを統合していると話している。本稿は、ボッシュ社の声明、ソニーの課題、および映像監視におけるソニーの将来について検証する。

統合

ソニーとの大きな変化に関する現地報告に応えて、ボッシュ社はIPVMに次のように述べている。

「ソニーの映像セキュリティ販売およびマーケティング・チームは、グローバルなボッシュの販売組織に統合されている。この統合により、ボッシュ・ブランドのセキュリティと安全性の完全なポートフォリオをソニーの顧客にも拡大している。今後、ボッシュとソニーの顧客には、セキュリティとそれを超えた製品ポートフォリオの全範囲を提供できる、1つの共同販売およびマーケティングチームがある」。

以前は、ボッシュ社はソニーの販売とマーケティングとは別々に活動していた。そのため、特定のソニー営業担当者に加えて、ソニーの販売代理店があった。ボッシュ社は、ボッシュ/ソニーの社員とソニー製品販売代理店は残ると話している。ボッシュ社はまたIPVMに対して、ソニーが自社製映像セキュリティ販売を削減したり終了したりしていないことを強調している。

利点・・その他のリソースへのアクセス

明確な利点の1つは、ボッシュや他の多くの業界の主要企業と比較して、ソニーが販売およびマーケティングのリソースの不足に苦しんでいたことだ。ソニーの「唯一の」リソースを大幅に拡大する場合を除き、現状の組織は小さすぎて、より大きなフィールド組織と効果的に競争することはできなかった。ボッシュ社に直接参加することで、より多くのリソースを獲得できる。

HIKVISION社 OEM先情報

IPVMチーム　著

https://ipvm.com/reports/hik-oems-dir

本情報は会員以外にも公開する情報

中国政府が所有し、米国政府が取引禁止したHIKVISION社は、世界最大の映像監視メーカであり、OEM供給を通して多くの欧米企業に一般的に隠れたプロバイダとなっている。

以下のディレクトリには、HIKVISION社の一部製品をOEM提供で受けている60社以上の企業が含まれており、IPVMの本文には、ロゴマークと企業Webサイトへのリンクが含まれている。ほとんどの業界団体や協会はHIKVISION社 OEMをカバーしていない。また、ほとんどの協会は内部情報を公開していないため、出荷記録、製品ドキュメント、またはテスト製品を調べて確認したものだけを掲載している。

このリストまたは追加する他のリストに関するフィードバックがある場合は、info @ ipvm.comに電子メールを送信していただきたい。

- 2M CCTV
- 3xLogic
- ABUS
- Activecam
- ADJ
- Advidia (Video Insight / Panasonic brand)
- Alarm.com
- Alibi (Supercircuits)
- Allnet
- Alula
- Anaveo
- Annke
- Arcdyn
- Armix
- Avue
- Cantek
- CCTVStar
- DMP
- DSS
- Dunlop
- DVR Unlimited
- Epcom
- Esypop
- Ezviz
- Global Network Security
- GovComm Intelligent Transportation Systems
- Grundig
- GVS Security
- Hinovision
- Hitosino
- Hunt CCTV
- Hyundai Security
- Infinite Pixels
- Inkovideo
- Innekt
- Interlogix (UTC)
- Invidtech
- IP Cam Talk
- JFL
- Jlinks
- LaView
- LTS
- Matrix Security Solutions
- MicroView
- Nelly's Security
- Norelco SafeCam / Spider Vue / Invezia
- Northern (Tri-Ed / Anixter)
- Novicam
- Oculur / A1 Security Cameras
- Onix
- Pnet
- Power Technology
- Raster
- RVi
- Safety Vision
- Safire
- Scati
- SecurityTronix
- Sentry CCTV
- Siqura / TKH
- SnapAV / Luma
- Space Technology
- Syscom
- Technomate
- Trendnet
- Vantage Security
- Vezco CCTV
- Videoteknika
- Winic
- Xyclop
- Zicom

生体認証利用統計2019

ブライアン･ローズ　著

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

150人以上のシステム構築者が、生体認証を使用する頻度と時期そして理由を説明した。本稿では、その傾向と主な理由また反対する主な理由を検証する。

大半のシステム構築者は、63%が全く生体認証を使用することがないと答えている。

使用が制限されている最も一般的な理由としては、

●顧客の要求なし　●高すぎる

●カードよりも優れていない

●スループットが遅すぎる

●信頼できない/悪い経験がある

スプリーマ社の生体認証情報漏洩を検証

ジョン・ホノヴィッチ　著

https://ipvm.com/reports/suprema-leak

Supremaが物理セキュリティ市場で議論されることは滅多にないが、韓国の生体認証企業は先般トムズ・ハードウェアからビジネス・インサイダー、さらにはBBCまでニュースを流した。

しかし何が起こったのか?本稿では次の項目を解説する。

●漏洩内容と方法

●影響を受けるスプリーマ社ユーザと影響を受けないユーザ

●スプリーマ社がクラウドサービスに関して行った重要な虚偽の主張

●この漏洩を招いた2つの基本的な問題-露出されたバケットとロギング

●メディア・リポートで行われたリークに関する主張

●指紋記録「盗難」のリスクの調査

●潜在的なGDPRリスクと関連する罰金

●スプリーマ社企業情報、収益、時価総額、株価変動

研究者レポート-vpnMentor

本質的に同じ投稿を実行しているメディアは多数あるが、決定的な情報源はvpnMentorからのものである。

リポート内容：何百万人ものユーザに影響を与える生体認証セキュリティ・プラットフォームのデータ侵害。レポートには、漏れた内容を示す85秒のビデオが含まれている。

警告!Windows 7のアップデートでNVRがクラッシュする

ブライアン・ローズ　著

https://ipvm.com/reports/win7-nvr

Windows 7をアップデートすると、アップデートの実行後、影響を受けるシステムは通常どおり起動せず、代わりに警告画面を表示する。本稿では下記について解説する。

●影響を受けるシステム

●問題の原因は何か?

●修正すべきベンダーの推奨事項

●DahuaとHikvision製品は影響を受けない

●Windows 7の寿命が近づいている

●これはVSaaSの勝ちを示しているのか?

IPVMは、Microsoftセキュリティ・アップデートKB4512506をインストールした後、起動しなくなるWindows 7およびWindows Server 2008R2システムのレポートを複数受け取った。問題は、このアップデートでは現在必要なSHA-2署名を使用しているが、組み込みOSサーバとNVRがSHA-1からアップグレードされたと誤って認識しているために発生する。

18以上のネットワーク・スイッチ・ベンダーで見つかった重大な脆弱性

ジョン・スカンロン　著

https://ipvm.com/reports/realtek-bashis

シスコ社、ネットギア社をはじめアジアの小規模ブランドを含む12を超えるブランドが、同じ重大な脆弱性を共有していることが判明した。最も重要なことは、ほとんどが同じ基本的なソフトウェアとハードウェアを共有しているサプライチェーンのリスクを示している。本稿では、次の項目について報告している。

●脆弱性の概要

●Realtek社の応答

●影響を受けるメーカ

●なぜ多くの企業が脆弱なのか

●セキュリティ業界への影響

●サプライチェーンのリスク

リアルテック社製スイッチ・コントローラ

様々なメーカが全て同じ中央構成部品としてリアルテック社スイッチ・コントローラ RTL83xxを採用している。どのメーカにもこの脆弱性を検出できなかった共有コア・ソフトウェアが含まれている。各メーカは、製品に添付されていたリアルテック社製SDKを使用していた。そのSDKには、リモート・コード実行に対応するスタック・オーバフローを含むいくつかの脆弱性があり、概念実証では、管理者レベルの資格情報へのアクセスの追加も削除もできる。

NEC、アサヒ飲料とクラウド型カメラ付自動販売機を共同開発

https://jpn.nec.com/press/201908/20190830_01.html

今回発表した製品は、地域の防犯･安全に貢献するため、防犯カメラの設置を検討している自治体や小売り、デベロッパ向けのクラウド型カメラ付自動販売機「まちを見守る自販機」で、NECの「映像クラウドサービス」を活用している。通常の自動販売機に小型カメラを搭載し、付属の通信機器により映像をクラウド上へ自動的に保管できる仕組みを採用している。

従来、防犯カメラを設置するには、機器選定や設置手配などの手続き、また、設置後のメンテナンスや有事の際の警察への映像提供といった映像管理が手間となっていたが、「まちを見守る自販機」の設置オーナーは、これら手間のかかる手続きや映像管理が不要となる。

なお、自動販売機の設置にあたっては、上部および正面にカメラ付自動販売機であることが分かる告知ボードを設置する。

法務省、パナソニック製「顔認証ゲート」の運用を拡大

https://news.panasonic.com/jp/press/data/2019/08/jn190830-3/jn190830-3.html

法務省出入国在留管理庁は、パナソニック社内分社であるコネクティッドソリューションズ社が開発したパナソニック製「顔認証ゲート」を、2017年10月から採用し、既に全国5か所の空港（羽田、成田、中部、関西、福岡）で、計137式を運用している。

さらに2019年度は、7月24日の羽田空港を皮切りに、新千歳空港（11月中旬運用開始予定）および那覇空港（2020年7月上旬運用開始予定）を加え、全国7か所に追加での66式、計203式の導入と、外国人の出国手続への拡大を図っている。外国人用の出国手続には合計123式が運用される予定。

令和元年７月２日
出入国在留管理庁

顔認証ゲート導入空港一覧（令和元年度）

空港	平成３０年度までの設置台数(A)			令和元年度設置予定台数(B)			総台数 (C)=(A)+(B)			外国人出国手続への活用に係る運用開始予定日
	上陸	出国	小計	上陸	出国	小計	上陸	出国	合計	
成田空港	31	30	61		9	9	31	39	70	2019年8月27日（火）
羽田空港	10	13	23	4	10	14	14	23	37	2019年7月24日（水）
中部空港	6	9	15	3	7	10	9	16	25	2019年11月7日（木）
関西空港	12	15	27	3	11	14	15	26	41	2019年9月25日（水）
福岡空港	5	6	11		2	2	5	8	13	2019年10月8日（火）
新千歳空港			0	3	6	9	3	6	9	2019年11月中旬
那覇空港			0	3	5	8	3	5	8	2020年7月上旬
合計	64	73	137	16	50	66	80	123	203	

ジェネテック社、Bosch社とMOBOTIX社とEUKLIS社製カメラ向けStratocastのサポートを発表

https://www.asmag.com/showpost/30556.aspx?name=news

ジェネテック社は、Microsoft Azureによるクラウド･コンピューティング･プラットフォームを搭載したクラウド･ベース･サービスとしての映像監視（VSaaS）であるStratocastが、BOSCH社とMOBOTIX社とEUKLIS社製新しいカメラ･モデルをサポートしたことを発表した。

Stratocastは、オンプレミス監視システムのインストールと管理に関して通常伴う費用と複雑さを解消して、信頼性が高く費用効果の高い映像監視ソリューションを必要とする企業組織の要求を満たすように設計されている。小規模な設置場所や遠隔地に映像監視を簡単に導入したい企業や中小企業のユーザに真のクラウド･ソリューションを提供する。Stratocastは、全てを徐々にクラウドに移行しながら、特定のオンプレミス･ストレージおよびハードウェア基盤を維持したいユーザ向けのハイブリッド･クラウド展開もサポートする。

Stratocastオープン･アーキテクチャにより、サポート機器のポートフォリオも継続的に拡大しており、アクシス社やVIVOTEK社の既存の数百ものモデルのサポートに加えて、BOSCH社とMOBOTIX社とEUKLIS社製のカメラをサポートする。

アバスト社、GPSトラッカーのセキュリティ上の欠陥を発見

https://www.avast.co.jp/index#pc

今回発見した欠陥は、Shenzhen i365 Tech社のGPSトラッカー「T8 Mini」と同社製の約30機種のセキュリティ上の深刻な脆弱性。リアルタイムの正確なGPS座標など、送信された全てのデータがクラウドに流出する可能性がある。さらに、設計上の欠陥により、第三者が位置情報を覗き見することや、マイクにアクセスして盗聴することも可能。アバスト脅威研究所の研究者は、保護されていないGPSトラッカーが世界でおよそ60万台使用されていると推定しており、こうしたIoTセキュリティの問題は、単一ベンダの責任範囲を超えていると指摘している。

アバスト社では、こうした製品の購入者に対し、より信頼性の高い企業ブランドの提供する、製品設計にセキュリティ機能を組み込んだ代替製品を選択するよう推奨している。また、全ての市販機器と同じく、初期設定の管理者用パスワードをより複雑なものに変更することを推奨している。それでも悪意のある個人が暗号化されていないトラフィックを傍受するのを防ぐことは不可能だとも述べている。

「初期設定のまま」は危険

アバスト脅威研究所はまず、http://en.i365gps.com からGPS製品と連携するモバイルアプリをダウンロードする指示に従い、T8 Miniの設定プロセスを分析した。注目すべき点として、このwebサイトはセキュリティの高いHTTPSではなく、HTTPプロトコル経由で提供されていた。その際、ユーザは割り当てられたID番号と「123456」という非常に一般的な初期設定のパスワードでアカウントにログインできる。この情報も、セキュリティの不十分なHTTPプロトコルで送信されていた。

ID番号は、デバイスの国際携帯機器識別番号（IMEI）に由来したもので、同社製の他のGPSトラッカーについても、アバスト社研究チームがID番号を予測・模倣することは容易だった。基本的に全ての機器は、こうしたIMEI番号の並びを踏襲しており、パスワードも固定なため、苦労することなく侵入することができると考えられる。

すべての情報が非暗号化

アバスト社研究チームが、シンプルなコマンド参照ツールを使用して発見した事実として、GPSトラッカーのwebアプリケーションから発信された全てのリクエストは、非暗号化の平文で送信されている。さらなる懸念材料として、こうした機器はGPSトラッキングの本来の用途以外にも下記の目的で使用できる。

- **電話番号の発信**・・GPSトラッカーのマイクを通じ、第三者は盗聴が可能。
- **SMSメッセージの送信**・・機器の電話番号を特定し、攻撃手法としてSMSを使用することや、デバイスから代替サーバへと通信ルートを変更することができる。
- **トラッカーへのURLの共有**・・遠隔地の攻撃者は、手を触れることもなく、機器に新たなファームウェアをダウンロードさせることができる。

Google PlayとiOS App Storeの両方で提供中のモバイル・アプリAIBEILEも、非標準のHTTPポートであるTCP:8018経由でクラウドとの通信を行っており、非暗号化の平文をエンドポイントに送信していることが判明した。アバスト脅威研究所がデバイス本体を分解し、クラウドへの通信状況を分析したところ、無許可で非暗号化のまま、GSMネットワークからサーバにデータ送信されていることを確認した。

T8 Mini GPSトラッカーで発見されたセキュリティ上の欠陥に関する詳細については下記を参照。

https://decoded.avast.io/martinhron/the-secret-life-of-gps-trackers/?fbclid=IwAR1Sd3xXk3zMcneLVyZwZBi9UT9Bt-hqvaqkuzK7whhmThSXORaIHD4Y14c

---

アクロニクス・ジャパン、本社を移転

https://www.acronis.com/ja-jp/

市場におけるサイバープロテクションの標準の確立をサポートするアクロニクス・ジャパンは、本社を下記に移転した。

〒106-6137
東京都港区六本木 6-10-1 六本木ヒルズ森タワー37階
TEL：03-4572-2500　FAX：03-4572-2501

Wi-Fi Alliance、新たなWi-Fi認証プログラム「Wi-Fi CERTIFIED 6」を提供開始

https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6

今回提供開始したWi-Fi CERTIFIED 6は、Wi-Fi のエコシステム全体を通じて容量、パフォーマンス、レイテンシが大幅に強化されているほか、様々なベンダから提供する製品が適切に連携し、優れたイノベーションと機会を提供する。

Wi-Fi CERTIFIED 6は、厳格な要件が求められるエンタープライズ環境のピークパフォーマンスから低消費電力・低レイテンシのホームネットワークや産業IoT環境に至るまで、多様なデバイスとアプリケーションをサポートする。また、Wi-Fi CERTIFIED 6は、Wi-Fi 5の4倍近い容量を実現しているだけでなく、ネットワーク上の全てのデバイスに最適化した接続環境とハイ・パフォーマンス・インフラストラクチャを同時に提供し、高密度のWi-Fi環境における接続体験の向上をもたらす。

Wi-Fi CERTIFIED 6は、次のような先進機能を提供している。

●**直交波周波数分割多元接続（OFDMA）**・・チャネルを効果的に共有することで、高い要件が求められる環境下でアップリンク/ダウンリンクの両方で高いネットワーク効率と低いレイテンシを実現する。

●**MU-MIMO（マルチユーザーMIMO）**・・一度に大量のダウンリンク・データを伝送できるため、AP(アクセス・ポイント)は数多くのデバイスにデータを同時に伝送することができる。

●**160 MHzチャネル**・・帯域幅を高め、低レイテンシで優れたパフォーマンスを提供する。

●**TWT（ターゲット ウェイク タイム）**・・IoTデバイスなど、Wi-Fiデバイスのバッテリー寿命を飛躍的に延ばす。

●**1024-QAM（1024直角位相振幅変調）**・・同じ帯域幅でより多くのデータをエンコードすることで、Wi-Fiデバイスのスループットを高める。

●**送信ビームフォーミング**：指定範囲内での高いデータレートによって、ネットワーク容量の向上を実現する。

なお、2019年から日本国内で試験運用している5Gとの関係については、相互補完性が高く、特にWi-Fi 6が運用面とコスト面でサポートする点を挙げている。

1周年を迎えたOSSA

https://www.asmag.com/showpost/30569.aspx?name=news

セキュリティ、安全、およびビル・オートメーションなど分野の革新的な組織であるOSSA(Open Security&Safety Alliance)は、最初の12か月以内に、危機メーカ、ソフトウェア開発者、システム構築企業、販売会社、システムオンチップ（SoC）企業など、30社以上の会員メンバーが参加して、このたび1周年を迎えた。

OSSAヨハン・ジュベガ会長は、「OSSAを通じて、競合他社の補完的な機関がブランドの壁を越えて、業界全体を新たな、より繁栄した効率的な方向に押し進めるために協力している。30年以上の有名企業で構成されるオープンなセキュリティと安全性のエコシステムを確立し、市場を変えるデジタル製品の映像カメラを初めて供給開始したことで、最初の1年で達成した進歩に本当に満足している。当連合、ユーザのためによりインテリジェントで生産的なソリューションを促進するために、共通の標準仕様文書と解釈を提供し続けている」と述べている。

現在、セキュリティと安全性のソリューションは断片化されており、より大きな成功を収めるために連携して動作するシステムへの共同アプローチはまだ存在しない。蓄積されたシステムには大量のデータが残されており、協力することで、より良い生活、安全、セキュリティの目的に利用することができる。

OSSAの使命は、製品とソフトウェア、サービスの開発と展開と運用、およびメンテナンスに関して、全ての企業が同じ「レシピ」から始めることだ。連合の目標は、セキュリティおよび業界の大部分が共通のベンダに依存しないOS(オペレーティング・システム）およびIoT基盤と連携し、データ・セキュリティ、プライバシー、製品などの一般的な課題に対して定義された一般的なアプローチを、実装または遵守することに同意することだ。複数のソリューションにわたる性能とデータの簡単な活用により、OSSAが定めた基盤の上に構築されたセキュリティおよび安全ソリューションに関して、使いやすさと信頼が大幅に向上する。そこから、企業は、連携型のデジタル市場を通じてアプリを介して差別化することができる。

1年目の顕著な進歩

発足後1年以内に、OSSAメンバー企業は、セキュリティ映

像機器用の共通OSの定義を含む最初の共通の基本的なデータ構造を作成した。また、デジタル市場を含む共有IoT基盤の一般的なアプローチと確立を定義し始めた。このフレームワークにより、あらゆるブランド機器でキャプチャされたデータを開放し、適切な目的で利用できるようになった。また、セキュリティおよび安全装置、システム、設定を考案、展開、保守する際の負荷を減らし、データの解釈と可能性への扉を開くことで革新を促している。このようにOSSAが構想するこのプラットフォーム革命は、参加企業全員に利益をもたらしている。

具体的な成果

この1年間で得られた重要な成果は下記の通り。

●ベンダに依存しない一般的なOSの定義を含む、共通の技術的な基本データ構造の文書化。特にデータ・セキュリティとプライバシーに対する一般的な市場アプローチの最初の説明。

●OSSAのメンバーであるSecurity and Safety Things GmbH（SAST）は、OSSAによって定義された共通の技術的な基本データ構造に記載されているOSの最初のバージョンを実現し、プロトタイプ・カメラの作成を可能にした。商用化プラットフォームの発売は2020年第1四半期を予定している。

●OSSAの発起人である5社であるボッシュ・ビルディング・アドバンスド・テクノロジ社、Hanwha テックウィン社、マイルストーン・システムズ社、ペルコ社、VIVOTEK社の他に、25社以上の独創的な国際企業が参加している。OSSAに参加するメリットには、連合のフレーム・ワークへの関与や、他の連合企業との連携や協議など、業界を改善するための変化を導く機能がある。

Razberi社とIronYun社、AI映像監視プラットフォームで提携

https://www.asmag.com/showpost/30500.aspx?name=news

AIベースの映像監視ソフトウェア企業IronYun社と、オープン・プラットフォームの映像監視ハードウェア企業Razberi 先端技術社は、技術提携を締結した。

IPカメラの導入により、物理セキュリティがネットワーク帯域幅の負担になっている。セキュリティ応答時間は、生と死の違いを意味する。Razberコアのような高品質の監視ストレージ・サーバがなければ、脅威を特定するために使用される4メガピクセルの映像を保存して迅速に取得するために必要な技術は実現できない。

Razberiコアは、集中型映像録画、強化されたサーバ・クラスのアプライアンス、およびサイバー・セキュリティ保護を必要とする業界向けのIronYun社製先端技術ソリューション。IronYun社の最も要求の厳しいセキュリティ顧客には政府および軍事産業などがいる。

次世代型人工知能映像監視ソフトウェア企業IronYun社は、2019第3四半期にRazberiコアのサーバ・ストレージを使用した映像監視ソリューションの展開を開始した。

Secutech Vietnam 2019の注目点は、産業および建物向けのソリューション

https://www.asmag.com/showpost/30534.aspx?name=news

IoTは、機器とサービスを統合するだけでなく、特に安全やセキュリティそして消防の分野で事業を統合している。このことは2019年8月14日から16日までの日程でベトナム社会主義人民共和国ホーチミン市で開催されたSecutech Vietnamで実証された。出展企業380社と14,239名の来場者が商談を繰り広げ、最新製品情報を収集した。21の国と地域の企業が出展し、多くの人がスマート・ソリューションの市場はますます競争が激しくなっていると発言している。

また、開催中におこなわれた会議のテーマは、市場の最新情報、政府の政策、セキュリティ、管理効率、IoTアプリケーション、そして火災安全性にまで及んだ。特に、火災安全の専門家のために、防火ソリューションに特化したセミナーでは、多くの業界からの洞察が披露された。講演者には、ベトナム消防警察署と韓国消防院の代表者が参加し、規制、UL認証、複合ビルの防火、インテリジェントアラームシステムなどについて議論した。

Secutech Vietnamは、メッセ・フランクフルト・ニューエラ・ビジネス・メディア社とベトナム展示会主催会社であるJSC社が共催している。次回は2020年8月20日から22日までホーチミン市のSECCで開催される。

4Kカメラシステムを選択する必要があるのか?

https://www.asmag.com/showpost/30561.aspx?name=news

言うまでもなく、映像監視の主要な傾向は4Kであり、これには長所と短所がある。ユーザがセキュリ·ティシステムを選択する際に4Kにアップグレードするかは、利用条件と要件により異なる。

映像放送では、超高解像度(UHD)映像の概念が勢いを増しており、メーカは4Kおよび8Kソリューションを展開している。マーケット·リポート·ワールド社の報告書によると、世界の4K先端技術市場は2017年に472億米ドル、2023年までに年平均成長率21.29%で1,502億ドルに達すると予想されている。

映像監視では、4Kもユーザの注目を集めている。4K(3840 x 2160)の解像度により、ユーザは画像の詳細を見ることができる。例えば、混雑した通りの個々の人や家に侵入する侵入者などが鮮明に見える。ただし、4Kシステムの購入またはアップグレードを検討する場合、エンドユーザは最終決定を下す前に、4Kの長所と短所を見て、自分の環境と要件を検討する必要がある。

長所と短所

前述のように、4Kの主な利点は高精細度だ。これは、ユーザが個々のフレームで侵入者、歩行者、傍観者などを識別する必要がある場合に特に重要となる。これは、法執行機関からスマートシティ、ホーム·セキュリティまで、幅広い用途に役立つ。

しかし、4Kシステムにも欠点がある。4Kカメラで生成された膨大なデータは、必然的に多くの帯域幅とストレージ容量を占有するため、帯域幅とストレージは考慮すべき問題となる。

ただし、帯域幅とストレージを節約するために、多くのカメラがフル·フレーム·レート未満で4K映像をキャプチャしていることに注意すべきだ。都市監視などのほとんどの4Kアプリケーションは、ユーザが各画像の詳細を見ることに関心があるため、実際にはフル·フレーム·レートに設定していない。

その一方で、限られた機能とコストも問題となる。「4Kセキュリティ·カメラの機能はまだ限られている。カメラ·セキュリティ·ナウ誌への最近のブログ投稿では、これらのセキュリティ·カメラには光学ズームオプションはまだない。4K防犯カメラはまだ他の防犯カメラよりも高価だ。小売店での店頭販売など、多くの一般的なアプリケーションでは、4K防犯カメラは必要ないかもしれない。

4Kを選択する前に考慮すべき要素

したがって、4Kは全ての導入事例に理想的なソリューションとは限らない。カメラ·セキュリティ·ナウ誌によると、ユーザが特定の基準を満たしている場合、4Kシステムの購入またはアップグレードが実行可能なオプションになる可能性がある。その1つは、4Kカメラと関連するストレージとディスプレイの購入が高コストの提案になる可能性があるため、ユーザの予算が潤沢の場合だ。

また、最高解像度の映像監視が必要な場合、ユーザは4Kを取得でき、使用量によってコストが正当化される。「セキュリティ·カメラ·システムが、多くの新しい車両全体をカバーする必要がある場合、4Kのセキュリティ·カメラ·システムへのアップグレードのコストは、破壊や盗難を監視するためおそらく正当化できるだろう。

さらに、ユーザが1台のセキュリティ·カメラで広い範囲を監視する必要がある場合も4Kが役に立つ。「その優れた解像度により、単一の4Kセキュリティ·カメラを使用して広い範囲をカバーできます。スポーツ施設やイベント会場で採用する場合、4K防犯カメラは、画質を犠牲にすることなく会場の広い広範域をカバーするための正しい選択だろう。

モバイル·アクセスがカード·システムよりも安全な理由

https://www.asmag.com/showpost/30478.aspx?name=news

アクセス資格情報として携帯電話を使用する機能は、先端技術の採用が歴史的に遅れている市場における最大の傾向の1つです。調査会社ガートナー社は、2020年までに、5つの機関のうち1つが従来の物理アクセス·カードの代わりにスマートフォンを使用してオフィスやその他の施設にアクセスすると予測している。

ガートナー社調査部長デイヴィッド·アンソニー·マアーディ氏は、「従来の物理アクセス·カードをスマートフォンに置き換えることで、コスト削減とユーザ·エクスペリエンスのメリットを実現することができる。セキュリティ責任者とリスク責任者は、物理セキュリティ·チームと密接に連携して、スマートフォンでアクセス認証情報を使用して既存の物理カードを置き換えることによる総所有コストのメリットを得ることができる」と述べている。

HikCentralとメニシング・プロ社、ケア・プロテクト社患者支援ソリューションを支援

https://www.asmag.com/showpost/30499.aspx?name=news

ケア・プロテクト社が医療の安全性と監視サービスの業務を大規模な民間企業にまで拡大したいと考え、メニシング・プロ社製オフサイト・クラウド映像ストレージと組み合わせ、Hikvision社製HikCentral映像管理ソフトウェアを採用した。

ケア・プロテクト社は革新的な組織で、ヘルスケアおよびソーシャルケア環境で優れた、持続可能かつ一貫したケア提供を促進するために設立された。この革新性は、同社が先端技術をケア提供サービスの中心に統合する方法に反映されている。最新の安全なクラウド・ベースの映像ストレージ・サービスとともに、最新のカメラとオーディオ先端技術を使用し、24時間体制で健康とソーシャルケアの専門家チームが評価している。

性能の高い監視システムにより、高レベルの精査が保証されている。その結果、療養中の大人も子供も安全に保護されていることが分かり、その家族は安心感を得られる。いかなる場合においても、システムの使用は親族または近親者限定の事前同意が必要となる。

ケア・プロテクト社の独立したモニターは、必要な全ての開示および規制サービス（DBS）チェックとセキュリティ産業局（SIA）のライセンスとともに、長年の健康と社会的ケアの経験を備えた非常に優れた資格を持っている。全体として、保護と品質および臨床ガバナンスの責任者を支援および助言するために不可欠な、高レベルのセクターの知識と専門知識を提供している。

ケア・プロテクト社が設立された主な理由の1つは、健康および社会的ケア環境でのケア不足または医療過誤の事例に関する一般的な懸念への対処を支援することにある。その結果、音と動きの検出アラームと赤外線撮影が利用されるため、インシデントが見られたり聞こえたり、接続やメンテナンスの問題が発生した場合に即座に警告を発することができる。映像録画には、プライバシー設定を使用して、必要に応じて合意されたゾーンまたは視認区域をブロックすることも含まれている。

ケア・プロテクト社のサービスで映像映像が非常に重要な役割を果たしているため、その映像の視聴を管理するシステムが安定しており、信頼性が高く、効果的であることが極めて重要です。

ケア・プロテクト社の顧客の1社は大規模な民間医療提供者で、ケア・プロテクト社は、英国全土の病院の小児病棟および成人病棟の寝室と共用エリアを監視している。ケア・プロテクト社は、複数の異なる事業提供会社の高齢者介護施設も監視している。

HikCentralの進歩

HikCentralは、包括的でインテリジェントな監視プラットフォームだ。新しく改良されたHikCentralは、標準の既製サーバにプリインストールされたVMSを介してデータと情報を提供し、高度な実況映像と再生、サーマル画像、キュー検出、低帯域幅の適応性、アクセス・コントロールによる映像接続などの高度な機能を備えている。ケア・プロテクト社で使用されているように、強化されたアラーム管理とスマートウォール操作も含まれている。

HikCentralは、カメラ、スマート・ウォール・モニタ、および画像を複数の画面に送る映像デコーダを管理している。これらの画面は、ケア・プロテクト社の顧客である民間医療機関21の病院サイトをカバーしている。

IDEMIA社、クラウドフロー管理を強化するMFace Flexを発売

https://www.asmag.com/showpost/30549.aspx?name=news

IDEMIA社は、MFace Flexを発表した。MFace Flexは、速度、精度、効率を最適化する、ブレのない顔面生体認証ソリューションであり、空港、スポーツ施設、テーマパーク、その他のイベント会場など、通行量の多い場所での個人認証体験を合理化する。MFace Flexは、個人が識別システムを停止や接触または対話することなく、複数の顔を時間内に認識することができる。

MFace Flexソリューションを使用すると、個人は識別プロセス全体を通して動き続けることができるため、このソリューションは、大規模システムでの安全で効率的な処理に特に効果的となる。MFace Flexは、独自設計により特殊な生体認証キャプチャ機器の必要性を排除することで展開コストを最小限に抑え、既存基盤を可能な限り再利用する柔軟性により顧客のROIを向上させる。MFace Flexは、商業輸送、イベント会場、競技施設、テーマパーク、ゲーム会場など、幅広い環境での識別の課題を解決することができる。

サンワサプライ、最大600m延長可能なLANケーブル延長PoEエクステンダーを発売

https://direct.sanwa.co.jp/ItemPage/500-SWH010?utm_medium=Release&utm_campaign=500-SWH010

本製品は、LANケーブルからデータと電力を受けて動作可能なLANケーブル延長PoEエクステンダー「500-SWH010」。電源ケーブル不要で、LANケーブルを通じてPoE対応スイッチングハブやPoEインジェクターからの電源供給で動作できる。本製品を5台接続すれば、理論値で最大600m（推奨420m）までLANを延長可能。延長した先にPoE対応機器を接続できる。

■主な特長

●1Gbps（1000Mbps）の通信速度に対応

●ケーブルのストレート/クロスを自動識別する「AUTO-MDIX」機能に対応

●放熱性、耐久性に優れたファンレスのメタル筐体仕様

●幅79.3×奥行86.8×高さ25.8㎜の小型サイズ、本体質量は約196g

●壁掛け可能なネジとアンカーが付属

●販売は同社WEBサイトに限定。

■主な仕様:

●IEEE802.3(10BASE-T)、IEEE802.3u(100BASE-TX)、IEEE802.3ab(1000BASE-T)、IEEE802.3x(Flow control for Full-Duplex)

●PDポート:IEEE802.3af/at、PSEポート:IEEE802.3af

●スイッチング方式:Store&Forward

●伝送方式:

・10Mbps、100Mbps/全二重、半二重、・1000Mbps/全二重

●ポート構成:

・１０００ＢＡＳＥ-Ｔ/１００ＢＡＳＥ-ＴＸ/１０ＢＡＳＥ-Ｔ（RJ-45)AUTO-MDIX PoE ポート(PSE)×1ポート

・PoEポート(PD)×1ポート

●消費電力:約0.88W

●動作時環境条件:

・使用時温度‥10～40℃

・使用時湿度‥10～90%

ADLINK社、既存システムのドロップイン代替品の新型COM Express Type 2モジュールを発表

https://www.adlinktech.com/Products/Computer_on_Modules/COMExpressType2/Express-SL2?lang=ja

https://www.adlinktech.com/Products/Computer_on_Modules/COMExpressType2/Express-KL2?lang=ja

今回発表した製品は、第6/7世代のIntel® Core™プロセッサを採用した最新のCOM Express Type 2コンピュータ・オン・モジュール。新型のExpress-SL2/KL2モジュールは、Type 2に関連した従来の全てのI/Oに対応したことで、既存のType 2対応システムの製品寿命を今後最低10年延長できる。

最新のExpress-SL2/KL2は、第6/7世代のIntel® Core™プロセッサ（Celeron®およびXeon®搭載製品もオプションで用意）を搭載し、PCIバス、PATA、VGAといった従来のインタフェースに採用されているType 2のピンアウトに対応している。また、ハードウェアの互換性に加え、Windows 7、Windows 8.1、Windows 10、WES 7、Embedded Linuxから業界標準のYocto Project（https://github.com/adlink）、Ubuntu LTS、CentOSといった様々なOSに対応。Express-SL2/KL2は、従来規格と主要なソフトウェアに対応しているので、システムの円滑な移行とパフォーマンスの向上を求めるお客様のニーズに適合している。

Express-SL2/KL2には商業用（0℃～60℃対応）および高耐久性（Extreme Rugged、-40℃～+85℃対応）の両方のバージョンが用意されている。

ロックシステム、モニターBOX最新版を発売

http://locksystem.co.jp/security/monitorbox

ロックシステムは、物理セキュリティシステムを、適切運用管理する「モニターBOX」最新版を発売した。モニターBOXは、物理セキュリティを「安全」にできるだけ「簡単に」クラウド管理することで、ユーザに「安心」を提供する製品として開発された。

これまでの課題

映像監視システムの運用を管理する上で、トラブル、コスト、運用保守、設置施工の面で課題があった。

●**トラブル（故障・停止など）**‥システム故障時の対応に時間がかかり、その間システム運用ができない。また、過去の映像が見えない。

●**コスト**‥システム死活状況を確認する機器の設置場所に困る。また、それらの複数の機器の管理と機器の時刻設定作業が負担。

●**運用保守**‥複数拠点をネットワークで管理する場合コストが高く、セキュリティ面も懸念される。システムの休止は回避したい。

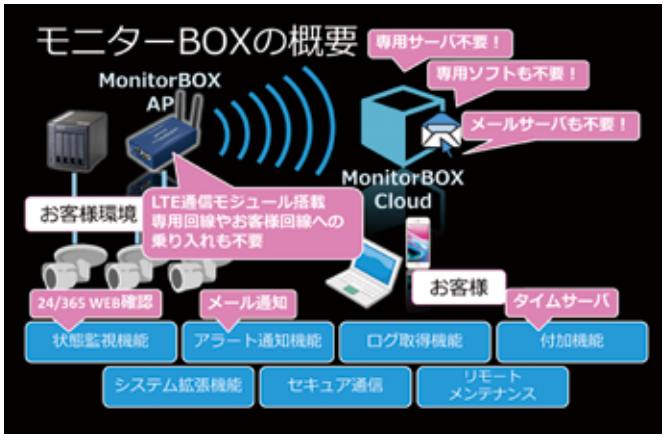
●**設置施工**‥屋外設置の配線や複数階のフロア間の配線コスト、作業員の現地での長時間作業など、負担が大きい。

モニターBOXによる解決策

●**トラブル対応**‥状態監視で異常を検知し、メールで通知。録画エラーも検出し、遠隔メンテナンス機能による素早い対応を実現。

●**コスト削減**‥専用サーバもメールサーバも不要で、低消費電力で済む。1拠点装置で50端末まで管理が可能で、しかも拠点数の制限がなく、大規模案件にも対応できる。さらにタイムサーバ機能で時刻同期の作業からの開放。

●**運用保守**‥ネットワーク構築、ルータ、専用回線、顧客ネットワークへの接続など一切不要、しかも高度なセキュリティで保護することで、販売会社や保守事業者による保守点検が可能。



●**設置・施工の軽減**‥装置本体の広範な動作温度で屋外利用が可能。カメラ映像もモニタリングでき、フロア単位での設置などが可能。オフショアで設定作業ができ、オンサイトでの作業を最小限化。

新機能

モニターBOX最新版には、新機能を追加した。

●**SIM付きパッケージの提供開始**‥NTTPCコミュニケーションズとの協業により、LTE通信のSIM付きのモニターBOXパッケージの提供を開始。

●**高耐久SSD搭載NASの提供開始**‥国内メーカELECOM社との協業により、高性能高耐久エンタープライズSSD搭載の高速NASを提供開始。実効容量1.9TBと3.8TBモデルをラインナップ。

●**イベント・アラーム機能**‥NVRやその他のIoT機器の「異常検知とメール通知」機能。順次対応機器を追加予定。

●**ストレージ機能**‥モニターBOXに高容量SSDを接続し、NASとして使用できる機能。これによりエッジストレージ機能を持つカメラ等機器のデータ保存先として活用できる。

導入効果

●**安全**‥機器の状態をモニタリングすることで故障にすぐに気づくことができ、しかも遠隔で調査や対処し、システムを健全に維持することができる。

●**安心**‥ユーザが投資した設備や機器の状態を把握し、安心と満足を持って使用することができる。

●**IoT機器での活用**‥HUBやNAS、ルータなどIoT機器の状態に対して、遠隔でPingやHTTPチェックが可能。

モニターBOXに関する問い合わせ先

株式会社ロックシステム

http://www.locksystem.co.jp/cs-team@locksystem.co.jp

TEL:045-450-2131

ウエスタンデジタル、「サンディスクSD™カードシリーズ」を一新

今回発表したのは、サンディスクのSD UHS-Iカードは、エクストリーム･プロシリーズ、エクストリーム･ プラスシリーズ、ウルトラ･プラスシリーズ。当該各種UHS-Iカードは、同社独自の技術を用いて、UHS-I規格で定義された104MB/秒以上の読取り速度を可能とし、この技術に対応した当社の下記UHS-Iカードリーダを用いることで、高速データ転送を実現する。

【製品の主な特徴】

■SDカード新製品･･エクストリーム･プロ･シリーズ

製品名･･サンディスク･エクストリーム･プロSDXC™ UHS-Iカード

1.読み取り最大170MB/秒、書込み最大90MB/秒の超高速データ転送（※1）

2.RAWデータや4K動画ファイルなどを十分に保存できる最大1TBの大容量

3.4K動画やフルHD動画の撮影に最適な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

4.容量は、1TB･512GB･256GB

製品URL･･https://www.sandisk.co.jp/home/memory-cards/sd-cards/extremepro-sd-uhs-i

■SDカード新製品･･エクストリーム･プラス･シリーズ

製品名･･サンディスク･エクストリーム･プラス SDHC™/SDXC™ UHS-Iカード

1.読み取り最大150MB/秒、書込み最大70MB/秒の超高速データ転送

2.4K動画やフルHD動画の撮影に最適なビデオ･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.容量は、128GB･64GB･32GB

製品URL･･https://www.sandisk.co.jp/home/memory-cards/sd-cards/extremeplus-sd-uhs-i-70mbps

■SDカード新製品･･ウルトラ･プラス･シリーズ

製品名･･サンディスク･ウルトラ･プラス SDHC™/SDXC™ UHS-Iカード

1.読取り最大130MB/秒で、PCへ高速でデータ転送可能（※1）

2.フルHD動画撮影に適したビデオ･スピードクラス10、UHSスピードクラス1、CLASS10に対応（*1）

3.容量は、128GB･64GB･32GB

製品URL･･https://www.sandisk.co.jp/home/memory-cards/sd-cards/ultra-plus-sd

■SDカードリーダ新製品：

製品名：サンディスク SD™ UHS-I カード･リーダ

1.読取り最大170MB/秒の高速なデータ転送（※2）

2.SD™/SDHC™/SDXC™ に対応

3.USB 3.0に対応し、必要に応じてUSB 2.0との下位互換性も確保

4.USBバス･パワー対応でACアダプタなど外部電源不要

製品URL･･https://www.sandisk.co.jp/home/memory-cards/memory-card- readers/sd-uhs-i-card-reader

---

富士フイルム、レンズ一体型の遠望監視カメラを発売

https://www.fujifilm.co.jp/corporate/news/articleffnr_1449.html

「FUJIFILM SX800」は、同社の光学技術と画像処理技術を駆使して開発した、レンズ一体型遠望監視カメラ。本製品は、世界最望遠800mmまでの焦点距離をカバーする光学40倍ズームが可能な高性能「FUJINON レンズ」を搭載。高い防振性能、最短0.3秒の高速･高精度AF、優れた陽炎･霞軽減機能も実現しており、遠方の対象物を鮮明な映像で瞬時にとらえることができる。

■主な特長

(1)世界最望遠800mmまでの焦点距離をカバーする光学40倍ズームを実現

●広角端20mmから世界最望遠800mmまでの焦点距離をカバーする高性能「FUJINON レンズ」を搭載。

●最大1.25倍のデジタルズームも装備し、焦点距離1000mm相当の遠望監視が可能。

●広角端20mmの映像の青枠部分をクローズアップ。焦点距離1000mm相当では、約1km先にある車のナンバー・プレートをとらえることができる。

(2)高い防振性能を発揮

●新開発した防振機構を搭載

●高性能ジャイロセンサーにより微小な振動も検出

●精密加工を施したセラミックボールを防振機構の駆動部に採用し、防振時の摩擦抵抗を極限まで低減。

(3)リア・フォーカス方式の採用などにより、最短0.3秒の高速・高精度AFが可能

●小口径レンズを高速で駆動させるリアフォーカス方式を採用。

●像面位相差AFとコントラストAFを組み合わせることで、最短約0.3秒の高速AFを実現

●コンティニュアスAFも可能となり、リアルタイムで対象物にフォーカスを合わせ続けることが可能

(4)優れた陽炎・霞軽減機能を搭載し、鮮明な映像を提供

●最先端の補正アルゴリズムと画像処理エンジンにより、陽炎・霞を高精度に検出してリアルタイムで補正

●可視光から近赤外線までの幅広い波長域に対応する多層コーティング処理

●高性能イメージ・センサや最先端の画像処理技術などで、ノイズの少ない鮮明な映像を実現

(5)設置時の作業工数を大幅に削減

●レンズとカメラを一体で開発し、それぞれの性能を最大限引き出せる設計と組立

●従来必要であった光軸やフランジバックの調整が不要となり、設置時の作業工数を大幅に削減

■価格‥オープン価格

アクシスコミュニケーションズ、高性能PTZカメラを発売

URL‥https://www.axis.com/ja-jp/products/axis-p5655-e

今回発表した製品は、汎用性の高い監視用途向けの、費用対効果に優れたAXIS P5655-E PTZ ネットワークカメラ。本製品には、一層高度になった画像処理とセキュリティ機能、インテリジェント機能、そして非常に効率的なビデオ圧縮をそれぞれ提供する、次世代のチップセットARTPEC-7を搭載している。

AXIS P5655-Eは、高感度のイメージ・センサとForensic WDR機能を備え、撮影シーン内に暗い部分と明るい部分が混在している場合でも、鮮明な映像を提供する。また、Axis Lightfinder 2.0テクノロジーを採用しているため、低光量の環境下でも彩度の高いカラー画像を撮影でき、動いている被写体でも鮮明な画像を撮影することもできる。

さらに、電子動体ブレ補正機能が、振動や揺れの影響を最小限に抑える。高度な分析を可能にする優れた処理能力を備えており、4つのシーン・プロファイル(屋内、屋外、フォレンジック、トラフィック)から状況に応じて選択することができる。このカメラは、プロファイルごとに露出時間、ホワイトバランス、開口、シャープネス、コントラスト、ノイズを特定のシーン要件に合わせて自動的に最適化を行う。

また、署名付きファームウェアはファームウェアが改竄されていないことを保証し、許可されたファームウェアのみがインストールされるようにしている。さらにセキュアブートは、必要に応じて、工場出荷時の設定後、カメラにマルウェアが一切含まれていないことを保証している。

【主な特長】

●HDTV 1080pおよび32倍光学ズーム

●Forensic WDRおよびLightfinder 2.0

●署名付きファームウェアとセキュアブート

●フォーカス・リコールおよび電子動体ブレ補正

●H.264およびH.265対応のZipstreamで、ネットワーク帯域幅とストレージの必要量を大幅に削減。

●双方向音声、PoE+、4つのI/Oポートを装備。

●24V AC/DCに対応。

●IP66、NEMA 4X、およびIK10規格に準拠

TOA、小型AHDコンビネーション･カメラを発売

https://www.toa.co.jp/products/security/ahd/ahd_camera/ah-c1714.htm

今回発売した製品は、AHD（Analog High Definition）規格AHD2.0方式を採用し、旋回台、電動ズームレンズを一体化した屋外･屋内兼用ドーム型コンビネーション･カメラAH-C1714。フルHD（1920 x 1080）の画像サイズの映像を出力し、制御線を接続することで、RS-485信号で遠隔制御が可能。

制御信号を映像信号に重畳することができるため、レコーダと同軸ケーブルを接続するだけで遠隔制御を行うこともできる。有効画素数が約213万画素の1/3型CMOSセンサを採用していることで、高精細な画像が得られる。また360度エンドレスで水平旋回可能で、水平旋回、垂直動作200度/秒の旋回台と10倍の光学ズーム･レンズを搭載し、任意位置を最大64ポジションまでプリセット記憶が可能で、記憶させたポジションは瞬時に再生することができる。さらに32倍電子ズーム、トレース機能、ツアー機能、白黒モード、プライバシー･マスク、揺れ補正、WDR（ワイド･ダイナミック･レンジ･･AHD出力時のみ）、E-WDRを搭載している。本体はアルミ･ダイカスト、ドーム･カバーはポリカーボネートを採用し、耐衝撃性に優れている。

【主な仕様】

- ●電源･･AC24V 50/60HzまたはDC24V
- ●消費電力･･10W
- ●カメラ出力･･1系統　AHD2.0信号/NTSC信号
  VBS1.0（p-p）　75Ω　BNC接栓
- ●電子ズーム･･32倍
- ●最大画角･･水平：約54度(W)～7度(T)、
  垂直：約30度(W)～4度(T)
- ●使用温湿度範囲･･-10℃～+50℃、90%RH以下
  （結露がないこと）
- ●防塵防水性能･･IP66適合
- ●耐衝撃性能･･50J
- ●寸法･･カメラ部外形：φ157 x 158.5(H)㎜、
  ドーム外形：φ99㎜
- ●質量･･1.9kg

【本体価格】

- ●オープン価格（実売予想価格は約28万円）

レノボ･ジャパン、ThinkSystem SE350の提供開始

https://www.lenovo.com/jp/ja/data-center/iot-edge-solutions

本製品は、耐久性と信頼性に優れたエッジ･コンピューティング向け最新サーバ。エッジ･サーバ特有の各種要件を考慮して設計、構築されているため、サーバ設置場所の制約を緩和した高い汎用性を有する。様々な接続およびセキュリティ･オプションを提供し、Lenovo XClarity Controller の使用により容易に管理することができる。モデルは、有線モデルが3機種、無線対応モデルが3機種。

【主な仕様】

- ●1Uの高さ、ハーフ幅のIoTエッジ･サーバ
- ●1ソケット･インテル(R) Xeon(R) D-2100プロセッサ、最大16コア
- ●最大256GBメモリ搭載
- ●有線（SFP+）モデルと無線対応（WiFi/LTE）モデル、5G対応予定
- ●データ･ストレージは、最大16TBのSSDストレージ
- ●NVIDIA T4 GPUの搭載サポートにより、AIソリューションへの活用
- ●高い堅牢性、周囲温度0～55℃に対応、耐粉塵、対応衝撃30G、対応振動 最大3G
- ●システム管理 Lenovo XClarity
- ●高セキュリティ
  ･ThinkShield SecureVaultキー管理（モーションおよび不正侵入／改竄防止対応）
  ･SED暗号化ストレージ(オプション)
  ･付きロック対応筐体(オプション)
- ●本体寸法･･高さ：40㎜、幅：215㎜、奥行：376㎜

【メーカー希望小売価格（税別）】

- ●有線モデル･･368,000円より
- ●無線対応モデル･･478,000円より

アクロニス社、個人ユーザ向けデータ保護バックアップソフトウェア「Acronis True Image 2020」を発表

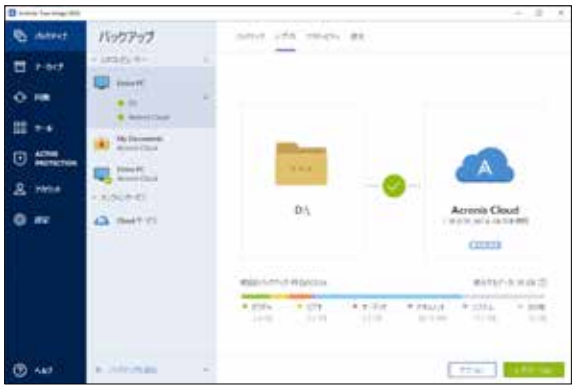
http://www.acronis.com/ja-jp/personal/computer-backup/

本製品は、個人向けの「簡単・オールインワン・安心」のデータ保護ソリューション。従来から定評のある高速バックアップをさらに性能アップ、Acronis Active Protection にて提供されるセキュリティの拡張やWi-Fi 環境でも快適に使うことができる細かい機能を拡張している。

【主な新機能および機能強化の概要】

■新機能　Dual Protection（デュアルプロテクション）

ローカル・バックアップをクラウドに自動的に複製することで、オフサイトのコピーをいつでも復元に使用できるようになる。また、バックアップとアプリケーションを同時に実行することで、バックアップにおける「3-2-1 ルール」で推奨されるオフサイト・コピーを効率化。



※クラウドストレージへのオフサイトコピー、バックアップ機能はAdvanced Edition以上で提供。

■機能強化 バックアップ技術の改良

アクロニスの新技術を使ったバックアップ・フォーマットを採用（Archive-3）、最速のバックアップがさらに改良。

■機能強化　トレイ通知センター

メッセージがデスクトップトレイにプッシュされるため、バックアップ管理コンソールを開かずにバックアップのステータスを監視できるため、問題にすばやく対応し保護強化のためのタイムリーなヒントを受け取ることが可能。

■機能強化 Acronis Active Protection の改良

進化するサイバー脅威へ対抗するため、Acronis Active Protection に搭載されている機械学習エンジンの検知機能を強化。Acronis Active Protection で検知されたイベント検出理由の表示を追加。

■機能強化　電源管理の拡張

電源を管理することでノートPCの電源を維持するため、バッテリを長寿命化。バックアップの最小電力レベルを指定、バッテリ電力を使用するバックアップを完全に停止かの設定ができる。

■機能強化　選択した安全な Wi-Fi でバックアップ

データをリスクにさらす安全でないパブリック・ネットワークや従量接続のWi-Fiを回避することが可能。選択されていないネットワークにコンピュータが接続されている場合、全てのクラウド・バックアップを一時停止。

その他に、Acronis True Image 2020 には100 以上の改善・拡張機能を含む。

【発売日】

2019年8月21日‥Acronisオンラインストア

2019年10月11日‥パッケージ版、他オンラインストア

【製品ラインナップおよび標準価格（いずれも新規購入価格、税別）】

●買い切り型

Acronis True Image 2020 1 コンピュータ‥5,074円

Acronis True Image 2020 3 コンピュータ‥8,130円

Acronis True Image 2020 5 コンピュータ‥10,167円

Acronis True Image 2020 1 コンピュータ

アカデミック版‥3,037円（パッケージ版のみ）

●買い切り型（アップグレード版）

Acronis True Image 2020 1 コンピュータ‥3,037円

Acronis True Image 2020 3 コンピュータ‥6,093円

Acronis True Image 2020 5 コンピュータ‥8,130円

●年間サブスクリプション(250GB クラウドストレージ付)

Acronis True Image Advanced 1 コンピュータ‥5,074円

Acronis True Image Advanced 3 コンピュータ‥8,129円

Acronis True Image Advanced 5 コンピュータ‥10,166円

●年間サブスクリプション(1TB クラウドストレージ付)

Acronis True Image Premium 1 コンピュータ‥10,166円

Acronis True Image Premium 3 コンピュータ‥15,259円

Acronis True Image 2020 Premium 5 コンピュータ‥16,277円

オプテックス、新製品2種を発表

【車番認証システム用投光器「パルススター」】

本製品は、高出力の赤外光とカメラのシャッタースピードを同期させる設計により、夜間や悪天候などあらゆる条件下でも、高速に移動する車両のナンバー・プレートを鮮明に撮影することが可能となる。

■特長

- ●従来比4倍の投光量および最大60mの照射により遠距離からの車番認証が可能
- ●赤外光とカメラ・シャッタースピードを同期し、高速移動車両の映像を提供（TTL方式：Through the Lens）
- ●5モデルおよび付属の交換レンズにより、設置される場所や投光距離に合わせて選択できるラインアップ
- ●白とびや黒つぶれを抑制する上、均一配光により画角全体を明るくクリアにすることが可能

■主な仕様

波長	IR(850nm)				
型式	PSTR-i24-LV	PSTR-i32-LV	PSTR-i48-LV	PSTR-i72-LV	PSTR-i96-LV
発光時消費電力	220W	295W	440W	660W	880W
電源電圧	DC 24V				
消費電力(最大)	22W	30W	44W	66W	88W
照射距離目安（水平×垂直）	10°x10° 25-30m	10°x10° 30-35m	10°x10° 35-42m	10°x10° 43-50m	10°x10° 50-60m
	20°x10° 15-17m	20°x10° 17-20m	20°x10° 21-24m	20°x10° 26-29m	20°x10° 30-34m
	35°x10° 13-15m	35°x10° 15-17m	35°x10° 18-21m	35°x10° 22-26m	35°x10° 26-30m
照射角度(付属レンズ)	35°×10°(標準装着)、20°×10°、10°×10°(レンズなし時)				
付属コントローラ	カメラ×1入力、投光器×2出力			カメラ×2入力、投光器×4出力	
トリガー入力	TTL方式(DC 3-24V)				
パルス幅	2ms(初期設定)				
12V DC 出力	1A(コントローラより出力)				
質量(投光器本体)	1,650g	2,250g	4,500g	6,000g	2*4,500g
質量(コントローラ)	1,700g	1,700g	2,000g	2,300g	2,300g
使用温度・湿度範囲	-20℃~45℃				
保護等級	IP66				

赤外光/白色光のハイブリッド・タイプ監視カメラ用投光器「Vario2 ハイブリッド」

本製品は、夜間、人の目には見えない明かりを照射する赤外光によるカメラ補助照明の用途だけでなく、搭載された白色光へ切り替えを行うことにより、カメラ映像を白黒からカラーに変換し、白色光による侵入者への威嚇が可能になるなど、的確な監視と迅速なセキュリティ対策を提供する。

■主な仕様

型式		VAR2-hy4-1		VAR2-hy8-1		VAR2-hy16-1		VAR2-IPPoE-hy4-1		VAR2-IPPoE-hy8-1	
波長		IR (850nm)									
定格光束		745lm		2980lm		5600lm		745lm		2980lm	
色温度		6000K									
最大照射距離(水平x垂直)単位:m		IR	White	IR	White	IR	White	IR	White	IR	White
	10×10°	130	70	290	140	450	195	130	70	290	140
	20×10°	90	45	165	85	235	130	90	45	165	85
	35×10°	70	40	150	75	225	95	70	40	150	75
	60×25°	45	20	85	40	120	55	45	20	85	40
	80×30°	30	15	60	30	95	35	30	15	60	30
	120×50°	20	10	40	20	55	25	20	10	40	20
電源電圧		DC24V						PoE+ IEEE 802.3at or 24VDC		60W PoE++(4-paiePoE) or 24VDC	
消費電力(最大)		13W		40W		78W		15W		43W	
外部入力		遠隔操作又は無電圧接点入力による切替制御									
外部出力		照度センサー出力 無電圧接点出力									
質量		950g		1650g		3100g		950g		1650g	
使用温度・湿度範囲		-50℃~+50℃/10%~90%RH(但し、結露なきこと)									
ケーブル長		約2.5m(φ6.5)		約2.5m(φ8.0)				約2.5m(φ6.5)			
保護等級		IP66									

セキュア、IDIS社製DirectCXシリーズ H.265 レコーダを発表

【DirectCX 4/8/16チャンネルH.265レコーダ、TR-2404/TR-2408/TR-2416】

■主な特長

- ●マルチのアナログカメラをサポート
- ●最大120/240/480ipsのフルHD録画
- ●H.265圧縮、インテリジェント・コーデックをサポート
- ●最大5MPの解像度をサポート
- ●HDMI出力UHDディスプレイ
- ●HDMIおよびVGA出力フルHDディスプレイ
- ●長距離伝送の同軸ケーブルをサポート
- ●同軸ケーブルを使用した高画質監視システム
- ●2つのSATAインタフェイスを使用し最大12TBまで拡張可能
- ●FENサービスによるワンクリック・ネットワーク構成をサポート
- ●販売開始・・2019年12月を予定

■問い合わせ先　株式会社セキュア

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

fire & safety
powered by Secutech

2020 年4月22 - 24日　台湾台北市南港展示ホール
firesafety.secutech.com

災害管理を強化するスマートなソリューション

第19回Fire & Safety展は、アジア太平洋地域の火災安全および災害管理双方の専門家を結びつけると、高い評価を得ているイベントです。

スマート防火と安全

スマート・ソリューション
- 介護施設と老人ホーム
- 超高層ビルと複合施設
- 鉄道とトンネル
- 住宅およびホテル
- 工場

製品のオンデマンド
- 消火設備・機器
- 火災警報設備
- 防炎・防火材料、耐火製品
- 冷凍空調設備
- 高品質の製品

スマート防災

革新的なソリューション
- 災害時の緊急対応
- 防災
- 減災

出展製品
- 災害管理システム
- 救助資機材
- 避難設備
- 非常時通信
- 通報機器、放送設備
- 個人装備品

アジア太平洋スマート防災サミット

ベトナム、フィリピン、タイ、ネパールの専門家や政府関係者と、災害に対する解決策を協議する場です。

◆お問い合わせ先

Kirstin.Wu@newera.messefrankfurt.com
+886 2 8729 1099 ext. 217

◆同時開催

secutech　MOBILITY powered by Secutech　SMbuilding powered by Secutech　info security powered by Secutech

製薬業界のセキュリティは、業界保護に不可欠

セキュリティ業界では、製薬業界はヘルスケア部門に仕分けされることが多い。これは分野の性質面で理にかなっているが、製薬分野自体は特別な注意を必要とする個別性がある。

この分野での急速な成長が見込まれ、セキュリティ上の懸念が高まる中、製薬分野のソリューション需要は今後も続くと予想されている。技術の進歩や接続機器に伴い、サイバー・セキュリティも懸念されている。本稿では、製薬分野における主な脅威、適切なソリューション、およびその実装方法の例を見てみる。

●プラスンス・アビー・トーマス
(コンサルタント・エディター)

アクシス・コミュニケーションズ
米国社ヘルスケア部門事業開発
責任者ポール・バラッタ氏

ハネウェル社
上級製品マーケティング責任者
エリック・グリーン氏

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

ADTコマーシャル社傘下レッド・ホーク・ファイア&セキュリティ社
法人営業&製品戦略担当
上級部長リック・タンピア氏

製薬業界のセキュリティの成長と動向

セキュリティ産業は米国が最も急成長している市場で、中国が続き、今後登場してくる新しい分野が需要を喚起すると予想されている。

個別市場としてのヘルスケア分野は、多くの場合、その特殊性からセキュリティ業界で多くの注目を集めている。この分野と密接に関連し重要視されている製薬分野の需要はあまり議論されていない。

ビジネス・リサーチ会社によると、製薬業界の世界市場は2017年から2021年の間に年平均成長率約6%と見られている。この点特に米国市場について確認すると、アクシス・コミュニケーションズ米国社ヘルスケア部門事業開発責任者ポール・バラッタ氏は、買収と繰り返して業界は成長し続けていると述べた。

成長の原動力

バラッタ氏は、「バイオ医薬品部門におけるリーダーシップの主な懸念の1つは、スタッフと製品そして情報の保護だ。2018年、小規模製薬会社が数社買収され、大規模医薬品企業の傘下に入った。大企業は、ケシから採取されるアルカロイドから合成された化合物であるオピオイドの流通に対する圧力により、製品開発から研究開発に焦点を変える役割を果たしてきたため、再編プログラムを開始した」と語っている。

この移行により、より多くの臨床科学基金と開発への再焦点化、情報（サイバー）および産業スパイに対する保護の強化が促された。また、スタッフの削減、統合、研究の強化、サイバー保護、産業スパイの組み合わせは全て、アクセス管理と、映像管理システム（VMS）およびカメラと音声を含む映像ソリューションの両方に必要なアップグレードで大きな役割を果たした。

バラッタ氏は「バイオ医薬品が業績の悪い企業やオピオイドの流通と虐待に対する政府の圧力から逃れて、スタッフや技術の増加が最近の動向となっている。この傾向は、事業統合が続く中で、今後3～5年続くだろう。さらに、製造工場を集約し、物流センターを市場近くに設置し、市場で優位に立つために産業の秘密を守るサイバー対策が増えている」と話している。

勢いを増す最近の変化

成長に伴い、製薬業界にも厳しい規制がある。ハネウェル社上級製品マーケティング責任者エリック・グリーン氏は、成長は続くものの今後数年間で規制が厳しくなる可能性があると考えている。

しかし、おそらくセキュリティ・サービス供給企業やシステム構築者にとっては、製薬業界内の新しい分野の一部に対して興味深いようだ。

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・ホイットニー氏は、「米国とカナダの各州レベルでマリファナの合法化を実施したことで、業界の主要な新しい部門が生まれた。製品設備は、複雑な記録管理要件とセキュリティ強化を構築したか既に実施している。また多くの新しい企業が製薬ゴールド・ラッシュに参入しているが、異業種企業を含めて既存企業がこの分野に参入している」と説明している。

これにより、製薬業界の製造と供給、販売と流通、小売販売網などとは縁のない、物理的なセキュリティや映像監視、アクセス・コントロールからサイバー・セキュリティ保護に至るまでのセキュリティ業界の参加者にとって全く新しい機会が発生した。

米国およびその他の地域の市場動向

調査会社IQVIAによると、米国は現時点で最も急成長している製薬市場で、今後数年間で年平均成長率4～5%を記録すると予想されている。中国が年平均成長率3～6%と続いている。

現在、米国では保険プランの価格と払い戻しに関する議論が新たに行われている。保険契約の変更はこの分野に影響を与えないかもしれないが、価格設定の変更は製造業者の取り分を狭め、ひいては予算とセキュリティ・ソリューションへの投資能力を損なうことになる。

製薬セクターが直面する脅威と懸念

製薬業界のセキュリティ・ソリューションとは?

システム構築者にとって、高品質のソリューションを提供するには、脅威を理解することが不可欠だ。ヘルスケア全体では、セキュリティに関してはその性質上、特別な注意を必要とする。

ハネウェル社上級製品マーケティング責任者エリック・グリーン氏によると、製薬業界は厳格なコンプライアンスの要求を満たしながら、知的財産とブランドの評判を保護するという課題に直面している。

グリーン氏は「これらの戦線のいずれかに障害が発生すると、数百万ドルの費用がかかる。当社ソリューションは、物理的なセキュリティを提供するだけでなく、コンプライアンス手順を設定して実施し、コンプライアンスを証明する広範な監査機能を介して証拠を提供するのに役立つ」と話している。

製品および知的財産の盗難

薬は価値が高く、環境相互作用に敏感だ。医薬品の取り扱いが安全であることを確認する必要がある。また、偽造薬などの問題を回避し、ビジネス上の理由から、処方を保護する必要がある。

ADTコマーシャル社傘下レッド・ホーク・ファイア&セキュリティ社法人営業&製品戦略担当上級部長リック・タンピア氏は、「製剤、医薬品、および薬物成分は高価であり、盗難を起こしやすい。「適切に保管されていない場合、短期間であっても範囲外の温度を経験する在庫は、患者の生命を脅かす可能性がある。製薬会社が規制への準拠の証拠を示すことができないか、違反していることが判明した場合、数百万ドルの損失、評判の低下、将来のビジネスを失う可能性がある」と指摘している。

製薬業界のセキュリティ・ソリューションとは?

システム構築者にとって、高品質のソリューションを提供するには、脅威を理解することが不可欠だ。

製品の性質やそれに従うプロセスによって、各企業は様々な要件により求められるソリューションが異なる。大まかに言えば、次の構成では、統合されたセキュリティ、火災、および生命安全ソリューションの一部として考慮する必要がある。

統合アクセス・コントロールおよび映像ソリューション

最も重要な構成は、侵入検知と遠隔表示機能を備えたIPベースの映像ソリューションと統合された電子アクセス・コントロールだ。

ADTコマーシャル社傘下レッド・ホーク・ファイア&セキュリティ社法人営業&製品戦略担当上級部長リック・タンピア氏によると、3つの技術をうまく組み合わせることで、企業は侵入システムの動作または動作解除するためのコードを入力するとともに、有効なアクセス制御カードを提示する必要がある二重認証システムを確立できる。

重大な状態の監視

温度のわずかな差でさえ、薬物や薬物成分が悪影響を受ける場合、潜在的に生命を脅かす状況を引き起こす可能性があることから、これもまた重要な機能だ。この在庫は数百万ドルを表し、問題が発生した場合に会社に多額の損失を被る可能性がある。これらは、単純なアラームを超

安全・被害防止

セキュリティ・リスクに加えて、製薬生産工場や研究所の担当者は、費用のかかる損傷、ダウンタイム、および火災や生命の安全に関する懸念に関連する人々や財産に対するリスクを防止および制限するという課題に直面しているとタンピア氏は付け加えている。そして「各施設では、火災、一酸化炭素、煙、熱の検知、および高感度で特別な危険検知のためのネットワーク火災警報検知システムを含むリスクと適切な保護を特定するための危険評価が必要だ」と付け加えている。

サイバー・セキュリティ

現在、サイバー・セキュリティの脅威に対して免疫を持つ業界は存在しない。製薬企業が取り扱う必要のある知的財産の価値が高い場合、データの堅牢な保護は避けられない。

ホイットニー氏は「サイバー・セキュリティの問題に取り組む製薬企業は、過去に既知のセキュリティ侵害が発生した箇所の見直しを含め、リスク分析監査を実施することがよくある。その後、業界標準が進化する一方で、同社はデータへの不正または悪意のあるアクセスや変更また削除に対して最も脆弱なポイントとシステムを特定して排除することに重点を置き、システムとデータへのアクセス・コントロールを強化し、新しいサイバー・セキュリティの最善策を実施することができる」と述べている・

規制要件

製薬会社は、強盗から強盗まで、内部および外部からの盗難から腐敗や汚染まで、幅広いセキュリティの脅威に直面している。これは、HIPAA規制、FDAコンプライアンス、および州薬局の仕様を含む様々な州および連邦の命令を遵守する必要がある米国などの先進市場では特に規制の厳しい業界だ。

これらの規制の多くは、特定の制限区域に入るために他の従業員が立ち会う必要がある薬剤師などの問題のコンプライアンスを確保するために、厳格な監査証跡を必要とする。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・ホイットニー氏は、製薬会社が法律と規制そして業界ガイドラインなどの複雑な法的要件の下で事業を展開することに同意している。

「米国では、FDA (Food and Drug Administration：アメリカ食品医薬品局)が21 CFRパート1を実施し、システム検証や電子監査証跡を含むプロセス全段階での管理を義務付けているが、他の国にも同様の要件がある。米国以外でも規制は厳格だ。欧州医薬品庁は、EU内の国の製造基準を規定し、基準への準拠を検証する検査を調整している」とホイットニー氏は述べている。

えたソリューションの必要がある。

タンピア氏は、「例えばドラッグ・キャビネットや金庫が許容温度範囲外になった時にアラームを受信するように設計されており、ドアの状態、電力、冷媒漏れの可能性も監視する」と説明している。

空気交換ソリューション

場合によっては、FDAは、一部の施設がその空気交換要件を順守することを要求する。空気連動ソリューションは、これらの状況に適している。

このソリューションでは、「クリーン環境」に入る複数のドアを使用する。設計上、スタッフメンバーが一度に1つのドアのみを開けることができるタイミング・インターロック機能が含まれている。これは2ドア間隔と3ドア間隔で行われる。

火災ソリューション

タンピア氏は、ウェット、ドライ、プレアクション、および洪水パイプ・スプリンクラー・システムなど、用途に応じて幾つかの異なる消火の代替手段が利用可能だと述べている。ガス、泡、および水ミスト抑制システムもオプションであり、非常に早期の警告煙検知、光学炎検知、および水ベースまたはクリーンエージェントの火災抑制システムだ。

「クリーン・エージェントの消火システムは、薬物検査室、コンピュータ室、プロセス制御区域などの人がいる繊細な機器を備えた区域に適している。洗浄剤の液体は水のように見えるが、消火時に通常水に関連した損傷を引き起こさない」と同氏は話している。

一括通知システム

通報・避難システムは、脅迫や暴力行為に加え、自然災害、

火災、事故などの緊急事態が発生した場合の建物の住民への警戒を支援する。この大量通知ソリューションは、このような緊急事態が発生した場合にすぐに大きなグループに通知することができ、緊急対応を加速し、潜在的に命を救うことができる。

小売薬局のソリューション

小売薬局の場所は、ドアの接点とモーション・センサを備えた侵入制御システム、有線または無線のホールドアップまたはデュアアラームボタン、IPなど、支店の銀行施設が必要とする可能性のある同じ火災、生命安全、セキュリティ技術の多くを必要とする。施設内外に設置されたカメラ、双方向音声/映像、弾丸耐性ガラス/窓、薬局の抽斗、窓を備えた空気駆動システムなどがある。

ボールトとディストリビューション センターをセキュリティで保護するソリューション

アクシス・コミュニケーションズ米国社ヘルスケア部門事業開発責任者ポール・バラッタ氏によると、医薬品保管庫と物流センターの保護は大きな懸念事項だと指摘する。これらの領域は、セキュリティ上の問題の最高レベルで処理する必要がある。「境界から実際の金庫に至るセキュリティプログラムを開発することは、スタッフと製品を保護するために最も重要だ。最外周から始めて、高いフェンスと障壁を埋めて、掘り込み、サーマルカメラ、視覚カメラ、オーディ

オホーン、レーダによる侵入を防ぐことが全境界を保護する標準仕様だ。」

誰がいつ入場するかを文書化するために、システムに追加されることが多いアクセス・コントロール機能が幾つかある。建物と敷地の外側に映像監視システムを実装すると、薬室内またはその周辺の人と車両を識別できる。フェンスラインの近くをうろついたり、敷地内に入ろうとする障壁を乗り越えたりする人々を判断するための分析の使用は、標準装備する必要がある。さらに、流通センターを介した製品の全ての移動に対する侵入アラームと広範なビデオ範囲、センターを設置する必要がある。システムは、警備員、または必要に応じて武装した警察に通知するアラームをトリガーするように設定することができる。

製薬業界におけるITとOTの統合時のサイバー・セキュリティの懸念

この業界のデータは機密性が高いため、サイバー攻撃に対して脆弱だ。

IT(情報技術)とOT(運用技術)を扱う部門は、どちらも法律、規制、業界標準、およびガイドライン順守の経験がある。

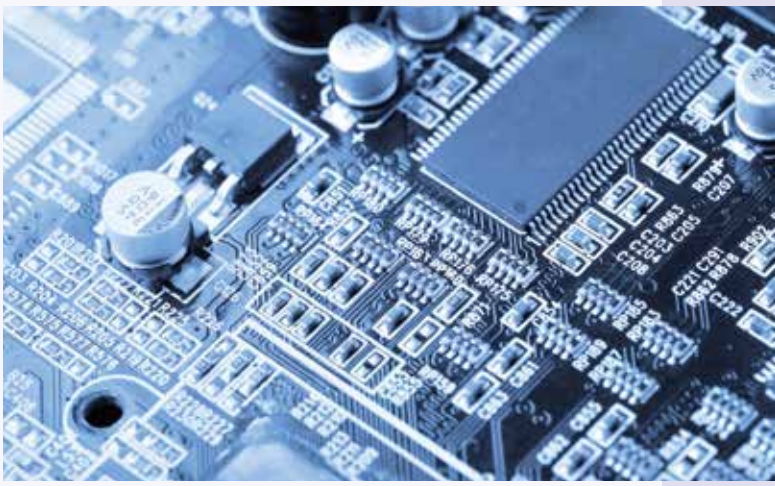
OTは、製造とテスト、開発と在庫および出荷の全段階で物理的セキュリティに大きく関係してきたが、ITは従来からネットワーク、システム、およびデータ保護に焦点を合わせてきた。

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・ホイットニー氏は次のように述べている。

「産業機器は、ネットワーク基盤を並列またはITシステムと組み合わせて活用するIoT(モノのインターネット)接続を特徴としている。IoTは製造業にとって大きな利点があるが、商業スパイ、製品の改ざん、テロリズム、活動家の行動、および新しいレベルのセキュリティを実装しないデータと製品の窃盗のサイバーリスクへの潜在的な経路も示している」。

現在、製薬業界やその他の製造業の組織は、サプライ

チェーン、製造プロセス、保管と出荷の両方を通じて、機器のセキュリティ監査とリスク評価を求めている。これにはパートナーとサプライヤーが含まれ、新しい製薬業界のセキュリティ基準、ベストプラクティス、および世界中の様々な法律に対応し続けている。



恰好のターゲット

アクシス・コミュニケーションズ米国社ヘルスケア部門事業開発責任者ポール・バラッタ氏は、デロイト社の調査では、製薬業界が世界中のサイバー犯罪者の主要な標的であり、数百万ドル相当の知的財産の損失が発生していると指摘している。

「バイオ医薬品は常にハッカーに攻撃に晒されていて、毎日攻撃されている。可能性のある脅威に対するトレーニングと従業員の認識が最善の防御策だ。それは簡単なルールで、例えば、メールの送信者がわからない場合は、添付ファイルを開いたりダウンロードしたりしない。また、外付けドライブは、会社が所有するデバイスに入れない。ファイアウォールとVPOは、悪意のあるハッカーから保護するための小さな方法にすぎない」と同氏は指摘している。

重要な優先事項

ハネウェル社上級製品マーケティング責任者エリック・グリーン氏は、同様のメモについて、データと資産の整合性を保護することに関して、ITが最も多くの注目を集め、この対応はコストがかかる可能性があると説明している。

「OT-プロセス、機器、および運用環境を監視、制御、保護するシステムは、別のエントリ・ポイントになる可能性があり、今日の絶え間なく接続されている技術一環境で同様の注意が必要になることがよくある。物理的なセキュリティ供給企業として、共存するだけでなく、製品が存在する環境のサイバー・セキュリティ体制を強化するために必要な機能とツールを提供することは、私たちの義務だ。当社の製品は、広範なサイバー・セキュリティのテストと評価を受けている。サイバー・セキュリティ・ソフトウェアの標準と最善策を常に追跡して、製品が顧客の環境に安全に統合されるようにしている」と同氏は話している。

企業情報の保護

多くの製薬会社にとって、ビジネスを誤った方法で傷つける可能性のあるデータを保護することは優先事項だ。バラッタ氏は、効果的なサイバー・セキュリティとは、全ての機器のパスワード保護を含む適切な手順でリスクを評価し、効果的なリスクを軽減することだと強調している。

「これには、ネットワークの一部である全てのセキュリティ機器も含まれている。侵入、バックドア、さらにはサービス・ポータルを提供する製造業者からも保護する必要がある。そうしないと、外国政府がIT基盤にアクセスしてしまう危険性がある」と同氏は付け加えている。

セキュリティと脆弱性の管理は、適切なパスワード、ファイアウォール、ユーザと従業員へのテストとトレーニングを最優先に行う必要がある。セキュリティ機器では、強化ガイドやその他のリファレンスを使用して、システムへの侵入を防ぐことだ。

世界中の製薬企業のセキュリティ導入事例

アクシス・コミュニケーションズ社が中国の医薬品工場をどのように確保したかを探る。

医薬品分野でのセキュリティは、製造プラントと保管セグメントに限定されない。ソリューションは、顧客の手に届くまで資産を保護するために必要だ。アクシス・コミュニケーションズ社が中国にある北京同仁堂國際有限公司

(TongRenTang Health Pharmaceutical)の安全を確保するように求められた時、考慮すべき幾つもの要因があった。

必要なもの

「北京同仁堂國際有限公司の経営陣は、営業時間後のスタッフ・オフィスのセキュリティ監視のため、視覚化された管理を作成したいと考えていた」とサイト上で述べている。「そのためには、信頼性が高く、操作しやすい統合デジタル映像セキュリティ・システムが必要だった。同時に、包括的かつ拡張可能でなければならない。その結果、視覚化された管理プラットフォームは、画質、互換性、安定性、および信頼性に関して非常に高い要件を持つ必要があった。システムの主な要件は、エレベータ、オフィス区域、エレベータ前ロビー、主要出口、会議室、廊下、駐車場や様々な主要な店などの場所を監視している。

使用された機器

北京映像コムとその統合可視化管理プラットフォーム「キャッチャー」と協力して、アクシス社は150台のカメラを搭載した統合ネットワークシステムを選択した。インターネット・ケーブルで建物内のLANに接続し、バックエンド管理プラットフォームが集中管理を行っている。

アクシス製ネットワーク映像カメラは、IPネットワーク(LAN/イントラネット/インターネット)に基づいてデジタル映像画像を直接送信している。顧客は、いつでもどこでも任意のネットワーク・コンピュータから最大800x600の解像度の高品質のリアルタイム監視画像を閲覧することができる。可視化された管理を実現し、システムの多様性を高めている。新しい監視ネットワークは、シンプルで柔軟な方法で構築され、拡張性が高い。

使用されるソリューション

アクシス社は、この案件に複数の異なるカメラを採用した。モデルはインストールされた場所の要件に応じて選択した。

オフィスエリアでは、固定ドーム型ネットワークカメラを採用した。エレベータ前ロビーには、低照性対応のSVGA解像度ドーム型カメラを設置した。出口区域と廊下区域に同製品を設置した。駐車場は、カメラが低照度条件で苦労することが多い場所で、低照度対応の別のモデルを採用した。最後に、会議室には固定ドーム型カメラを設置した。

中央管理サーバは、システム全体の中で全てのネットワーク映像カメラ、エンコーダ、および様々なシステム・モジュールを一元管理するため、統合可視管理プラットフォーム「キャッチャー」をインストールした。顧客は映像録画と検索モードの多くのモードをサポートする映像録画の管理のためのストレージ・サーバを持っている。ストリーミング・メディア・サーバは、機器の同時ストリーミングを増やし、帯域幅を節約するために使用している。

スケールアップの可能性

製薬会社のような場所を確保する上で大きな懸念事項の一つは、将来的にカメラが増える可能性があることだ。これには、デバイスを統合するためのソリューションを採用する必要がある。アクシス社のソリューションは、このオプションを提供している。同じ場所または遠隔地でより多くのカメラが必要かどうかにかかわらず、インターネットを介してコア・ネットワークに統合することができる。 a&S

NVR、サーバ、クラウドの映像管理システムに必要な様々な IT 専門知識

イーグルアイネットワークス社創業者兼CEO ディーン・ドレイコ

コストと製品機能。この2点が多くの場合、監視カメラとその映像管理システム·ソフトウェア、映像記録用サーバ、そしてNVR（ネットワークビデオレコーダ）を購入する際の決定要因となります。ただし、3点目として考慮すべき非常に重要な要因があります。それは、記録機器を構築する上で必要とされるIT専門知識のレベルの高さです。

通常、セキュリティ監視カメラとその記録機器（サーバ、コンピュータまたはNVR）の購入者が製品を選択する際に、コストとその製品の機能性を見て検討します。特筆すべきもう一点が、記録機器を構築する上で必要なIT専門知識の豊富さです。システムのサイバー·セキュリティも確立する必要があります。

なぜITの専門知識が必要か?

アナログカメラを映像監視に使用していた時は、ITの専門知識は必要ありませんでした。各カメラのケーブルは、セキュリティカメラとVCR（映像カセットレコーダ）の背面にある入力端子口に接続していました。ネットワーキングは関係ありませんでした。しかし今では、カメラとレコーダは高度なネットワーク機器です。そのため必要となってくるIT専門知識の内容は、カメラ台数と記録装置の種類によって異なってきます。

それぞれのシステムに必要なIT専門知識は異なりますが、セキュリティ映像記録には次の3つの方法があります。

1. NVR
2. サーバ·ベースのネットワーク映像記録システム（オンプレミス）
3. クラウド·ベースの映像記録システム

NVR

NVRは、機能と構成が固定されたコンピュータ機器です。もし修正すると製品保証が無効になります。NVRは、一定数のカメラ台数に基づいて「平均」使用のために設計および製造されています。そのため、まず画像解像度とフレーム·レートに関する各カメラの映像品質要件を満たすためのセキュリティの専門知識が必要となります。次に、特定のNVRメーカのモデルが、各カメラに求められている映像品質のカメラ台数を処理できるかどうかを判断するには、ITの専門知識が必要となってきます。

NVRの設計を評価するのにも、ITの専門知識が不可欠です。例は、多くのエントリレベルのNVRは、RAID HDD（ハード·ディスク·ドライブ）の冗長性を有していません。最新のNVRは最新の大容量HDDを使用するため、1個のHDDが故障すると、記録された映像データの半分または全てが失われます。しかも故障したHDDを交換するまで、映像を記録することができません。

また、NVRのネットワークカードの品質とスループット容量も確認する必要があります。特にNVRで映像解析を処理する場合は、NVRのマザーボードも評価する必要があります。マザーボードには、カメラの映像ストリームをデコーディングするための独立したグラフィックス·プロセッシング·ユニット（GPU）チップが含まれていますか?映像管理ソフトウェアは、GPUプロセッサ機能を最大限に活用していますか?多くのNVRは、特に映像解析が関係する場合、顧客が期待する高解像度と映像フレーム·レートを処理できません。

NVRのオペレーティング·システムを含め、映像システムのサイバー·セキュリティ保護を確立するには、ITの専門知識が不可欠です。ほとんどのNVRメーカは、デフォルトでサイバー·セキュア構成を有効にしていません。一部のNVRには、修正できないほどの重大なサイバー·セキュリティの脆弱性が存在します。また、大部分のNVRはデュアル·ファクタ認証をサポートしていません。例えば、NVRのソフトウェアにアクセスするための従来のログオン名とパスワードに加えて、クレデンシャル·カードまたはテキスト·メッセージとして送信されたコードの使用などです。

したがって、ITの専門知識を持つユーザがNVRを評価するように求められた場合、代わりにNVRではなくサーバ·ベースの記録映像を推奨することがよくあります。サーバ·ベースの記録により、顧客は記録映像サーバの構成を決定できるため、顧客の映像処理およびサイバー·セキュリティの要件に正しく適合させることができます。

サーバ·ベースのセキュリティ映像記録

サーバ·ベースの映像記録には、最高レベルのIT専門知識が必要とされます。その理由の1つは、サーバの構成が異なる市販サーバを様々なシステムで利用できるからです。ほとんどの汎用サーバは、平均使用·ビジネス用途向けに設計されています。映像システムには独特な要件があり、高性能映像システムを設計するには、映像システムの動作をよく理解する必要があります。

例えば、単一の大容量ドライブを使用するのではなく、RAIDの冗長性を利用して、複数の小型HDDで構成されるストレージ·システムを設計する方が適切です。RAIDで大容量ドライブを再構成するには、小さなドライブを再構成することよりも時間がかかります。交換ドライブが再構成されるまで、記録性能が大幅に低下します。

また、一般的に必要とされるよりも高い性能を発揮できるサーバを設計することが求められます。したがって、サーバは、RAIDの再構成時にもピーク時のトラフィックをサポートするように構成する必要があります。これらには複雑な計算が求められます。

カメラ台数が多い案件では、高性能サーバが必須となります。おそらく多くの場合、複数のサーバが必要となります。それぞれが8、10、12、または20コアの複数のCPUを使用することにより、映像処理のボトルネックになるCPUの問題を排除できます。1ギガビットまたは10ギガビット·ポートなどの複数の高速ネットワーク·ポートを使用し、帯域幅を集約することにより、サーバのネットワーク·ポートが映像入力のボトルネックにならないようにすることができます。

さらに、サーバを仮想化するため例えばVMwareを使用して、ハードウェア資源をリソース·プールに集約し、2つの仮想マシンとして共有することで、それぞれがVMS記録アプリケーションを実行します。それにより、CPU、GPU、RAM、ストレージ資源の大規模な仮想化プールを備えた大容量高速サーバを構築することができ、多くの映像ストリームの処理とその映像解析処理計算の必要に応じて共有することができます。

ストレージ資源は、2台か3台、またはそれ以上のHDDの同時損失が起きても、記録を続けるように設計されています。そして、予備のHDDは電源を落とさず、自動的に交換可能です。

このようなサーバは、映像ストリーム·トラフィックでの最悪レベルに対応できるように設計されています。例えば、絶え間なく降り続く雨のため、常時全ての屋外カメラが動体検知記録してしまう場合です。このようなサーバは、最悪の場合に備えた映像ストリーム量と映像処理のニーズに十分なリソースが利用できるように、サイズをハイスペックにしておく必要があります。これにより、ハードウェアと電気の費用の両方を上げ、更に強力なサイバー·セキュリティのコストを追加する必要があります。サーバ、仮想化、ストレージ、データベース、ネットワーキング、およびサイバー·セキュリティに関する高度な専門知識を持つIT部門は、このタイプの高性能システムを設計および維持することはできます。

ただし、初期および継続的なITと高性能機器のコストは、システムの総所有コストを大幅に上昇させます。これが、サーバ·ベースのシステムのセキュリティ映像処理機能を妥協させる主な理由です。高性能システムの作成と保守の費用は許容できません。これで合理的なコストで高性能を得るために、多くの顧客がクラウドベースの映像システムを現在検討している理由が容易に理解できるでしょう。

クラウド·ベースの映像管理システム

クラウド·コンピューティングは、高性能で可用性の高いコンピューティングを安価な値段で提供できるように設計されました。数千または数百万の顧客が、コンピューティング基盤の費用と、それに必要なITおよびサイバー·セキュリティの専門知識を共有しています。クラウド·コンピューティングの鍵となる強みがこれを可能にしています。これらは、国際標準ISO / IEC 17788：2014で定義されており、クラウド VMSに適用されるときに以下の通り要約されます。

クラウドの主な特徴

広範なネットワーク·アクセス

クラウドVMSはネットワーク経由で利用でき、標準のインターネット·ブラウザを介してアクセスできます。ユーザは、携帯電話、タブレット、ラップトップ、ワークステーションなどの様々な機器を使用して、ネットワークにアクセスできるならば、どんな場所からでもVMSにアクセスし、作業できます。

測定されたサービス

クラウドVMSの顧客には、使用した分のみの料金をお支払いいただきます。例えば、特別な会社のイベントのためだけに映像解析を使用する場合、使用するサブスクリプション期間（通常

は1か月）のみをお支払いいただきます。

マルチ・テナント

1つのVMS顧客のアカウントで、複数の顧客がリソース・プールのリソースを共有します。ただし、各顧客に割り当てられた特定のアプリケーション、コンピューティング、データベース、ストレージ、およびネットワーク資源は、他の顧客から隔離され、アクセスできません。そのため、各顧客のデータは個別に管理され、各顧客に割り当てられたリソースは他の顧客のリソース使用量の影響を受けません。各顧客のVMSは、他の顧客の使用レベルに関係なく、その高パフォーマンス性を保持します。

オンデマンド・セルフサービス

クラウドVMSの顧客は、クラウド・サービス・プロバイダとのやり取りを最小限に抑えるか、あるいは全く行わずに、必要に応じて機能を有効または無効にできます。これにより、変更を行うために必要な費用、時間、および労力が削減されます。

迅速な弾力性とスケーラビリティ

顧客のクラウドVMSに必要なコンピューティング、ストレージ、またはネットワーク・リソースが増減すると、リソースはニーズに合わせて迅速かつ弾力的に自動的に調整されます。例えば、雨が降ってより多くの映像ストレージ容量が必要な場合、自動的に提供され、新しいストレージは不要になった時に解放されます。このプロセスは顧客には見えません。一般的なオンプレミス・サーバとNVRなどのようにリソースが制限されないので、顧客には問題は生じないのです。

リソース・プール

クラウドVMSを非常に安価に手にすることができるのは、リソース・プールの機能があるからです。クラウドの物理リソースと仮想リソースをリソース・プールに集約して、複数の顧客に効率的にサービスを提供することができます。このしくみの複雑さはそれぞれの顧客には見えません。このITの専門スキルのコストは、すべての顧客に的確かつ効率的に割り当てられています。

クラウド VMSの主な利点

最適に設計されたクラウドVMSシステムの強みは、クラウド・コンピューティングのハードウェアおよびソフトウェア・リソースがセキュリティ映像の高性能のために特別に設計されていることです。クラウド・コンピューティングの規模の経済性と専用基盤を組み合わせることで、以下に列記したような機能を安価なクラウドVMSサブスクリプション費用に含めることができます。

- ホット冗長コンピューティング
- ダブルおよびトリプルの冗長性を用いた映像データ・ストレージ
- 定期的な情報セキュリティ監査
- 頻繁な脆弱性スキャンニングとサイバー・セキュリティ侵入テスト
- 自動的に適用されるアプリケーション・セキュリティの更新
- 継続的配信

継続的配信とは、ソフトウェアの各作業が完了するたびに、ソフトウェア更新を自動的にできるようにするために使用されるソフトウェア・エンジニアリング・アプローチです。更新は通常、年に1、2回ではなく、数週間ごとに行われます。

クラウドVMSオンプレミス機器

さらに、クラウド・コンピューティング機能の多くは、クラウドVMSに送信する前に映像をバッファリングするローカル設置機器にまで拡張されています。クラウドVMS機器は、自己構成型でクラウド管理されています。新しいセキュリティまたは機能の改善が利用可能になると、アプライアンスは自動的に更新されます。適切に設計されたクラウドVMSの場合、そのローカル設置機器にはルーターとファイアウォールの機能が組み込まれており、マルウェアへのカメラの感染や映像への不正アクセスを防ぎます。したがって、顧客が必要とする唯一の専門知識は、ワークステーション、ラップトップ、タブレット・コンピュータ、またはスマートフォンを使用してアプリケーションにアクセスできることだけです。サービス・プロバイダがカメラをインストールして接続するには、基本的なネットワーク知識が必要なだけです。高度なITシステムの専門知識は必要ありません。

これで、映像管理システムに必要なIT専門知識のレベルが高くないかVMS購入の重要な決定要因である理由を簡単にご理解いただけたでしょう。 a&S

■筆者紹介

ディーン・ドレイコ氏は、世界最大のクラウド・ベースの映像監視会社であるイーグルアイネットワークス社創業者。同氏は、他にも複数の優れたセキュリティ関連企業を設立。またイーグルアイネットワーク社だけでなく、クラウド・ベースのアクセス・コントロール企業Brivo社のオーナー兼会長でもある。ドレイコ氏はかつてバラクーダネットワークス社の創業者兼CEOとして、業界初となるメール・セキュリティ・アプライアンスや様々なサイバー・セキュリティ製品を開発した。同氏はミシガン大学アナーバ校電気工学科学士号、カリフォルニア大学バークレー校電気工学科学修士号を取得。金融グループのゴールドマンサックスはディーン・ドレイコ氏を「2014年の最も魅力的な起業家100人」の一人として挙げた。

連載記事連動 FAQ

質問　イーグルアイネットワークス社の専門分野は?

回答　当社は、クラウド映像監視におけるセキュリティとオペレーションを担う会社です。そして、映像監視のAPIプラットフォームと連携して、オンデマンドでVMSのセキュリティとオペレーションを提供しています。

質問　イーグルアイネットワークス社は、このビジネスを立ち上げてから、どれぐらいになりますか?

回答　当社は、2012年夏から開発に取り掛かり、2014年1月、初の製品となるEagle Eye Cloud VMSを正式に発表しました。

質問　Eagle Eye Cloud VMSは、どのようなシステム構成でしょうか?

回答　Eagle Eye Cloud VMSは、Eagle Eye Cloud Video APIをベースに設計･構築されており、アクセス･コントロール･システムなどの様々な異なるタイプのシステムに対しても柔軟に対応いたします。

質問　Eagle Eye Cloud VMSの利用方法について、どのようなハードウェアが必要ですか?

回答　当社では、ユーザの方にBridgeをオンサイト環境で導入していただきます。

質問　Bridgeとは何ですか?

回答　Bridgeとは、監視画像が保存されている当社のデータセンタに接続するための、クラウド管理型のオンプレミス装置です。Bridgeは、インターネット接続が切断された場合に備えて、映像をバッファリングします。Bridgeは、暗号化、データ重複排除、帯域幅管理、動体分析、映像圧縮なども行います。

質問　現在NVRとIPカメラ16台のシステムを稼動しています。現在のシステムのデータのバックアップとして貴社のクラウドVMSと連動させることは可能でしょうか?

回答　はい、バックアップ目的でNVRシステムをEE Cloudに接続することができます。弊社には、Eagle Eye Cloud Replication用の特別な製品がございます。EE Cloudバックアップのコストは、保持期間とカメラの解像度によって異なってきます。この際に必要なハードウェアは、Eagle Eye Bridgeです。詳細については、当社までお問い合わせください。

質問　現在使用しているNVRとIP カメラにバックドアが付いているため、データの漏洩を懸念しています。データ漏洩を防ぐために貴社のクラウド VMS を導入することは可能でしょうか。その場合、設定期間はどのくらいかかりますか?

回答　Eagle Eye Cloud VMSは、ほとんどのNVRやDVRとは異なり、強力なサイバー･セキュリティが特徴です。Eagle Eyeアーキテクチャは、カメラをインターネットから隔離し、サイバー･セキュリティも保証します。Eagle Eye Cloud VMSの設置時間は通常30分が目安です。

質問　まず現在稼働中の NVR にある過去のデータだけを貴社クラウド VMS に移行して、契約期間が終了してから、システム全体をクラウド VMS に移行することは可能でしょうか?

回答　通常、NVRとDVRはクローズ･ドソリューションであり、このためのオープンAPIがないため、古いNVRまたはDVR映像をEagle Eye Cloudにアップロードすることはできません。Eagle Eye Cloud VMSを並行して稼働させ、契約期間の終了時にシステムの切り替えを完了することをお勧めします。

質問　現在使用している NVR ベースの監視システムと同等の内容で構築していただくことは可能でしょうか?

回答　はい可能です。

質問　NVR と IPカメラ8台のシステムを貴社クラウド VMS に移行する場合の構築期間と概算はどのくらいですか?

回答　NVRおよびIPカメラ8台の場合、切り替えは通常30分以下で完了します。お客様に掛かる月額費用は低コストに抑えられます。システム内容により概算が変動しますので、詳細については当社までお問い合わせください。

イーグルアイネットワークス株式会社
〒150-0034 東京都渋谷区代官山8-5　代官山8.5 ビル4階
TEL:03-6868-5527　E-MAIL:APACsales@een.com

9月

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

10月

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

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

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

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

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

SECUTECH THAILAND
会期：2019年10月28日～ 30日
開場：10:00 - 17:00
会場：バンコク国際貿易展示場(BITEC)
　　88 Bang Na-Trat Rd, Khwaeng Bang Na, Khet Bang Na, Krung Thep Maha Nakhon 10260
主催：Messe Frankfurt New Era Business Media Ltd.
URL：www.secutechthailand.com

11月

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

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

2020年1月

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

2020年3月

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

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

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

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

ISC WEST
会期：2020年3月18 ～ 20日
開場：10:00 - 17:00
会場：米国ネバダ州ラスベガス
　　サンズエクスポ
主催：Reed Exhibitions
URL：https://www.iscwest.com/

2020年4月

SECUTECH Expo　2020
会期：2020年4月22日～ 24日
開場：10:00 - 18:00(最終日は17:00)
会場：台北南港國際展覧館
　　台湾台北市南港区経貿二路1号
主催：Messe Frankfurt New Era Business Media Ltd.
URL：https://10times.com/secutech-expo

2020年5月

SECUTECH INDIA 2020 & Fire and Safety India 2020
会期：2020年5月7日～ 9日
開場：10:00 - 17:00
会場：ボンベイ･エキジビション･センター
　　インド共和国ムンバイ市
主催：Messe Frankfurt New Era Business Media Ltd.
URL：http://secutechexpo.com/index

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

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

読者の声

サイバー攻撃の恰好の餌食になる要因となるバックドアを装備している製品の公表を

サーバー攻撃のうちマルウェアは、管理者側の対策と防御で一定の防御が可能だと言われている。しかし、バックドアを仕込まれた機器に対しては、どのようにすればよいのだろうか。

最も確実な方法は、バックドアが仕込まれている製品を採用しないことだろう。しかし、その情報はどこにあるのかが、一般ユーザにはわからない。政府や中央機関でも、具体的なメーカ名や製品名を発表していない。これで民間を含めた組織の安全が守られているとは到底思えない。さらに言及すれば、販売側がその意識を持っていないか、営業上支障をきたすことになるからか、ダンマリを決め込んでいる。

日本政府は、民間企業を含むすべての組織に対して、情報漏洩や搾取さらにはシステム破壊を招くバックドアに対して情報を公開する責務があると考えるのは私だけだろうか。

(東京　公務員)

5Gの登場で映像監視システムはどのように変わるのか

既に米国や韓国で商用化されている5Gは、2020年には日本でも一般での利用が開始されるという。またLAN環境での導入は試験的に開始されているという。LANでの使用であれば、外部との遮断が容易だろうから問題点も限られるだろう。

しかし、利用が本格化した場合、映像監視システムやセキュリティ統合システムはどのように進化するのだろうか。また、既存システムに導入するにはどのような点を考慮すべきなのだろうか。特に社会インフラにおける導入では、想定することができる様々な利点と留意点が明らかにすべきだろう。つまり、新しいテクノロジーは導入する前に十分な検証が不可欠となるだろう。

このテーマについては、ぜひ貴誌で特集記事として取り上げていただきたい。おそらく既に活用している米国市場での提供側からの提案や実際の導入事例を紹介していただき、日本における導入時に参考になる情報を提供していただきたい。

（千葉　ソフトウェア開発業）

「読者の声」を募集しています。

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

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

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

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

secutech
THAILAND

2019年10月28-30日
タイ王国バンコク

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

www.secutechthailand.com

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

Concurrent with:

thailand lighting fair　thailand building fair

WORLDEX
Group of Exhibition Companies

messe frankfurt

第28回 セキュリティ・安全管理総合展

SECURITY SHOW 2020

出展申し込みはウェブサイトで!
申込締切日:2019年10月15日(火)

http://www.securityshow.jp/

日本のセキュリティが進化する4日間

2020年 3月3日(火)▶6日(金) 幕張メッセ[1・2・3ホール]

NIKKEI MESSE 街づくり・店づくり総合展

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

主催 日本経済新聞社