IPカメラの最新動向

要約:
　IPカメラは従来のアナログ監視カメラの単純な代替ニーズから、監視画像を積極的に活用する映像IoTへと利用ニーズが変化してきている。近年ではより高度化されたAIとの連携により、これまでの受動的な監視から積極的なサービスを提供する手段としての活用方法へと進化している。
　本セッションでは最新のIPカメラの活用例と、これを支えるHATSにおけるIPカメラシステムの相互接続性やセキュリティを確保するための取り組みについて説明する。

2019年12月6日
HATSフォーラム
マルチメディア通信相互接続試験実施連絡会
IPカメラ接続TSG主査　　中島　幸宏

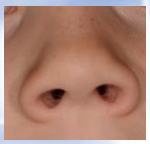
目次

1．カメラは視覚

■　人間が行動する際に必要とする情報は主に視覚・聴覚・嗅覚・触覚・味覚の5感から得ている。IoTシステムにおける感覚情報はこの5感に相当するセンサーを用いて情報を収集している。しかし、これまでのセンサーはある目的に特化した情報しか得られない。


視覚 ⇒ 83%

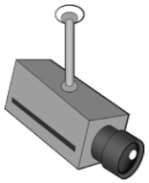

聴覚 ⇒ 11%


嗅覚 ⇒ 3%


触覚 ⇒ 2%


味覚 ⇒ 1%

従来のセンサーでは20%程度の情報しか得られない



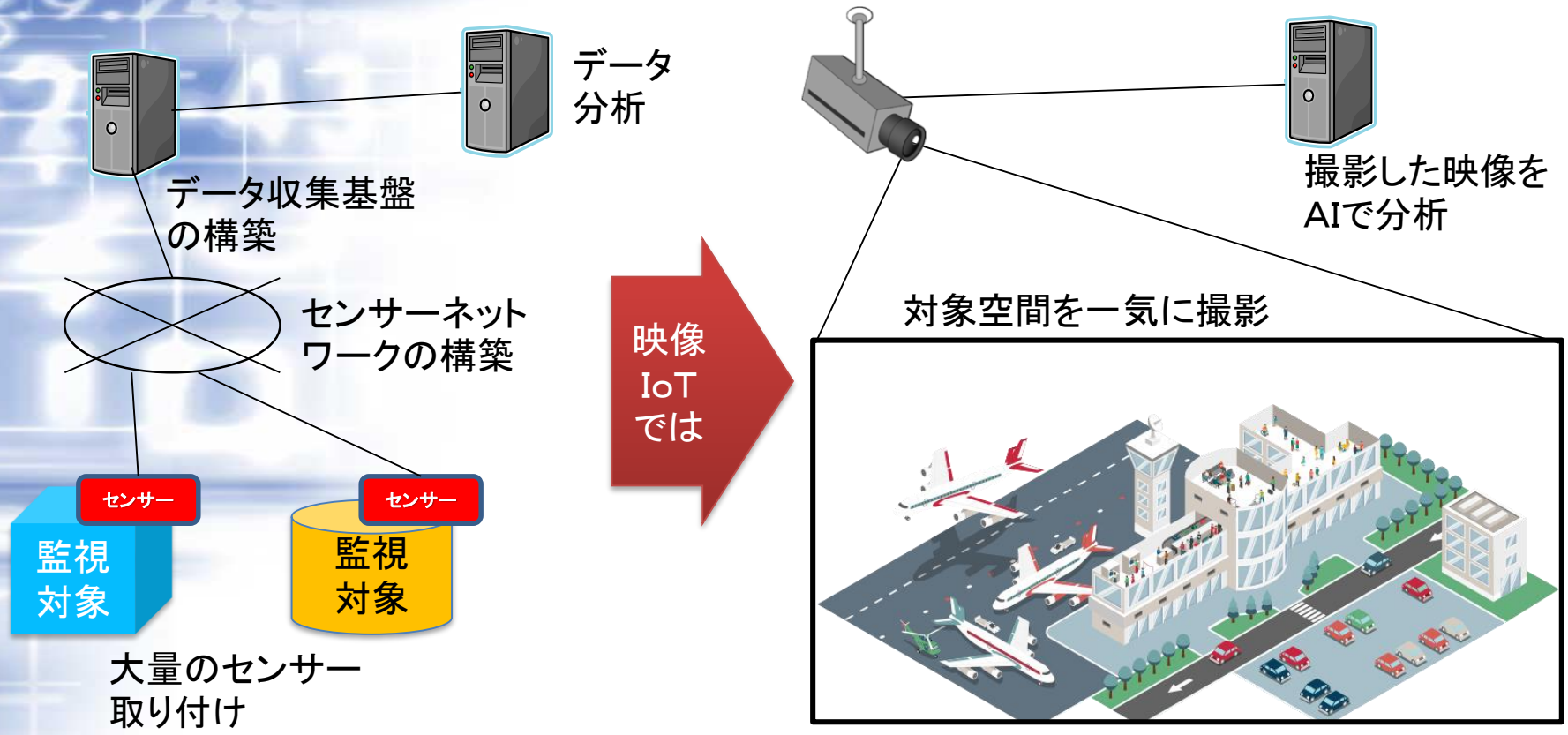
IPカメラは人間の視覚以上の情報を得られる

例：赤外線、望遠。。。。

IPカメラは人間の視覚に相当し、非常に多くの情報を得ることが出来るデバイスであり、使い方次第で従来のセンサーでは困難であった情報を得る事が可能

２．ＩＰカメラのメリット

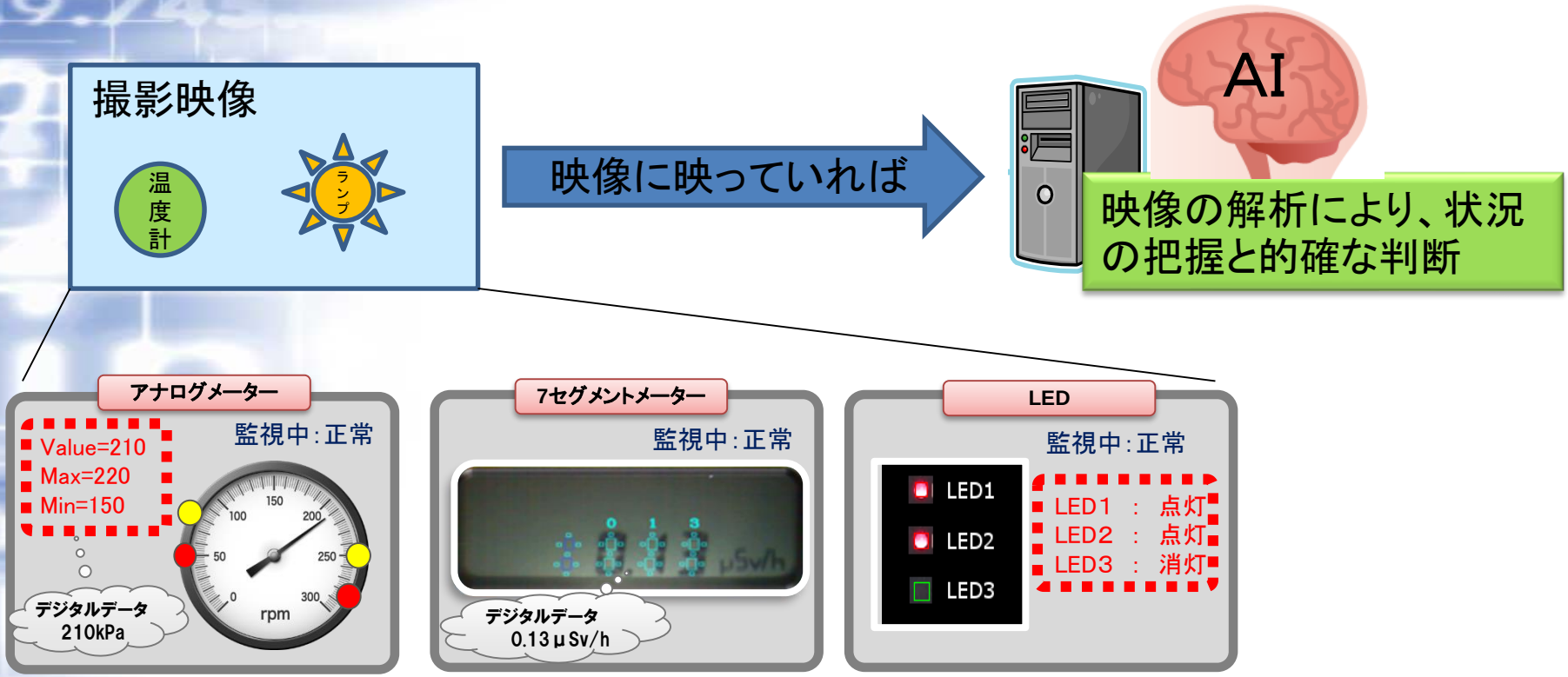
■　これまでのIoTでは、監視・管理対象に目的に沿ったセンサーを取り付け、さらに大量なセンサーのネットワークを構築する必要があった。



IPカメラ活用による「映像IoT」では、カメラ一つ取り付けるだけで空間全体をセンシングすることが可能となる。

３．ＩＰカメラはＡＩの目

■　IPカメラとAIによる「映像IoT」では、人間が目で見て判断して運用していた業務は現状の環境そのままに、容易に自動化へ移行する事ができる。

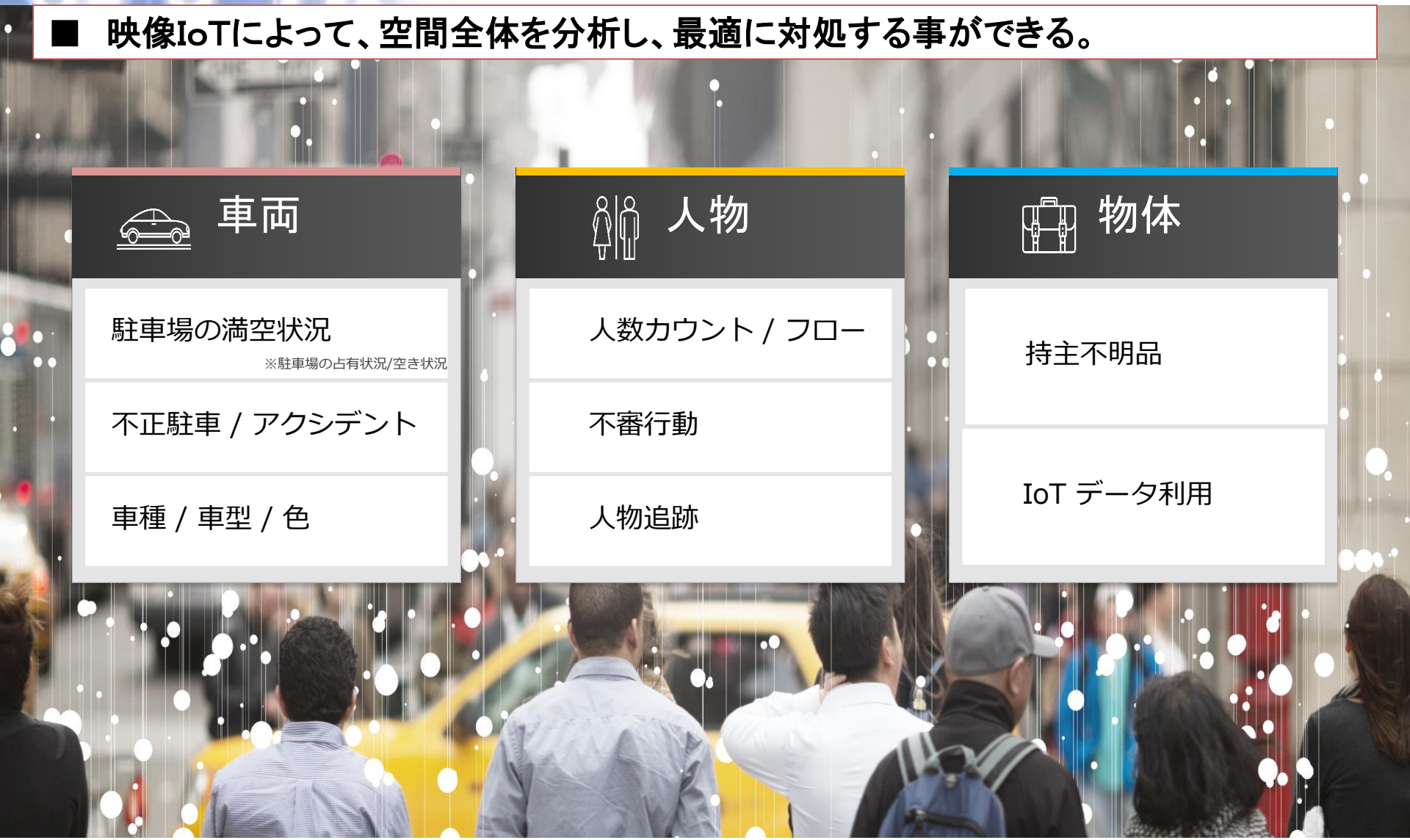


IPカメラによる映像IoTでは、AIで認識・判断するため人為的なミスは解消し、大量・高速な処理が可能となる。

4．都市全体を最適化

Harmonization of Advanced elecommunication Systems HATS

■ 映像IoTによって、空間全体を分析し、最適に対処する事ができる。



車両

- 駐車場の満空状況
  ※駐車場の占有状況/空き状況
- 不正駐車 / アクシデント
- 車種 / 車型 / 色

人物

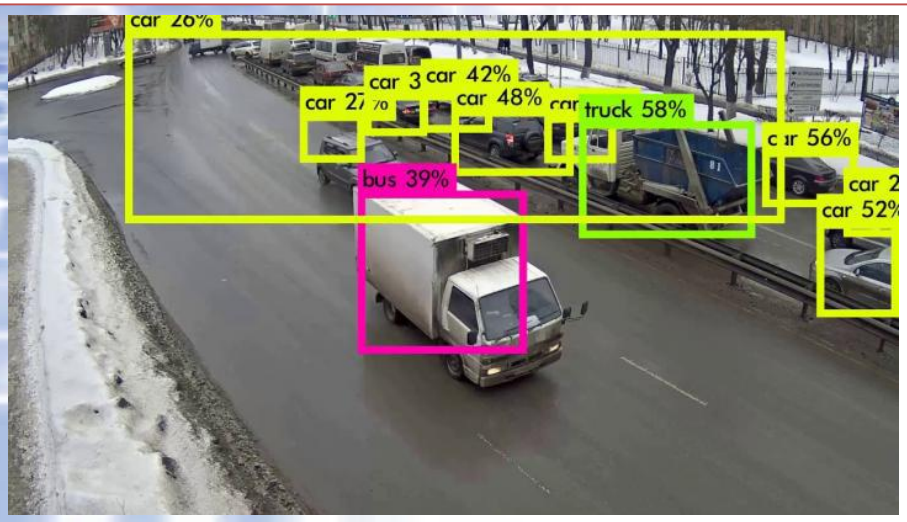
- 人数カウント / フロー
- 不審行動
- 人物追跡

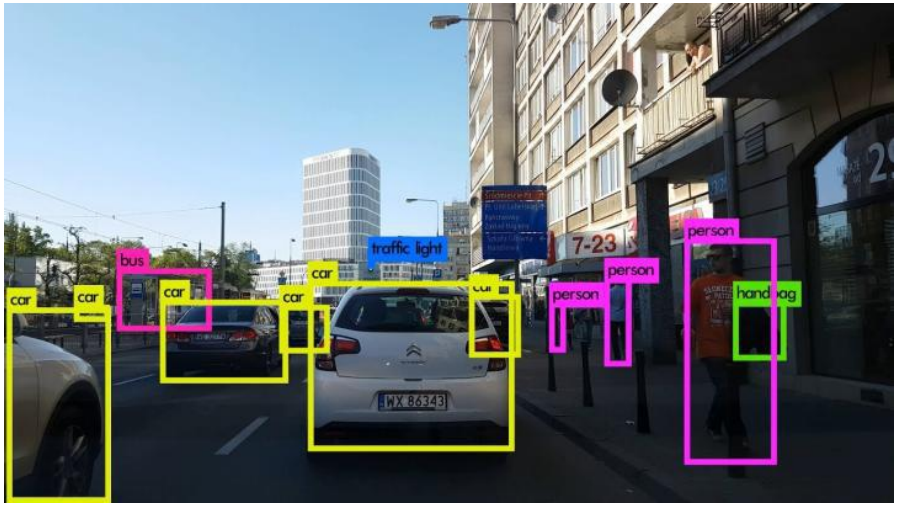
物体

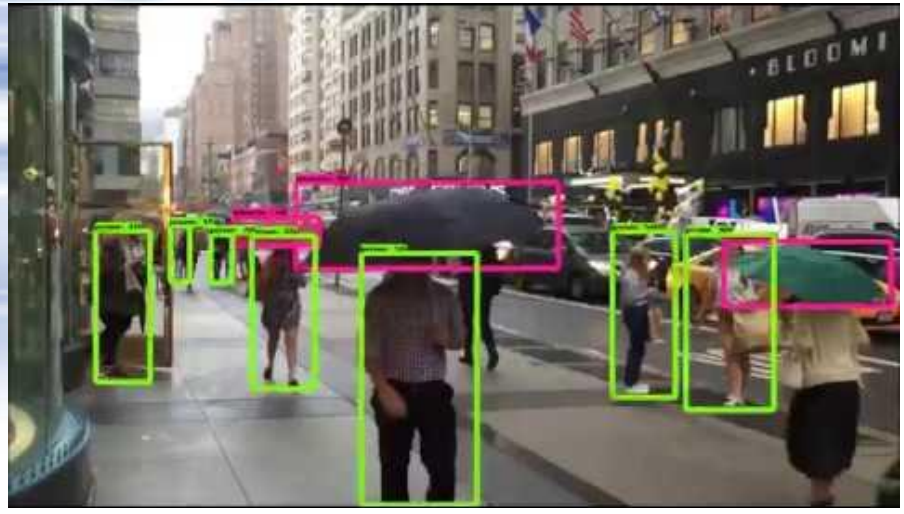
- 持主不明品
- IoT データ利用

５．街頭カメラの活用例

■ 従来は防犯目的の街頭カメラも、AIとの連携により各種の統計や監視に活用できる。



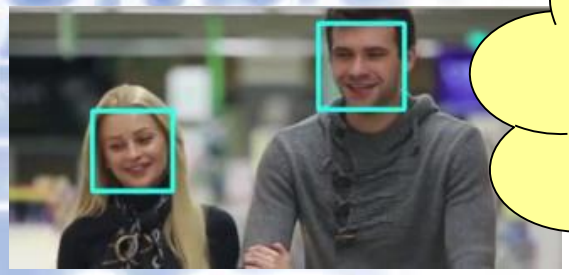




- 道路の通行量や混雑状況の把握
- 不正駐車の監視（自動的にアラーム）
- 特定車両の追跡
- 人物の追跡

6. 顔認識の活用例

■ 顔認識データベースにより、顧客情報を店舗間で共有。

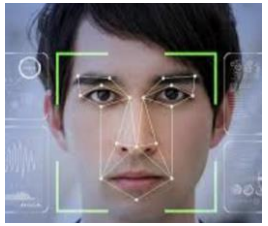


顧客情報の共有でより良いサービスを提供

✓VIP顧客の来店

✓会員カード不要のサービス提供

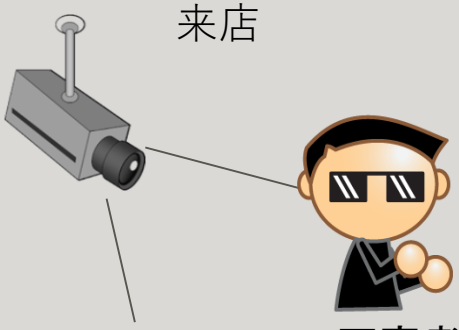
✓White list / Black list の共有とアラーム



Deep Learningにより少ないピクセルで正確に判断が可能に！

7．行動認識による防犯

システム導入前



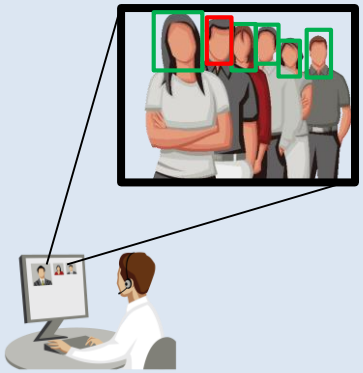
カメラ監視のみ
(入店確認)

売り場を徘徊商品を物色

不審者

盗難後に
気づく。

システム導入後



カメラ監視で予知
(盗難前に確認)

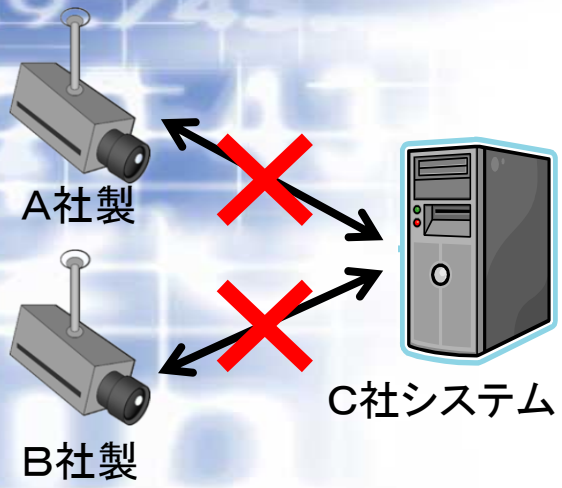
売り場を徘徊商品を物色
(警備等の近寄りや声掛け)

犯罪抑止

８．ＩＰカメラの標準化

Harmonization of Advanced Telecommunication Systems HATS

■　これまでのカメラシステムはメーカ独自の機能を追及し、メーカ間の製品を混在した運用が困難であった。このため、カメラ映像を統合的に利用する事が難しかった。



標準化

ONVIF（Open Network Video Interface Forum）

ONVIFはネットワークカメラ製品のインターフェースの互換性を広げるために作られた規格標準化フォーラム

- マルチベンダで構成されたシステムの相互運用性確立を目的に活動
- 2008年にアクシスコミュニケーションズ、ボッシュ、ソニーの3社で設立
- 世界500以上の団体が会員として活動、4500以上の機種・ソフトが準拠認定取得
- オープンかつスケーラブルなシステムを目指し、ITの標準化された技術（Webサービス、SOAP、WSDL）を積極活用

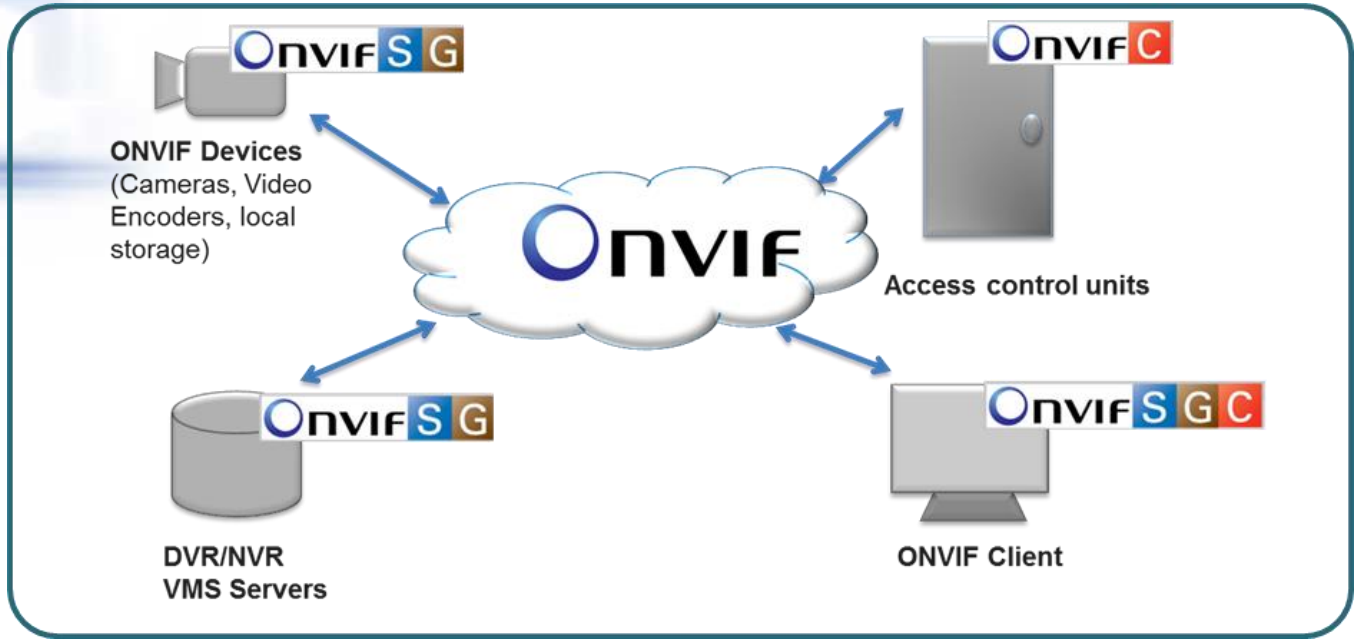
どのメーカーの製品も繋がる環境なら全ての映像を無駄なく活用でき、トータルで投資・運用コストを抑えることができる。

9. ONVIFとは

■ ONVIFはネットワークカメラ製品のインターフェースの標準化を推進中。

◆ プロファイルの導入(互換性のある機能の特定が容易)

- ✓ Profile S: ストリーミング (2012年12月公開)
- ✓ Profile C: アクセスコントロール (2013年)
- ✓ Profile G: ストレージ (2014年)
- ✓ Profile Q: セキュリティ検出 (2016年)
- ✓ Profile A: アクセスルール (2017年)
- ✓ Profile T: ストリーミング高度化 (2018年)



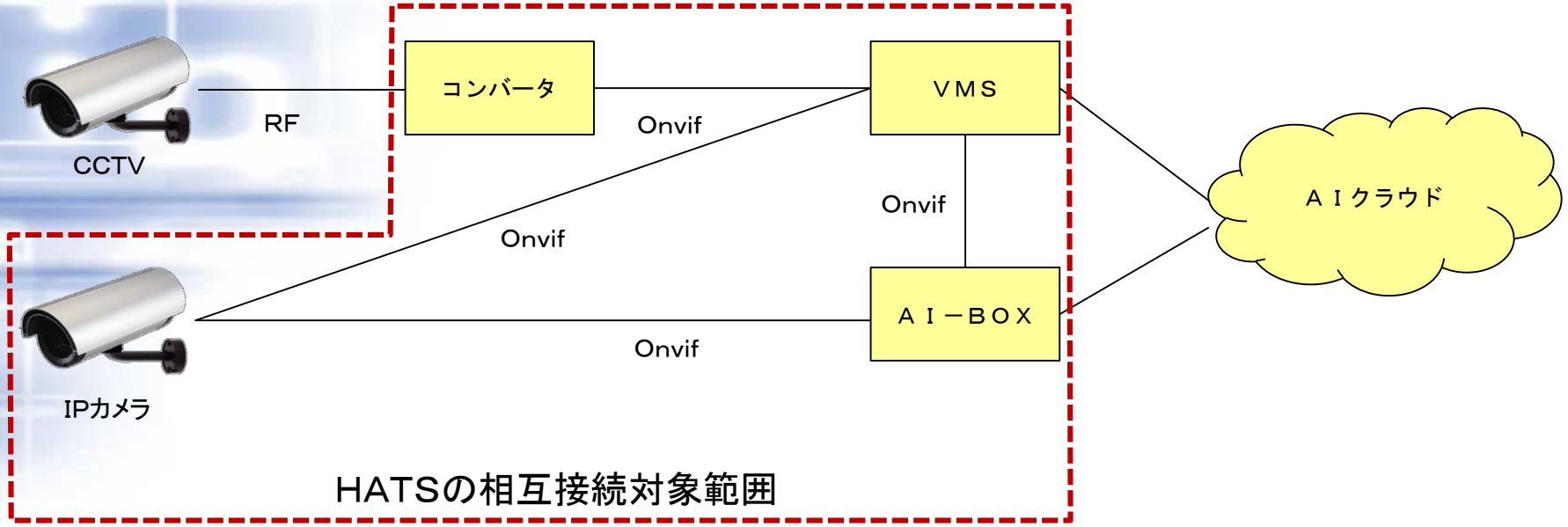
１０．複雑化するカメラシステム

Harmonization of Advanced Telecommunication Systems HATS

■ 映像情報はAIの進化と共に相互連携が不可欠。標準による相互接続性は重要。

■ 従来はカメラとレコーダのみのシンプルな構成

■ 近年では大規模な相互接続と、コンピュータシステムとの接続により構成が複雑化



１１．ＨＡＴＳの取り組み

Harmonization of Advanced Telecommunication Systems HATS

■　監視などに応用されるIPカメラと、これを利用した監視システムの構築に必要な、レコーダー、そのほかさまざまなセンサーや周辺機器などに関して、システムの構築を容易かつ確実に行えるように相互接続性の確保と、問題点の抽出をおこなう。

当面の課題

ONVIFで標準化が進められている仕様に関して、相互接続性の評価を通じて仕様に対する要望、改善点、追加機能などの提言をまとめる

相互接続とONVIFとの連携について

- 2012年度より、ONVIFとHATSは協力関係を構築
- HATSでは、相互接続試験をONVIFとは四半期ずらして実施
- 第7回 ONVIF Plug Fest（2012年9月）を日本国内にて共催
- その後3回試験を行い、最近では2017年3月に接続試験を実施

１２．ＩＰカメラのセキュリティ

もともと監視カメラは閉鎖空間で運用されていた

IoTの広がりで

サイバーセキュリティの対象へ

「IoT」という言葉が一般に用いられるようになる中、インターネットに接続される機器が普及するとともに、そのセキュリティに対する関心も高まっています。
監視カメラシステムにおいても、一般向けや業務向けの製品問わず、監視カメラやレコーダ装置、管理装置などをインターネットに接続するケースが増加しており、設置者が意図しない第三者による映像閲覧等、各種のセキュリティに対する脅威の事例がTVニュースなどで取り上げられるなど、社会的な関心を集めています。

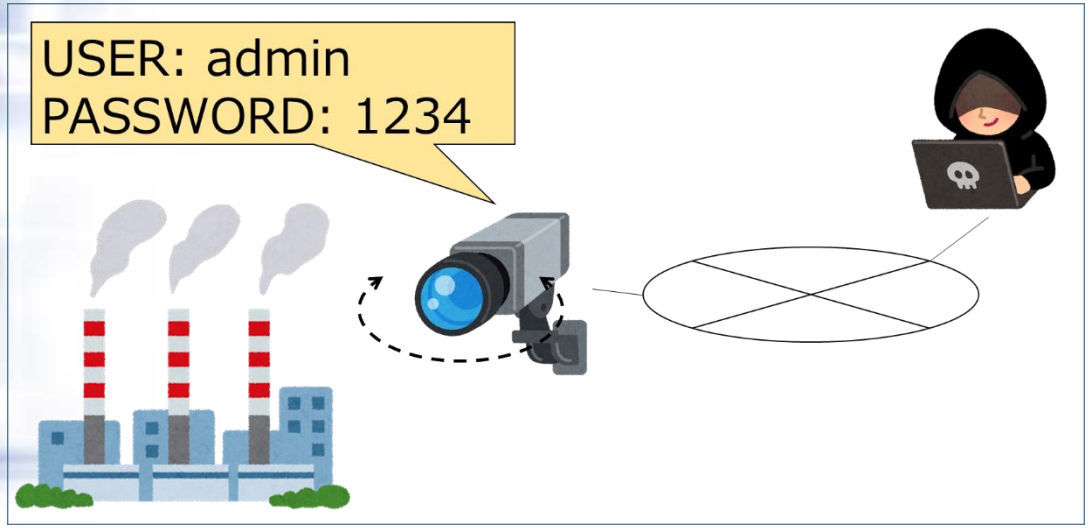
IPカメラもPCと同じ、情報機器です！！

HATS／CIAJでは、IPカメラのセキュリティ事故の事例を分析し、対策のガイドラインの広報活動を行っています。

１２－１．カメラ乗っ取り対策

事例1

初期パスワードや脆弱なパスワードの利用に起因する、第三者による映像不正閲覧・PTZ等の機器操作



監視カメラなどに初期設定されたユーザ名やパスワードは、メーカ毎にほぼ決まっていたり、WEBサイトなどから入手可能な説明書に掲載されているなど、誰でも知ることができると考えるべきでしょう。

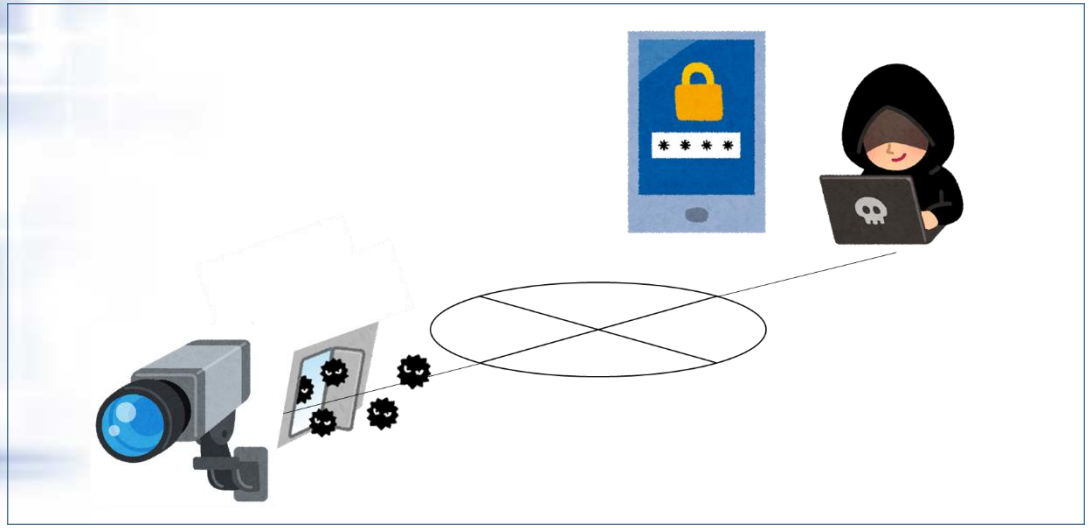
機器導入時には、必ずデフォルト以外の類推が困難なパスワードの設定を徹底しましょう。

１２－２．機器脆弱性対策

Harmonization of Advanced Telecommunication Systems HATS

事例2

脆弱性のあるファームウェアによるユーザID・パスワード漏えい



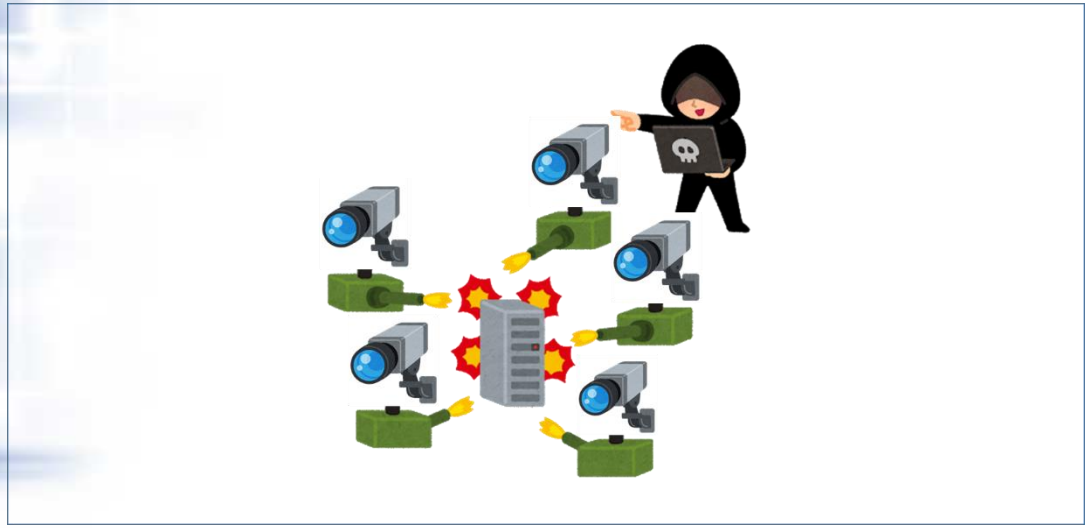
ユーザIDやパスワード、あるいは、それらを類推可能な情報がネットワーク上に流れたり、URIなどに含まれてしまうなどの脆弱性をもつファームウェアが監視カメラなどの機器に適用されていた場合、悪意のある第三者は、それらの脆弱性を利用して、ユーザ名やパスワードを入手することが可能です。

機器導入時には、必ずファームウェアが容易に更新できるものを選択すると共に、メーカのHPなどで脆弱性情報の提供がされている事を確認しましょう。

１２－３．ＤＤｏＳ対策

事例3

不正なファームウェア適用による「踏み台」化



事例1や事例2に示したような手段でユーザIDとパスワードを入手することにより、悪意のある第三者が監視カメラのファームウェアの更新機能を利用したり、ファームウェアの脆弱性を利用することによって、対象となる機器に不正なファームウェアを適用し、他のシステムに対するDDoS攻撃の踏み台として利用するなど、第三者への攻撃に意図せず加担してしまいます。

システム構築時には、必要が無ければ外部ネットワークから分離するか、外部ネットワークとの接続時は、ルータやファイアウォールの設置を推奨します。

１２－４．FIDOセキュリティ

■ 最新の機器ではFIDOに対応したIPカメラやVMSシステムも登場してきた。

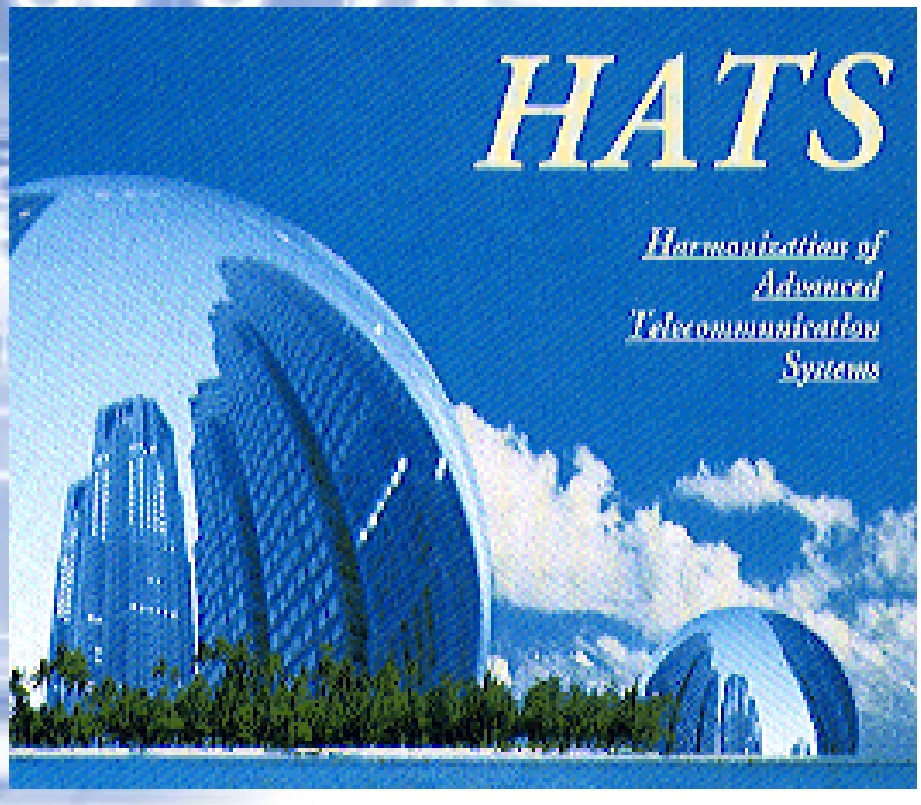
fido ALLIANCE simpler stronger authentication

FIDO（ファイド）は本人確認とサーバ認証を分けており、ネットワークに認証情報を流さず、サーバにも保管しないので、パスワードが漏洩するリスクがありません。

サービス

セキュアなLogin

FIDOキー



マルチベンダ化が進む中で
さまざまな高度情報通信機器を
安心して導入いただける環境作り
それがHATSの仕事です

Thank you !

HATSフォーラムに関するお問い合わせは下記にお願い致します。

高度通信システム相互接続推進会事務局
一般社団法人　情報通信ﾈｯﾄﾜｰｸ産業協会(CIAJ)
TEL：03ー5962－3452（笹野）
E-Mail：j-sasano@ciaj.or.jp
〒103-0026 東京都中央区日本橋兜町21-7　兜町ユニ・スクエア6F