

IoTセンサとしてのIPカメラとセキュリティ

要約:

情報通信インフラの高度化に伴い、あらゆるモノが情報ネットワークに接続されるIoTが本格化している。近年では従来のIoTで使われるセンサに代わって、より情報量の多いIPカメラを活用した「映像IoT」が広がってきている。

本セッションではIoT分野における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。

2018年10月17日

HATS推進会議

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WG主査 中島 幸宏

目次

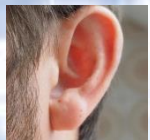
1. センサーと情報量
2. IPカメラのメリット
3. 映像IoTの背景
4. 既存の環境はそのまま
5. 都市全体を最適化
6. 行動認識による防犯
7. IPカメラの標準化
8. ONVIFとは
9. HATSの取り組み
10. IPカメラのセキュリティ

1. センサーと情報量

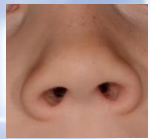
■ 人間が行動する際に必要とする情報は主に視覚・聴覚・嗅覚・触覚・味覚の5感から得ている。IoTシステムにおける感覚情報はこの5感に相当するセンサーを用いて情報を収集している。しかし、これまでのセンサーはある目的に特化した情報しか得られない。



視覚 → 83%



聴覚 → 11%



嗅覚 → 3%



触覚 → 2%



味覚 → 1%



IPカメラは人間の視覚以上の情報を得られる

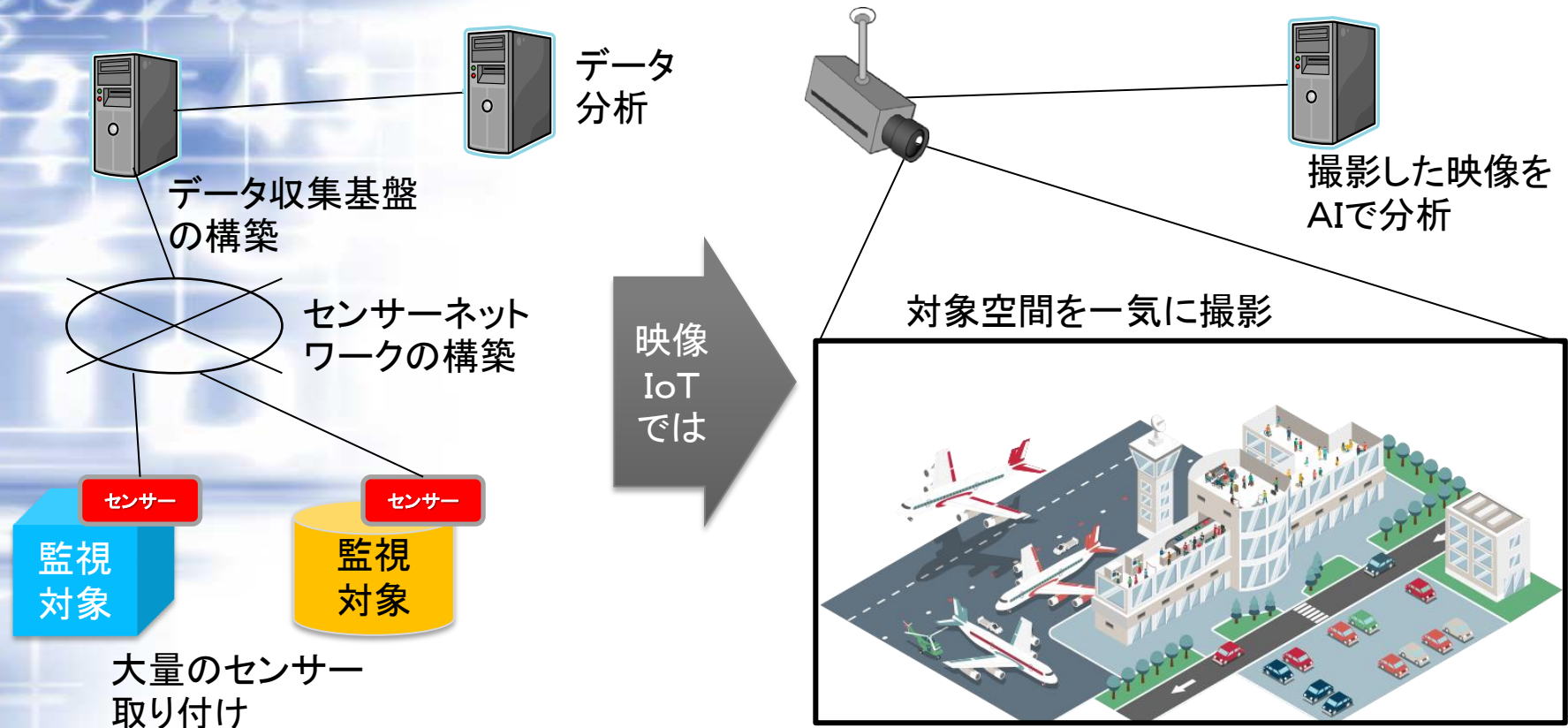
例：赤外線、望遠。。。。

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. 映像IoTの背景

■ これまでIPカメラは従来のCCTVと同様に監視カメラとして、主に防犯目的で映像を記録保存する用途が一般的。しかし、IoTの広がりと共に状況は変化している。

これまでの状況

帯域問題

- ・ 映像データは容量が大きく、伝送が大変
- ・ 通信回線の無い場所では使えない
- ・ 大量のデータを保存・処理するのが大変

画像の分析

- ・ 最終的に映像を人間が見て判断
⇒ 監視用途以外ではメリットが少ない

現在では

インフラの整備

- ・ 光回線の速度向上・低価格化・網羅性向上
- ・ WiFiや4G無線など、無線インフラの整備
- ・ クラウドサービスの発展

ICT技術の向上

- ・ コンピュータの処理能力の向上
- ・ AI技術の発展 ⇒ 実用レベルに
- ・ クラウドサービスの発展

通信インフラの発展と、コンピュータの高速化やストレージの大容量化に加え、AI技術の飛躍的な発展と、映像処理技術の向上により映像IoTが実用的に

4. 既存の環境はそのまま

■ 映像IoTでは、人間が目で見え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、専用センサーは不要。既存のメーター類をそのまま活用できる。

5. 都市全体を最適化

■ 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



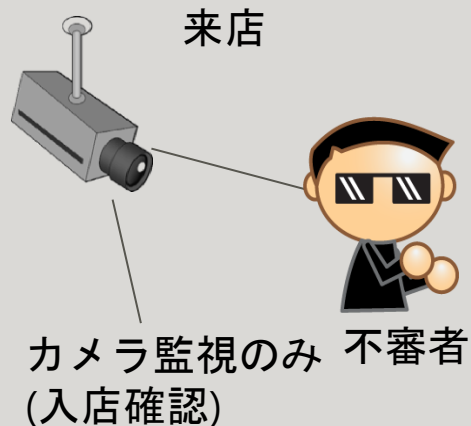
物体

持主不明品

IoT データ利用

6. 行動認識による防犯

システム導入前

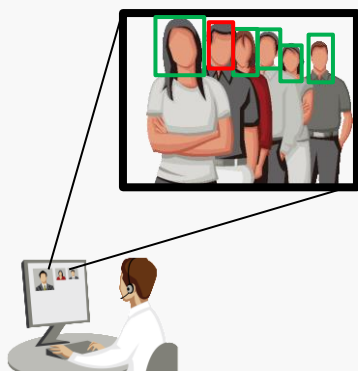


売り場を徘徊商品を物色



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)



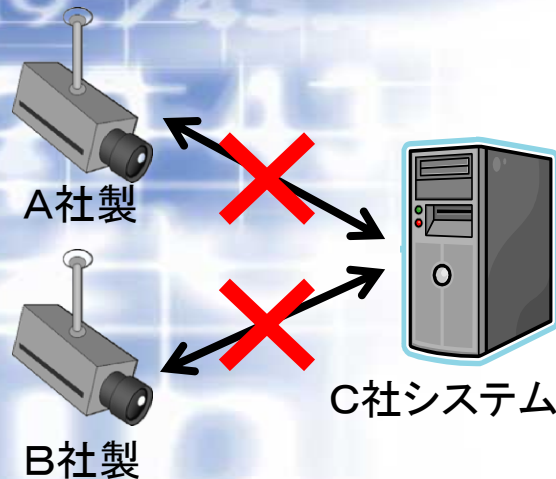
売り場を徘徊商品を物色
(警備等の近寄りや声掛け)



犯罪抑止

7. IPカメラの標準化

■ これまでのカメラシステムはメーカー独自の機能を追及し、メーカー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。



ONVIF (Open Network Video Interface Forum)

標準化

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

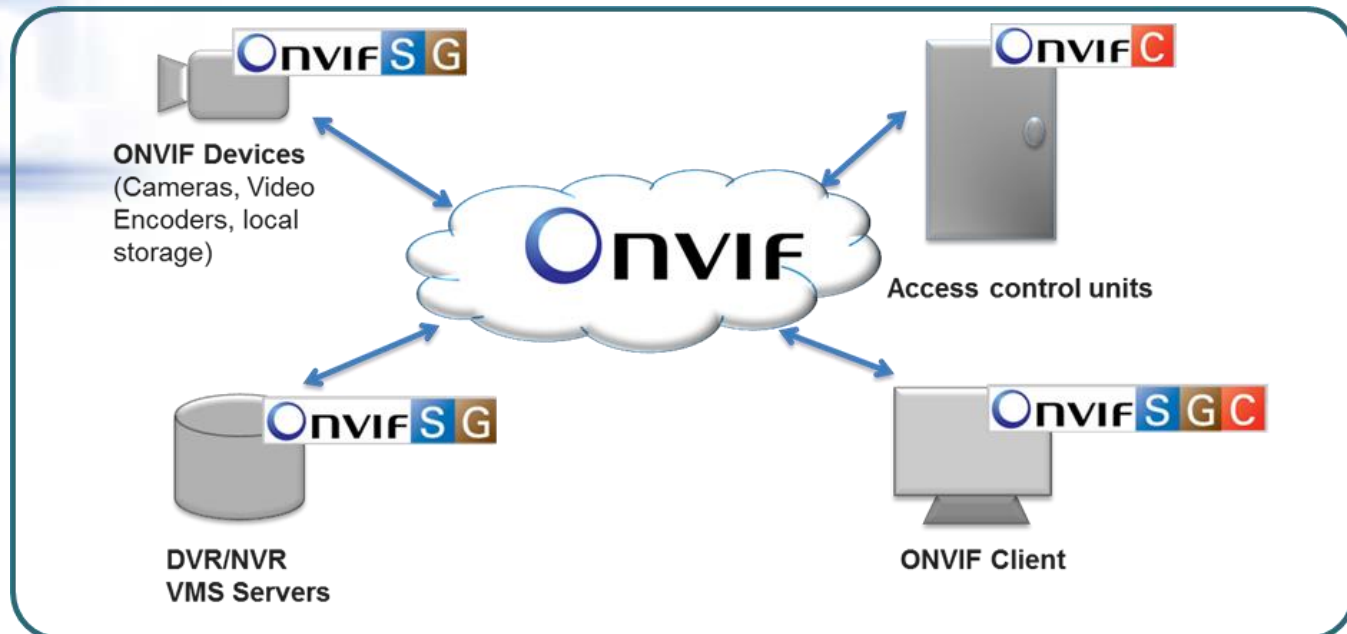
どのメーカーの製品も繋がる環境なら全ての映像を無駄なく活用でき、トータルで投資・運用コストを抑えることができる。

8. 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)



9. HATSの取り組み

■ 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でき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

10. 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

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。

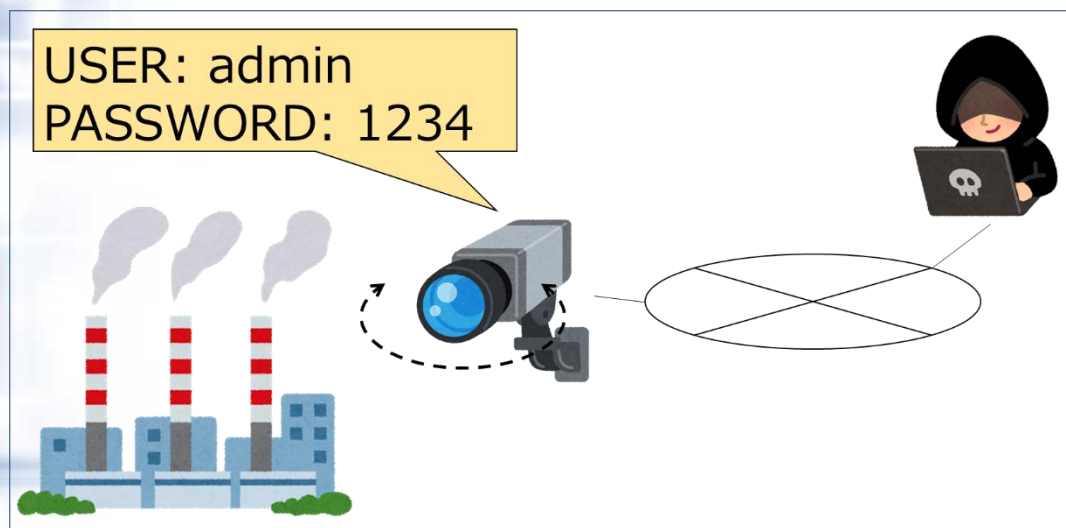
IPカメラもPCと同じ、情報機器です！！

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。

10-1. 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



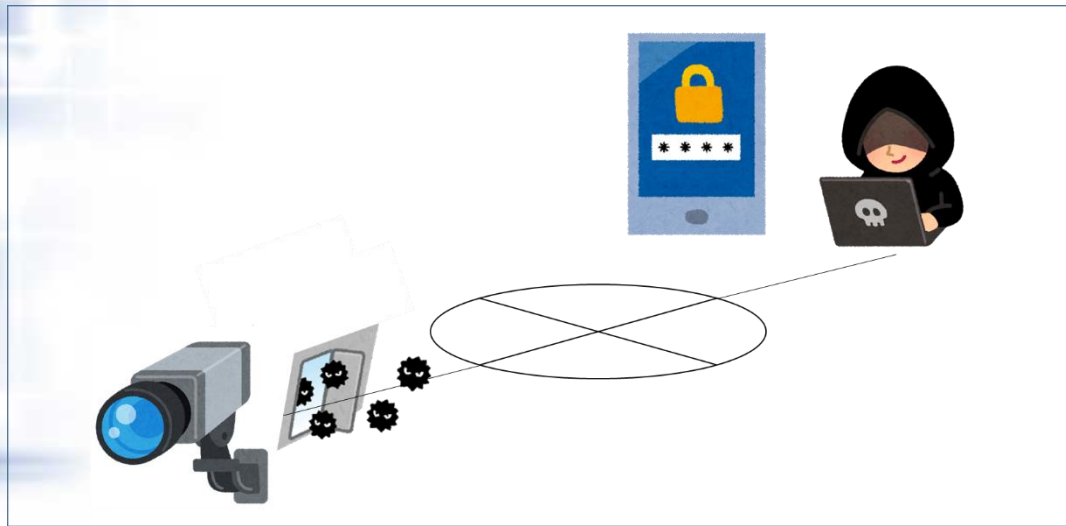
監視カメラなどに初期設定されたユーザ名やパスワードは、メーカ毎にほぼ決まっていたり、WEBサイトなどから入手可能な説明書に掲載されているなど、誰でも知ることができるべきでしょう。

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。

10-2. 機器脆弱性対策

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



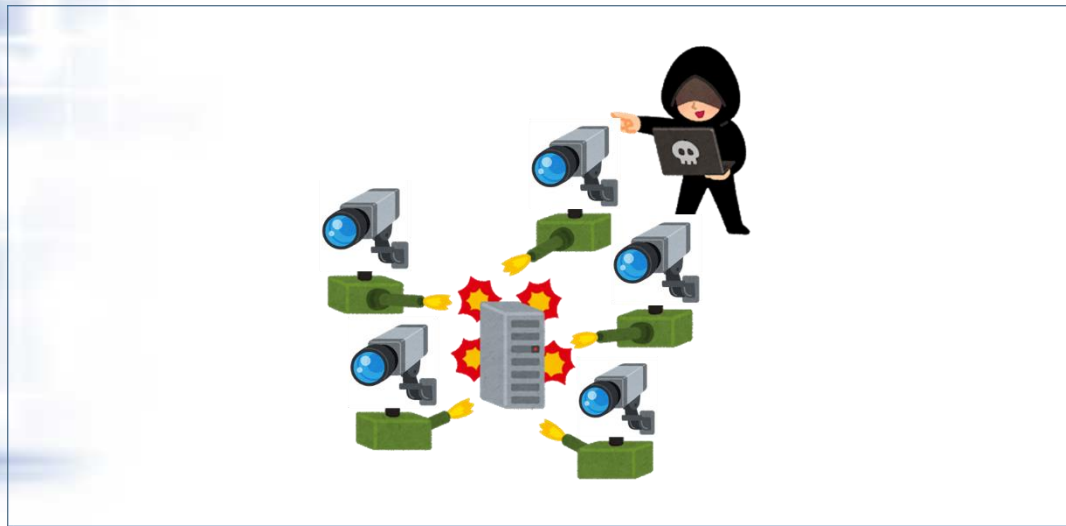
ユーザIDやパスワード、あるいは、それらを類推可能な情報がネットワーク上に流れたり、URIなどに含まれてしまうなどの脆弱性をもつファームウェアが監視カメラなどの機器に適用されていた場合、悪意のある第三者は、それらの脆弱性を利用して、ユーザ名やパスワードを入手することが可能です。

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、メーカーの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。

10-3. 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。



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

**Hall 2(A064)HATS PLAZAにて
実機デモと最新動向を展示中**

Thank you !

HATS推進会議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:03-5403-9354 (笹野)

E-Mail: j-sasano@ciaj.or.jp

〒105-0013 東京都港区浜松町2丁目2番12号 JEI浜松町ビル3F