NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IoT Security WG Report 2016
(2015年度:2015～2016)

コンシューマ向け IoT セキュリティガイド
(1.0版)

NPO 日本ネットワークセキュリティ協会
IoTセキュリティWG

2016年 8月 1日

改版履歴

2016年 6月 24日　　1.0版 公開

IoT Security WG Report 2016

はじめに

近い将来、多数のIoT製品が相互に接続され通信しあって生活や社会のインフラとして機能するようになります。そして、従来のITでは実現できなかった、個人の行動や状況にあわせたきめ細かい情報処理と最適制御が実現します。

それにともなって、セキュリティはIoTの重要な要素となります。しかし現状では、セキュリティの実現と実践を一般の利用者に任せるのは困難です。このため、IoT製品やシステム、サービスを提供する事業者の側が利用者のセキュリティ対策を設計時から作り込み、利用者に情報提供する必要があります。

このようなIoTセキュリティの課題を踏まえ、2014年に本WGは活動を開始しました。コンポーネントベンダーやシステムインテグレータ、サービス提供事業者などを交えて情報収集や議論を行った上で、IoTに関連するさまざまな仕様や規格、技術ドキュメント類を俯瞰し、それらをどのように整理するべきかを議論しました。そして、実際のIoTの利用形態を分析し、IoT利用者を守るためにIoT製品やシステム、サービスを提供する事業者が考慮しなければならない事柄を「コンシューマ向けIoT　セキュリティガイド」としてまとめました。

このガイドがIoTのセキュリティ向上の一助となれば幸いです。

IoT Security WG メンバー一同

IoT Security WG Report 2016

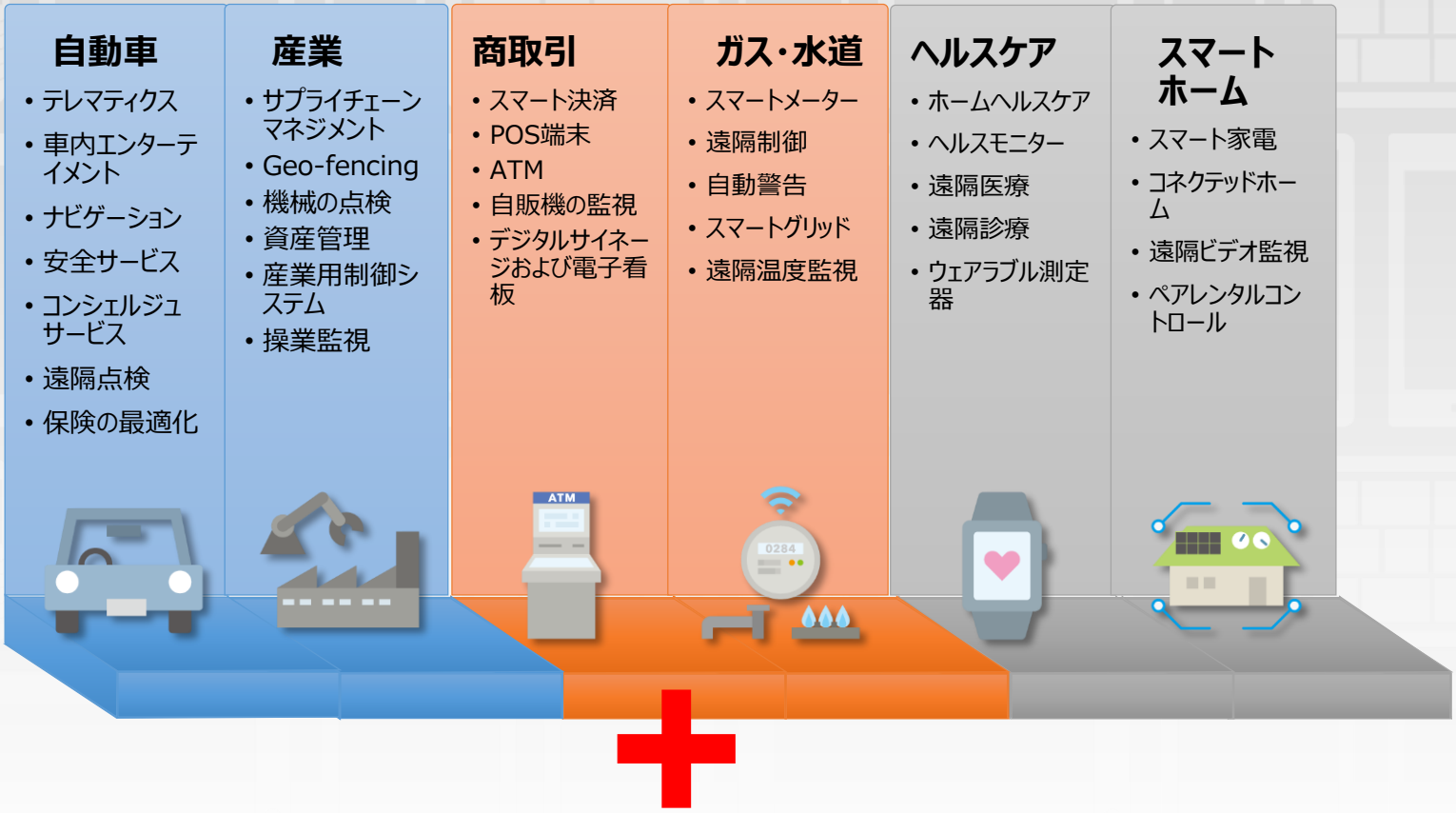
●目次

1. Internet of Things(IoT)の概要

IoT は提唱する人や組織によってあり方や適用範囲、技術が異なり、玩具から電力網、通信網などの重要インフラなど多種多様な領域で利用がされつつある。そのため「全体像が理解しにくい」という声がある一方、IoT を実現するための様々な規格や標準が提供されつつある。ここでは、これらを俯瞰することで、広大で入り組んだIoT の世界を概観してみる。

インフラ/産業から個人へ

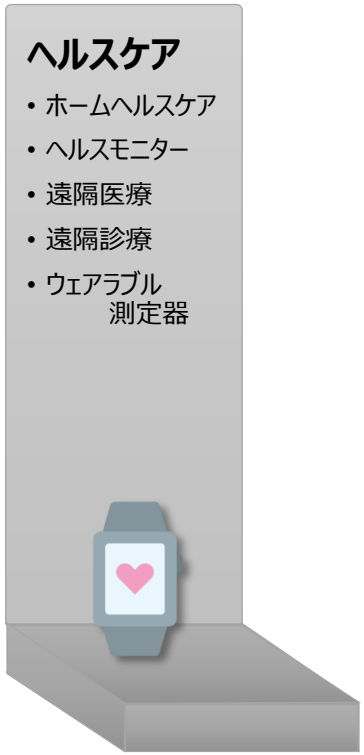
*Internetにつながる機器はより身近に



個人用マイコンボード（RaspberryPi など）、ネットワーク玩具 など

消費者向けと企業向け

- 代表的な区分として、これら六つの分野を挙げるが、各分野ごとに提供されるサービスや商品によって「消費者向け」のものと「企業向け（あるいは事業者、自治体などの組織）」の二つがある
- ヘルスケアであればウェアラブル端末（個人が身につけて利用するもの）は「消費者向け」であるが、自治体や特定の医療機関が住民や患者に対して提供し、健康状態を遠隔で把握するためのウェアラブル端末（たとえば携帯型の心電記録装置）は個人が使用するものの、その所有者や目的からは「病院・自治体向け」というのが適切である
- 心電記録装置であれば病院によって提供される遠隔診断というサービス、健康促進やライフログの記録が目的であれば活動量の記録サービスを利用するためにウェアラブル機器を利用することになる



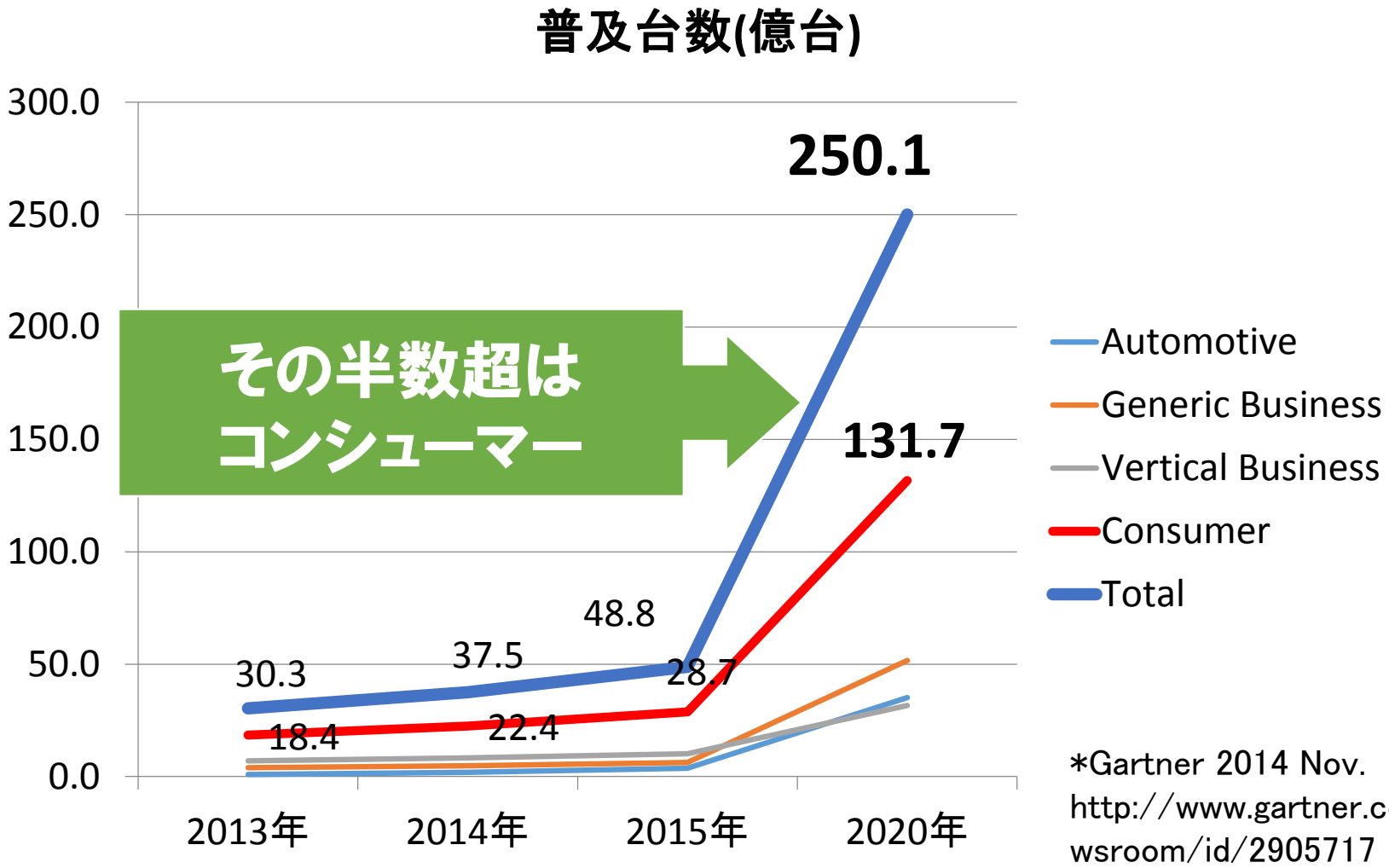
1-1.市場動向と未来予測

2020年の IoTの市場は、現在に比べそのデバイス数が現在の6倍、数百兆円市場になるとされる。そのデバイスの活用データ量が増加すれば、データの提供価値（付加価値）も上がると考えられる。この先、2025年以降にあるものは人工知能制御、現在はこの育成期間であるとの見方もある。人工知能の発達が与える雇用への影響、社会構造変化についても人工知能の専門家から二つの極端な意見（新たな雇用、雇用阻害）がなされている。

IoT およびその先の人工知能の発達は、IoTセキュリティにどう影響を与えるのか？多くのデバイスがネットに接続され、社会構造の変化（リソース共有が促進、所有のスタイルも変化）とセキュリティの変革（認可、多要素認証など）の同時進行、音声認識・画像認識への人工知能活用によってより個人に密接・リアルタイムな情報を扱う事でプライバシー情報への配慮はより重要となる。さらに、サイバー攻撃は一般人にとってもより身近になるだろう。

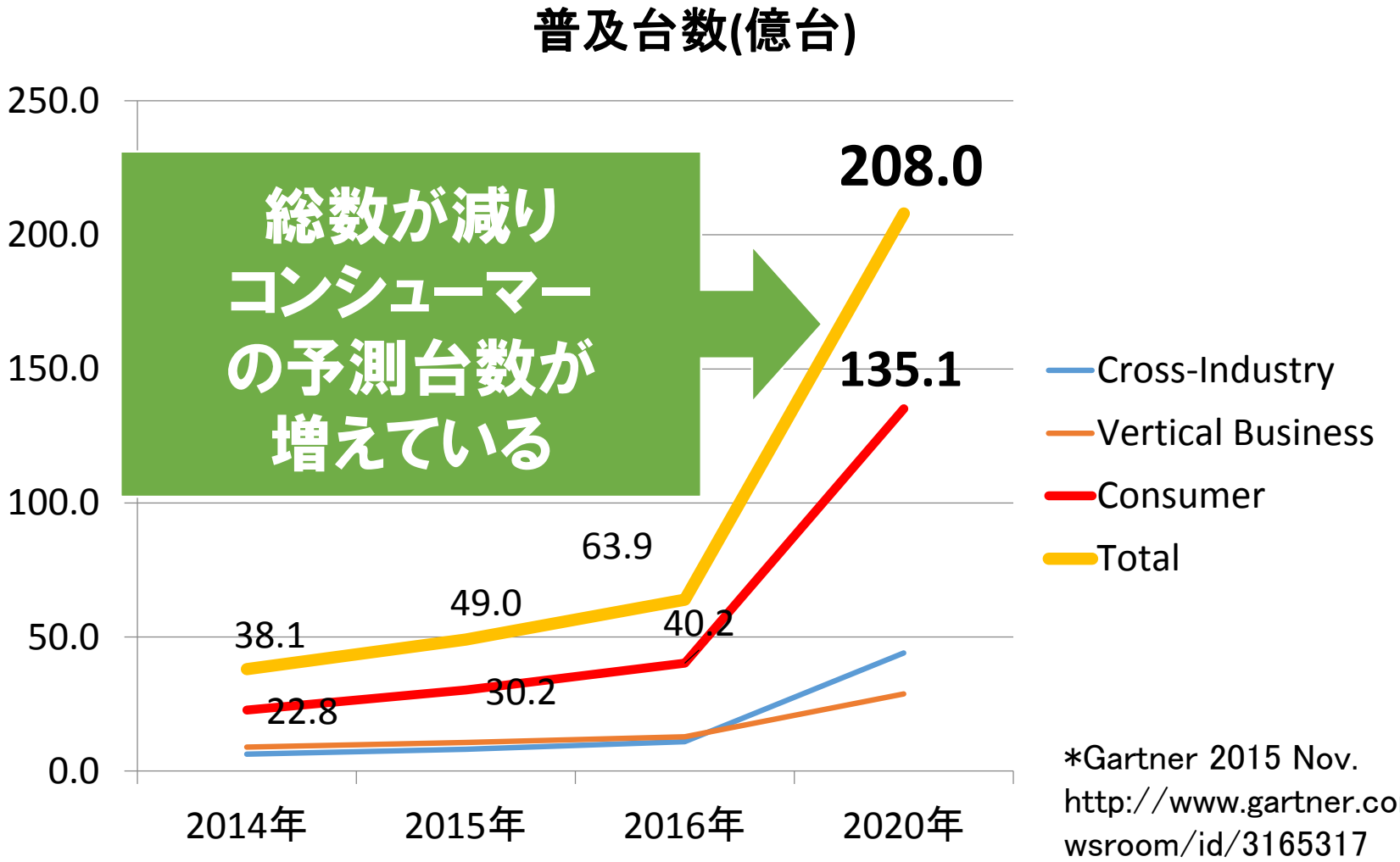
2020年までに 250億台の IoT

*2014年度予測



*Gartner 2014 Nov.
http://www.gartner.com/newsroom/id/2905717

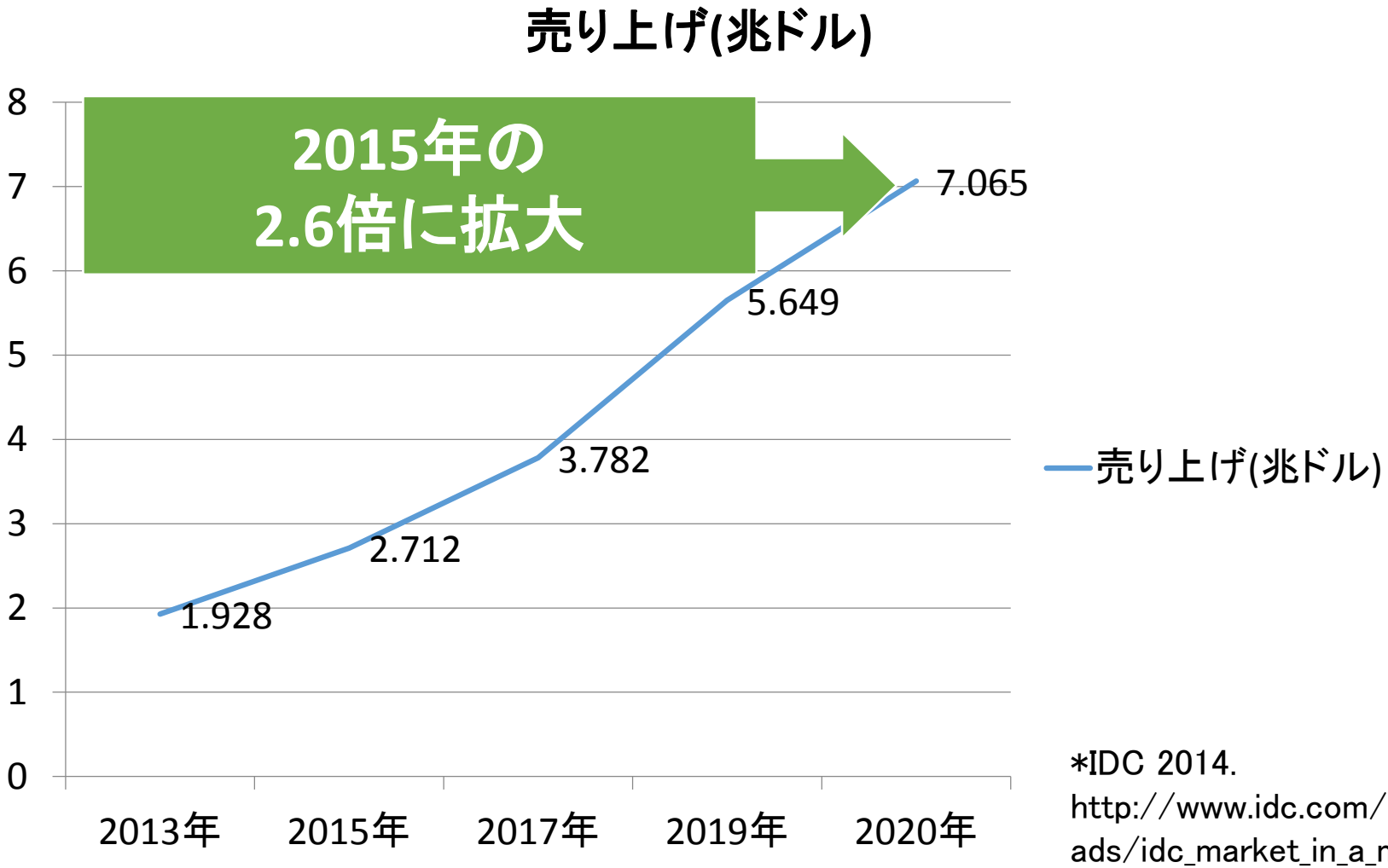
2020年までに 207億台の IoT
＊2015年度予測



＊Gartner 2015 Nov.
http://www.gartner.com/newsroom/id/3165317

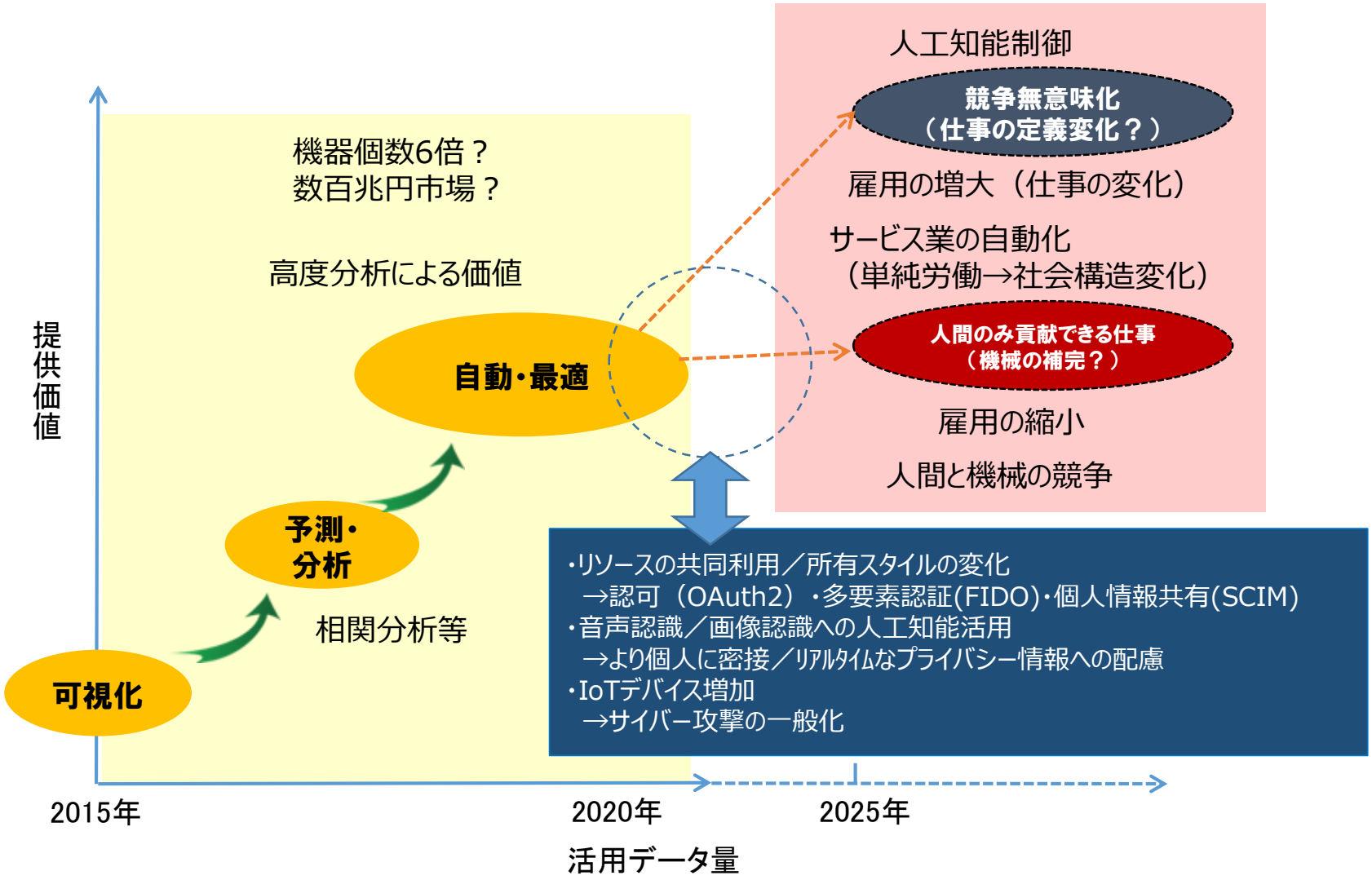
2020年までに 7兆ドル市場に

*2014年度予測



*IDC 2014.
http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf

IoT の市場・未来予測



市場予測

- Gartner社、IDC社などの調査会社による IoT 市場予測によれば、産業用途やインフラでの利用の予測は徐々に減少しているが、コンシューマー機器の拡大が想定されている
- コンシューマー機器が増えることは、管理されない機器の増加を意味し、サイバーセキュリティ対策の観点から、市場の拡大を見越した対応が求められる

1-2.IoTの技術

IoT 技術は「可視化」、「収集・予測・分析」、「自動制御・最適化」の組合せから成り立つ。

「可視化」は主にUI/UXで行う。
「収集・予測・分析」はセンサー情報の最適な収集とクラウド・人工知能等による高度分析。
「自動制御・最適化」はリアルタイム制御またはアプリに応じた最適な制御、セーフティなアクションなど
単に「モノが Internet繋がった」ということではなく、高度で知的な制御を含むもので、ユースケースによって異なる。

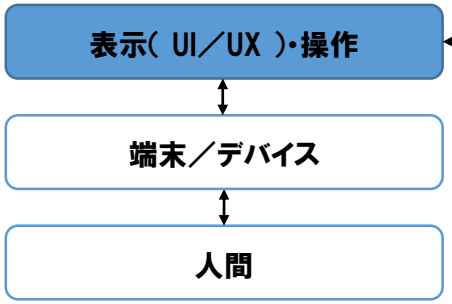
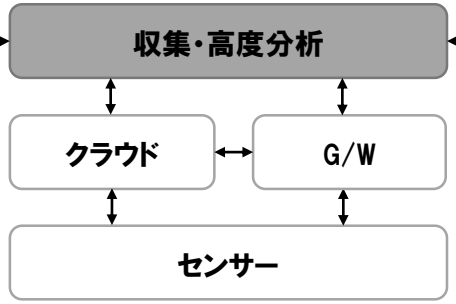
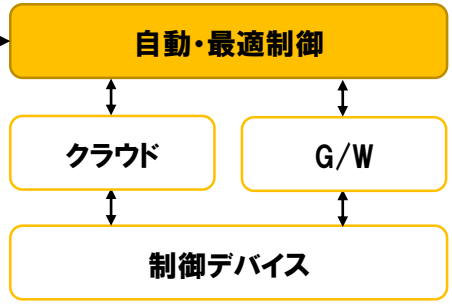
IoTの研究と標準

*IoTの調査研究と標準化

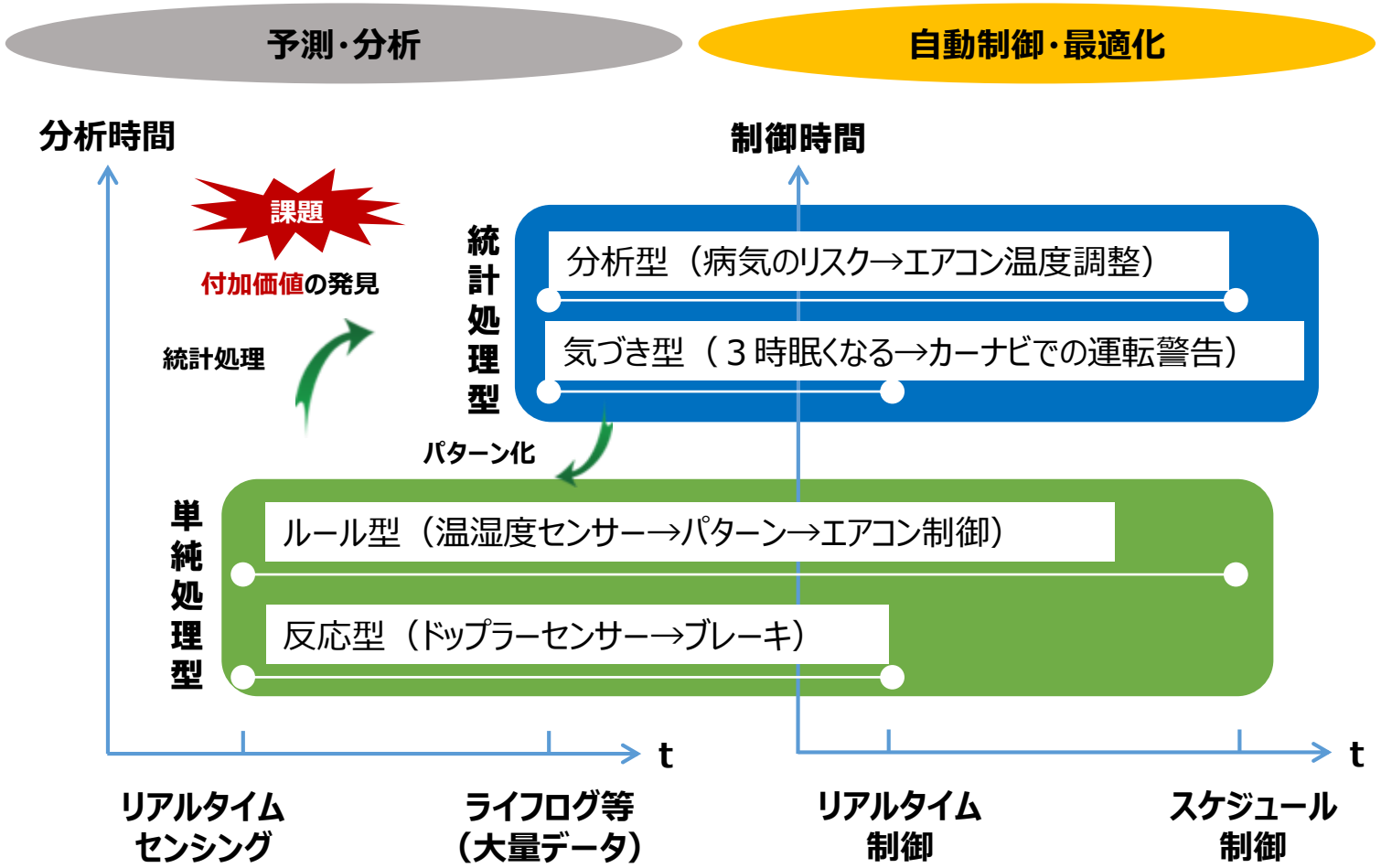
- IoTを安全かつ効果的に実現するための実証試験や調査研究の代表的なものとしてIoT-Aがあり、IEEE、ITU、ISO/IEC、OMG、など様々な標準化組織により標準化の検討が進められている
- 枠組みやアーキテクチャといったレベルでの検討を経て、現在ではAllseenやoneM2Mのなど複数の企業グループや組織から、実装・実現に必要なコミュニケーション、管理やセキュリティの提案がなされている
- 日本国内でも、当WGの他にIoT推進コンソーシアム、IoT推進研究会などが複数存在し、業種毎にグローバルな標準化の流れを見据えた標準化の検討がなされている

IoT-A , Internet of Things - Architecture : http://www.iot-a.eu/public
IEEE-SA , IoT Steering Committee : http://standards.ieee.org/innovate/iot/
IEEE P2413, Draft Standard for an Architectural Framework for the Internet of Things Working Group : http://standards.ieee.org/develop/project/2413.html
ITU Joint Coordination Activity on IoT (JCA-IoT) : http://www.itu.int/en/ITU-T/jca/iot/Pages/default.aspx
ISO/IEC: JTC1 SWG 5 Internet of Things(IoT) :http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:10270,25?q=jtc1%20sc%2038
OMG : http://www.omg.org/hot-topics/iot-standards.htm
Industrial Internet Consortium : http://www.industrialinternetconsortium.org/
oneM2M : http://www.onem2m.org/
TTC: 一般社団法人情報通信技術委員会 oneM2M : http://www.ttc.or.jp/j/std/committee/wg/onem2m/onem2mtopics/20141212/
Allseen Alliance : https://allseenalliance.org
Open Connectivity Foundation : http://openconnectivity.org

IoTの機能区分、要求項目等

機能区分	可視化 情報の見せる化・透明化 （何がどう動くかの把握部）	収集・予測・分析 情報の集約・分析 （システム制御の頭脳部）	自動制御・最適化 分析に基づく制御 （システム制御の実行部）
フロー			
要求項目	・カスタマイズ性 （ドローン：操作に応じた見せ方） ・制御／状態の認知 ・見やすさ ・操作のしやすさ	・効果的なデータ分析 ・性能／用途別の要件 （送信量／センシング間隔／回復／ライフサイクル対応）	・リアルタイム性 ・アプリに応じた最適な制御 ・セーフティなアクション
実装	・組込OS（Android、iOS、等々） ・アプリに合ったディスプレイ ・アプリに合った入力装置	・用件に合ったIoTプラットフォーム ・組込OS（RTOS～Linux等々）	・IoTプラットフォーム ・組込OS(RTOS～Linux等々）
例	・FPV（ドローン映像とコントロール） ・ウォッチデバイス（状態通知） ・スマートフォン（見やすさ、操作感） ・サイネージ（訴求力） ・音声入力（音声認識） ・ボタン／キーボード（簡単操作）	・センサー（温湿度、ドップラー反射、脳波、血圧） ・GPS（位置情報） ・ビーコン（存在確認、場所情報） ・カメラ（全方位、赤外線、距離画像等）	・エアコン（温度制御、風量、風向） ・照明（On/Off、明るさ） ・車（ナビ通知、衝突回避ブレーキ） ・シャッター（開閉） ・ドローン（モーター駆動）

IoTの区分と技術



「大量データの分析→相関分析→アクション」が新たな付加価値を生む可能性

IoTの処理連携（抽象化）

IoTの構成α：｛センサー、制御デバイス、端末｝、構成αに対してβ：｛アクション｝が決定、制御がされるとする

α：｛構成｝を選択・決定し、β：｛アクション｝を選択・決定すると考える

α:｛センサー群×制御デバイス群×端末デバイス群｝の各組の決定

β:｛アクション｝の決定

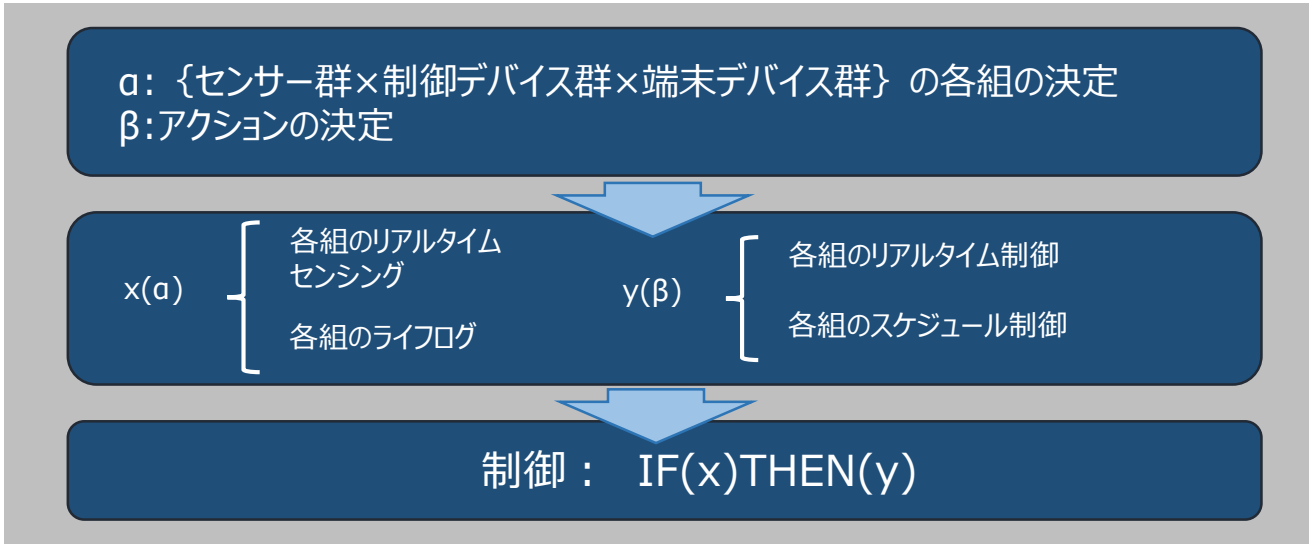
（例）

【課題】ある運送会社で「ドライバーの眠気」が課題

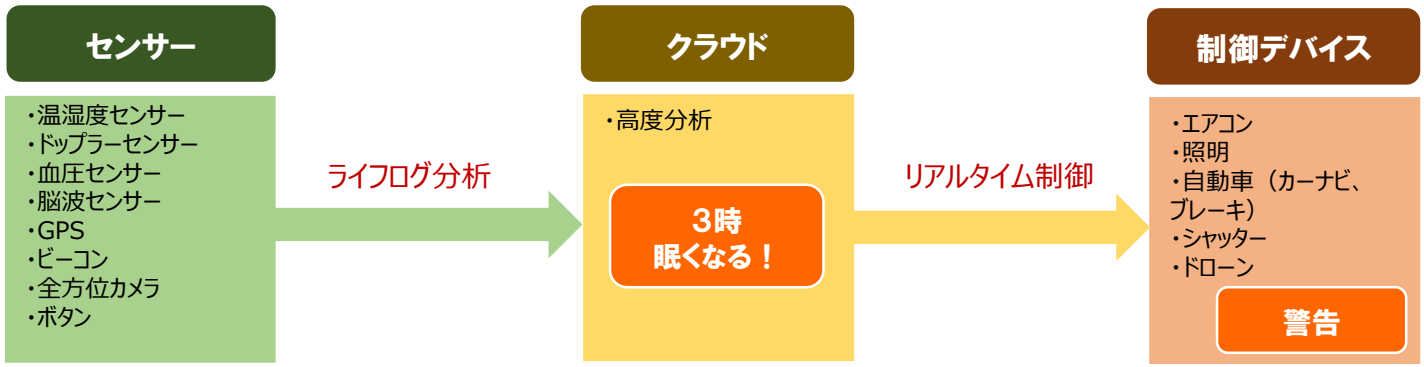
【解決策】「温湿度計」、「カメラ」、「血圧計」などのセンサー群と「警告音発生機」を組み合わせて音による「警告」を行なう組合せを｛α、β｝に対して規定する

リアルタイムでデータを分析し「眠気」に関係するデータのパターンを得る。「眠気」の発生を検知と同時に｛アクション｝（「警告」）が実行される

IoTの処理連携の抽象化



例）



IoTでの付加価値創造（抽象化）

【シーズから作り出す方法】

豊富なセンサーデバイスの組合せから課題の最適解を見つけ出す。所謂「研究室」的なものから、付加価値が創造される

データ収集段階	「様々な可能性（センサーの組合せ）」を考え、課題解決を導くデータ収集を行う段階
モデル想定段階	「データ分析」で得られた「相関」をもとに、ビジネスモデルの構築、ビジネス範囲の絞込みをする段階
ビジネス段階	付加価値と判断されたビジネスモデルからアクションの対価を得るためにシステムを運用する段階

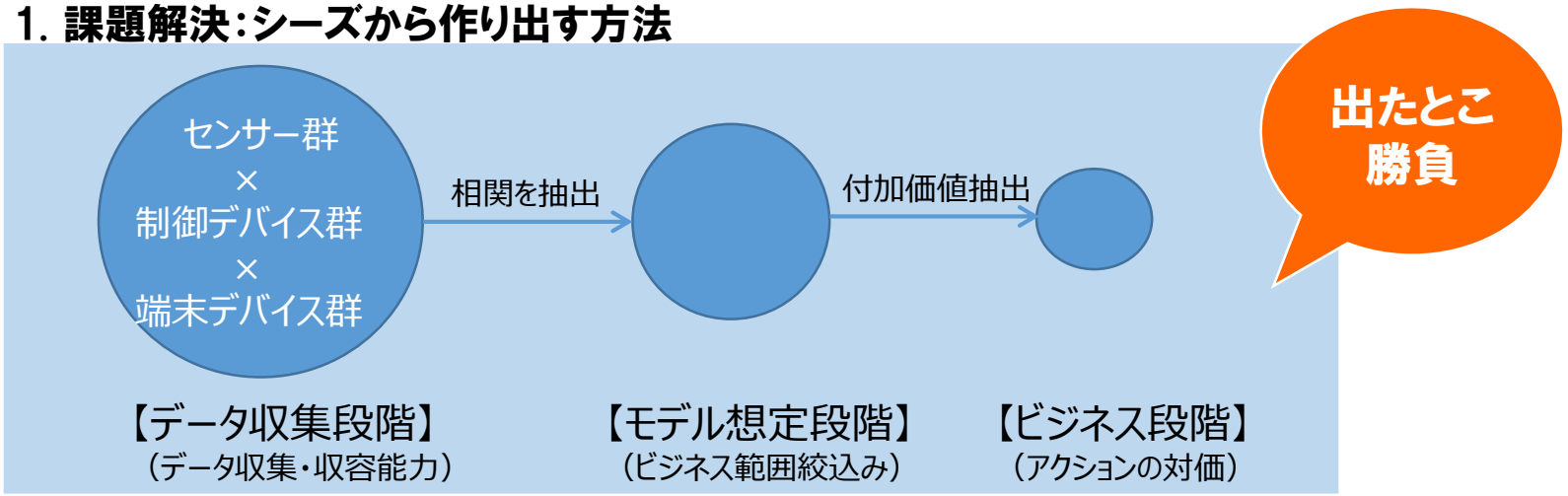
【ニーズから作り出す方法】

従来のビジネスニーズから、ビジネス主体同士が集まって課題の最適解を見つけ出す

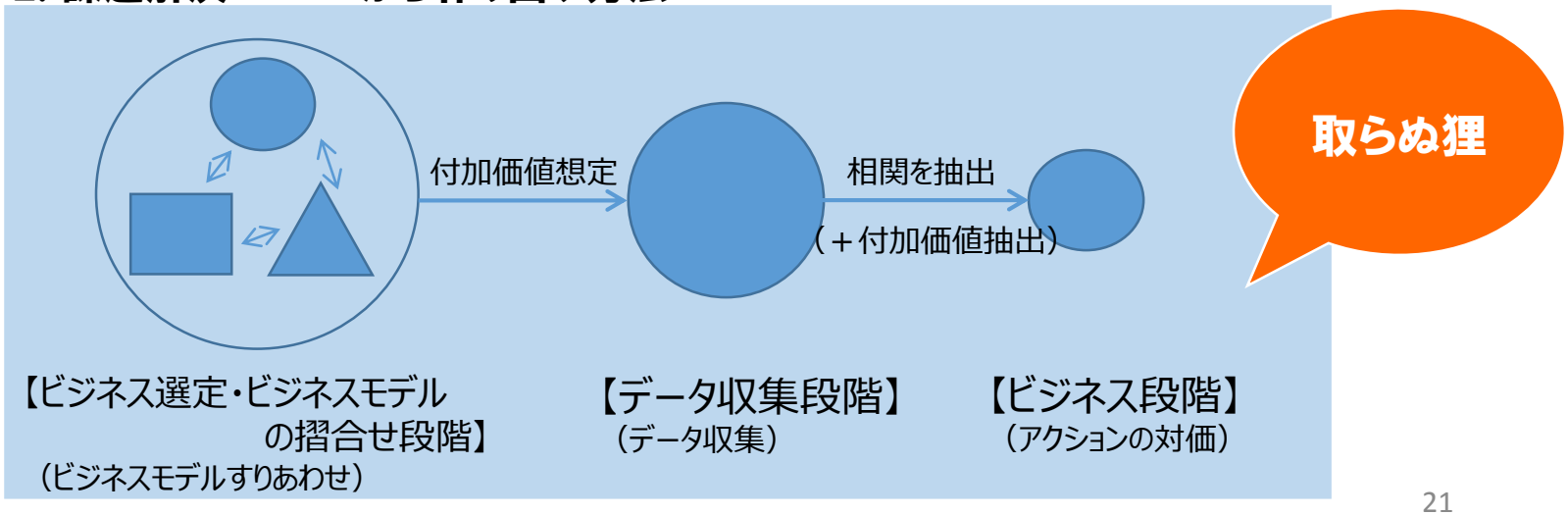
ビジネス選定・ビジネスモデルの摺合せ段階	ビジネスプレイヤー同士がコンタクトし、ビジネスモデルの摺り合わせ、および「付加価値」の想定をする段階
データ収集段階	想定ビジネスでの課題解決のための「データを収集」する段階
ビジネス段階	課題解決に繋がるデータの相関を利用してアクションの対価を得るためにシステムを運用する段階

IoTでの付加価値創造（抽象化）

1. 課題解決：シーズから作り出す方法



2. 課題解決：ニーズから作り出す方法



IoT制御の分類

・IoT制御を｛異常検知型、物体認識型、スケジュール型｝に分類。

例）ユースケース：｛店舗／工場／（プラント）系、ドローン／監視カメラ／人の認識、カレンダー＋家電制御｝など

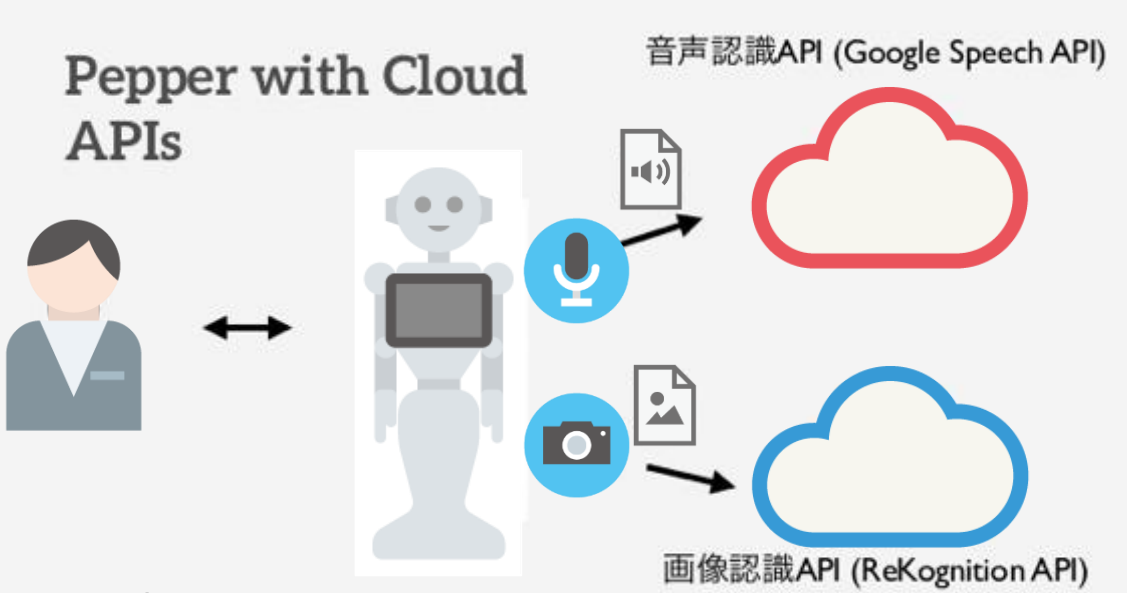
異常検知型	異常の設定に専門性が必要であり、データアナリティクスなどが必要である。
物体認識型	人の代わりに認識、または認識を補助するために判断および制御が行われることを想定。応用範囲は広いが誤検知での想定外の動作への配慮が必要。
パターン制御型	従来のシンプルな方法で、人間が制御を把握しやすい（何時に何が起こるなど）という利点がある。

ユースケースの選択と型の組合せが IoT制御の元になると考える

IoT制御の分類

分類	事例	課題	付加価値
異常検知型 ・異常検知（センシング） →分析→アクション データ アナリティクス （専門性が必要）	店舗／工場／プラント系 • 商品売上の異常を検知→分析→アクション（地図情報などで各店舗で見える化） • 工場ネットワーク内の不正プログラムを検知→分析（SIEM）→（自動アクションまではない） • プラント制御では異常検知後→即アクション（バルブを閉める）	・半自動（アクションまでの自動は不明確）、分析は専門家に依存 ・異常に対する明確なアクションがルール化されていない。（ルール化できるかが課題）	高度な気づきを提供できる（IT系システムインテグレーターが提供するIoT）
物体認識型 ・物体認識（センシング） →分析→アクション 人の代替で {判断、制御}	ドローン／監視カメラ／人の認識 • ドローンから物体を認識して飛行 • 物体認識→分析→アクション • 監視カメラの映像から車種を区別し、カウントする • 物体認識→分析→アクション • 人の顔や人体を認識、人の顔から人物を認識して名前を表示 • 物体認識→分析→アクション	・全自動（認識したものから、どうアクションするかがポイント）	応用ビジネスに広がりあり（ベンダーが提供するＩｏＴ）
パターン制御型 ・カレンダー・タイマ →アクション パターン制御 （シンプルな方法）	カレンダー＋家電制御など特定の組み合わせによって制御が可能なもの • カレンダーにアクションを記述、カレンダーの日時にアクションのメッセージが送信 • カレンダー・タイマ→アクション	闇雲な「音声認識」や「音声合成」または「センサー検知」よりも、シンプル。 ユーザーの「動作把握がしやすい」（シンプルだが、良く使われる方法）	既存サービス（ベンダーが提供するＩｏＴ）

音声認識、画像認識の例



出典：http://www.slideshare.net/shiraco/techcirclepepper

【API利用】
GoogleAPIの試用版では利用制限/日あり
GOOGLE_API_KEY=*api_key*
GOOGLE_CLIENT_ID=*client_id*
GOOGLE_CLIENT_SECRET=*client_secret*

・API呼出しは、特殊なID、秘密情報付でアクセスする

【個人情報利用の注意】
例）
顔認識（年齢/性別/表情/人種/….）
場所認識（海/山/レストラン…）
場面認識（・・・）
会話（・・・）

・データ取得時に{身体的特徴、行動情報、機微情報（思想）}を捕捉する可能性あり

例）APIの呼び出し（画像認識）

http://rekognition.com/func/api/?api_key=kkk&api_secret=sss&jobs="task"&urls="画像のURL"

```
client = Rekognize::Client::Base.new(api_key, api_secret)
client.face_detect(urls: "画像のURL", jobs)
```

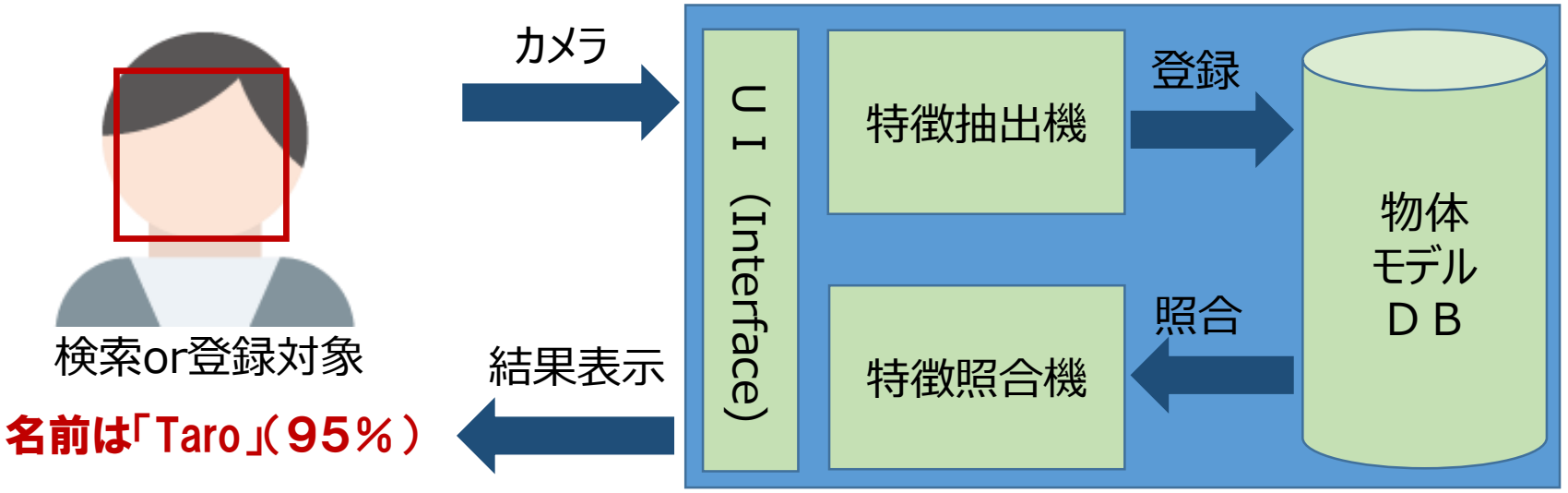
・画像を保存できる→個人情報の問題
・Facebookなどから友人の画像を参照できる

音声認識システムの例

出典：http://www.amazon.com/Amazon-SK705DI-Echo/dp/B00X4WHP5E

物体認識システム

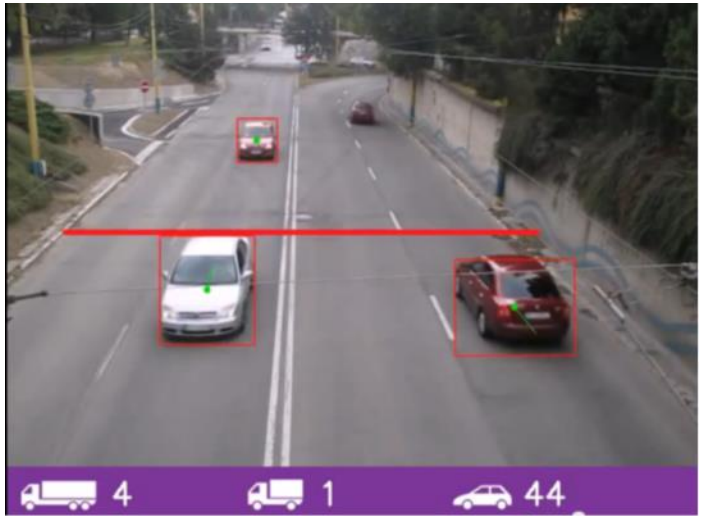
事前準備	認識させたい物体を「撮影」、局所特徴量を抽出し、「物体モデルデータベース」に登録
物体検索	・クエリとして認識させたい画像を写して局所特徴量を抽出 ・「物体モデルデータベース」中の各物体の「局所特徴量」との間で「類似度」を計算 ・その中から「類似度高いもの」を認識結果として返す



参考：http://www.m.cs.osakafu-u.ac.jp/IPSJ_3days/

物体認識

①車の識別とカウント（画像から識別）

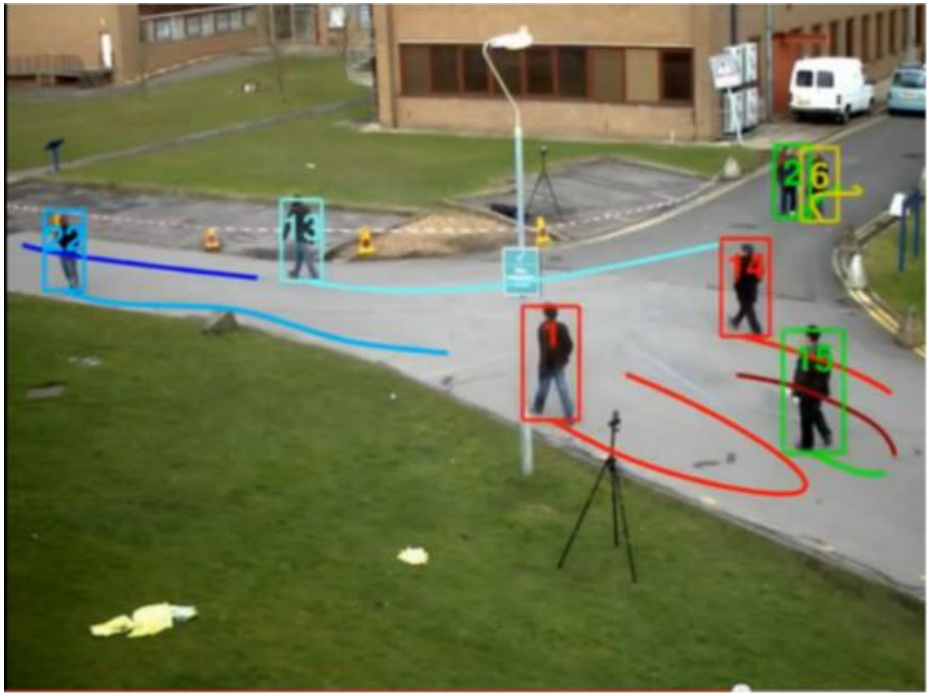


出典：https://www.youtube.com/watch?v=z1Cvn3_4yGo

②ドローンの位置認識（画像から識別）

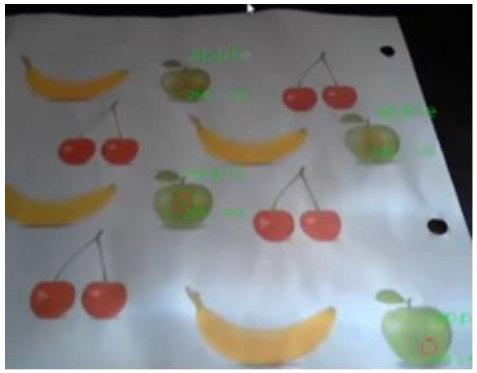
出典：https://www.youtube.com/watch?v=C95bngCOv9Q

③人の認識（画像から識別）

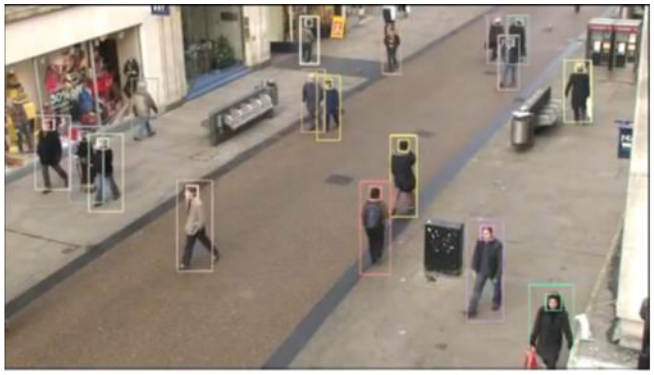


出典：https://www.youtube.com/watch?v=Z9X3IhHytrQ

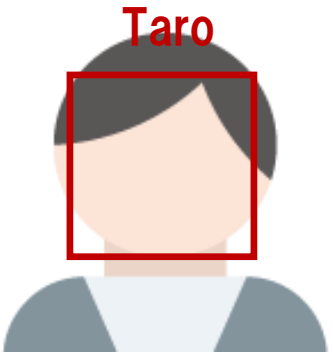
物体認識（その他認識）
＊画像から識別



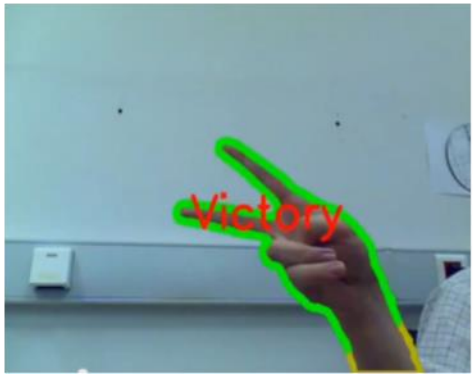
「りんご」の認識
https://www.youtube.com/watch?v=4KYlHgQQAts



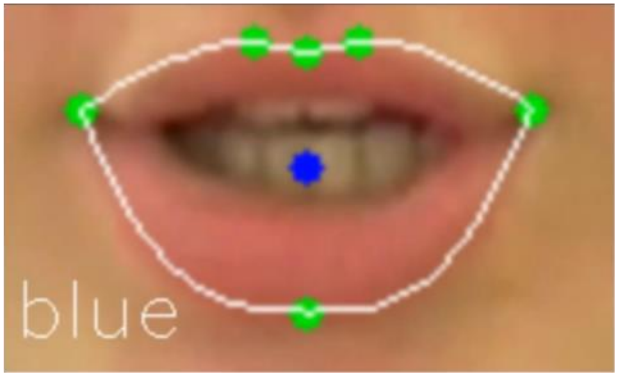
複数の「顔と人体」の認識
https://www.youtube.com/watch?v=InqV34BcheM



「人物識別」

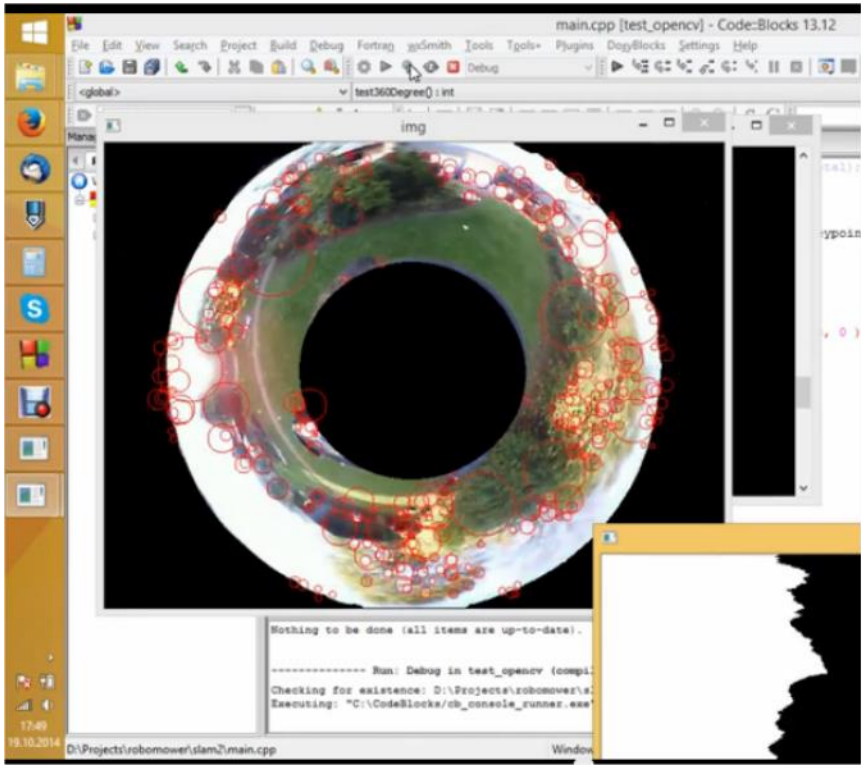


「形状」の認識
https://www.youtube.com/watch?v=_N41CP0f0Mg

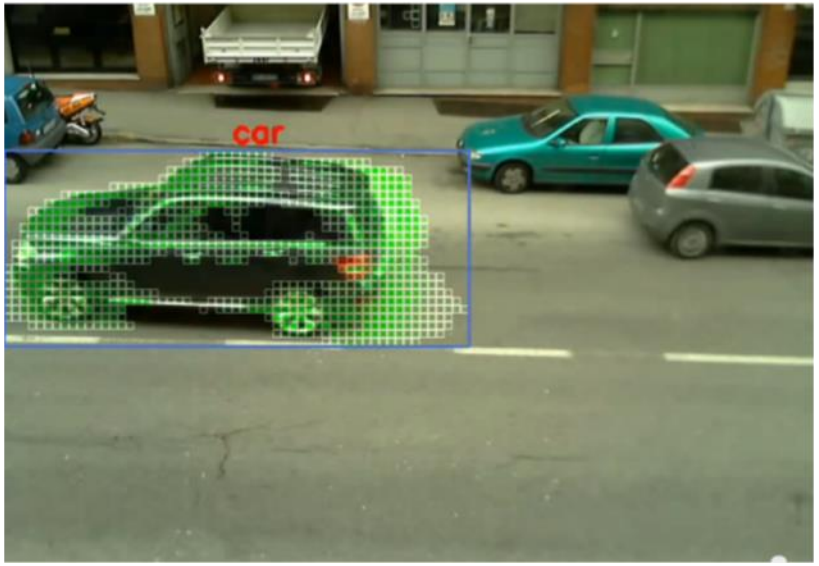


「唇」を読む
https://www.youtube.com/watch?v=jWvvz0Xh0uU

物体認識（その他認識）
＊画像から識別



「全方位カメラ360度」での認識
https://www.youtube.com/watch?v=db19BFfRYCA

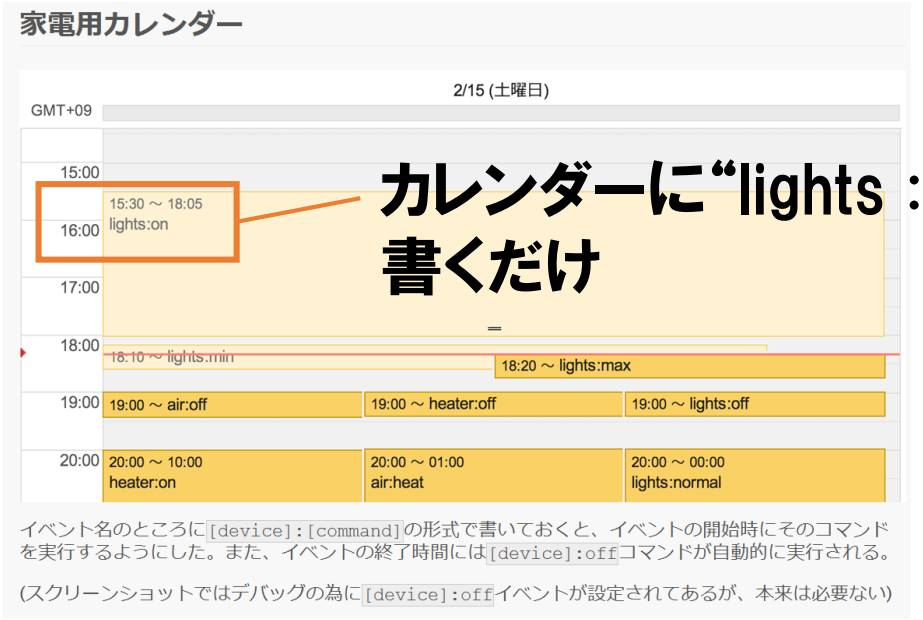


「車の分類」での認識
https://www.youtube.com/watch?v=1wxg4nUQ_DA

Google Calendarで家電を制御する

Before：従来、音声認識で家電を制御(hipchat、command line)していた。

After: 結局、おおよその生活パターンで「前もってスケジューリング」しておくのが多少効率は悪いが「一番楽」という結論に至った。特に朝に暖房を入れたり照明をつけるのは、気持よく起きることが出来てよい。以前の実装では家電の動作スケジュールを変えるには「コードで反映」するしか無かったので、今回は「柔軟にスケジュールを記述できる」ようにGoogle calendarを使った。「繰り返し設定や平日のみの指定ができ、状況が可視化される」ので便利だった（Raspberry Pi）。



出典：http://blog.fukayatsu.com/2014/02/15/home-automation-with-google-calendar/

異常検知型の例

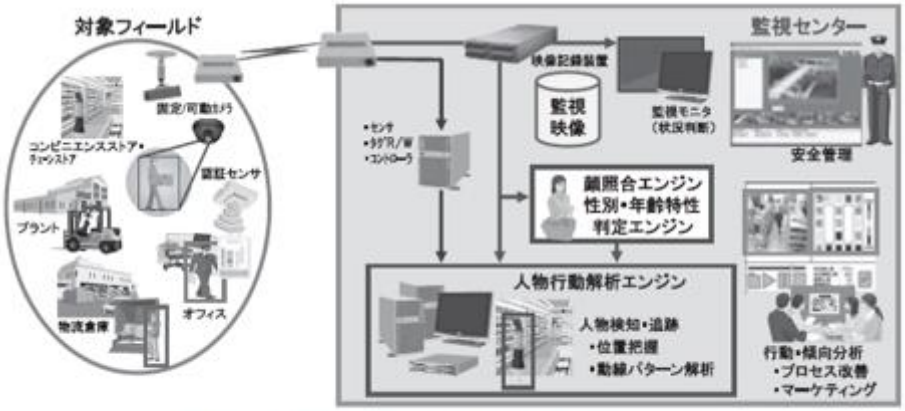


図1　動線解析システムのイメージ図

出典：人の行動を「見える化」する動線解析技術と活用例　原田 典明・青木 勝・三上 明子、峯下 聡志・斎藤 志傑動線解析　（NEC）
http://jpn.nec.com/techrep/journal/g11/n03/pdf/110303.pdf

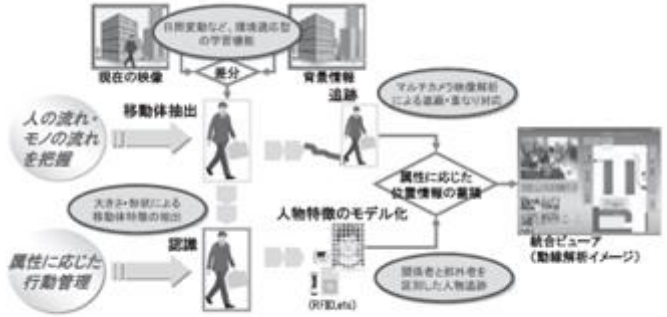


図2　人物の抽出・追跡技術の概要

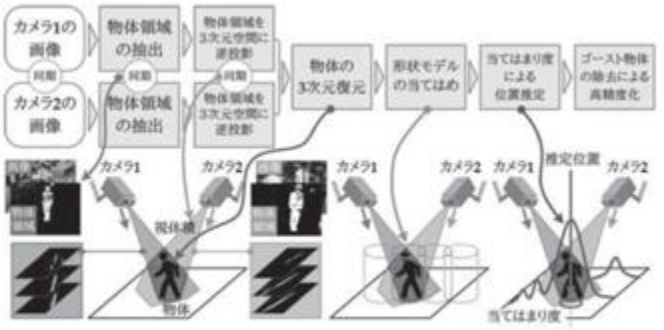


図3　人物の位置推定技術の概要

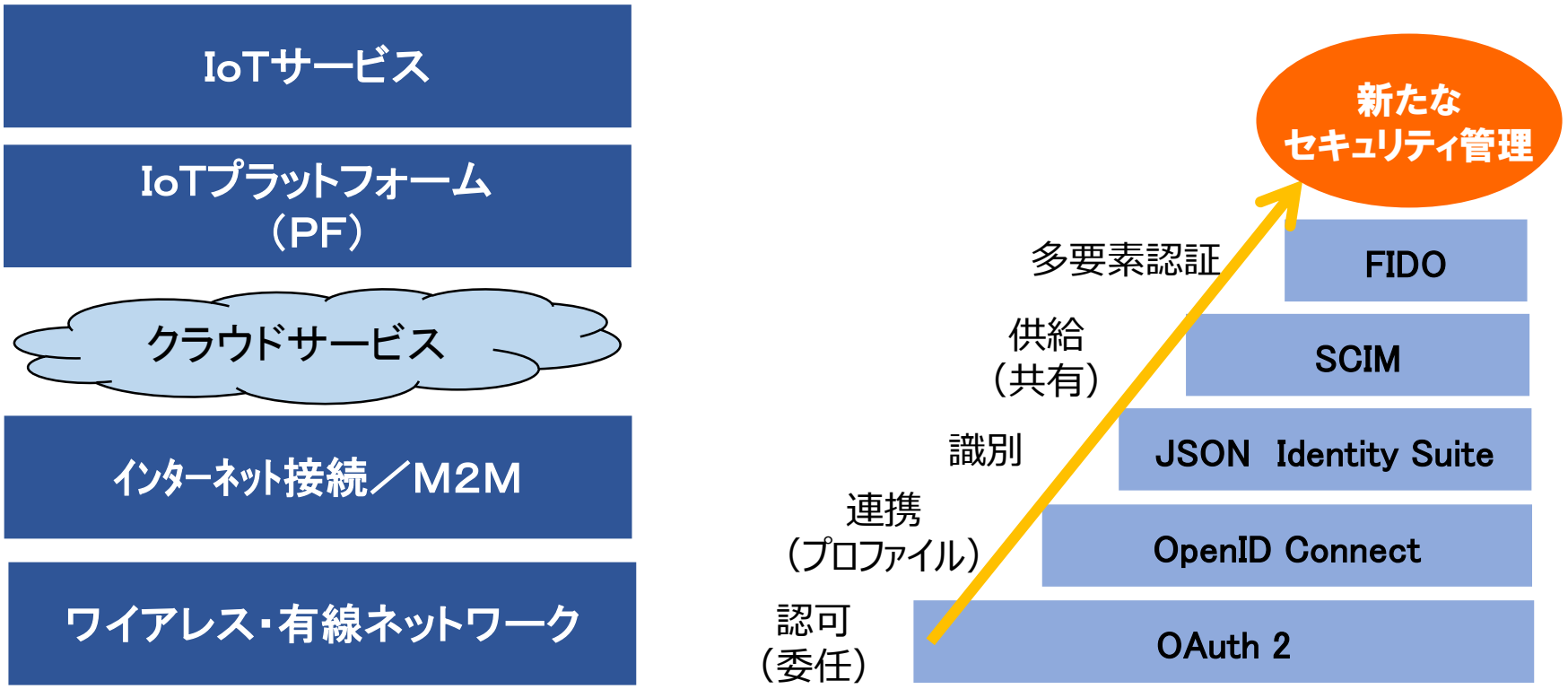
人の動線を学習・解析してマーケティングやプロセス改善に活かす
「大規模店舗等で顧客があるコーナーの商品棚を通らなくなった」
などの事象を分析する

IoT サービス・PFとセキュリティ

【現在の IoTサービスとプラットフォーム】

・ IoT のプラットフォームおよびクラウドなど「ツール（ IoTのSDKを含む）」となる部分の技術開発、運用・ビジネス化が先行
・サービス主体であるサービサーは IoTのプラットフォームおよびクラウドのツールを使うことで IoT を実現するモデル
・ IoT のプラットフォーム（PF）およびクラウドベンダーは、人工知能や音声・画像認識、ストレージなどのAPIを提供、 IoTのサービサーはそれを組み合わせることでサービスを実現する
・ベンダーは、ユーザーの個人情報・プライバシー情報を人工知能を使って最適なアシストの機能を強化、得られた情報（リソース）を他と共有し、全体の機能を押し上げる
・ IoT のセキュリティでは SSL/TLSといった VPN・暗号系のセキュリティに加え、リソース共有にあたってユーザーから認可（OAuth2）を受ける ・今後、多要素認証(FIDO)・個人情報共有(SCIM) が要求されつつある

IoT サービス・PFとセキュリティ



IoTは構造化される→IoTセキュリティも仕組み化される

1-3.IoT制御技術の例

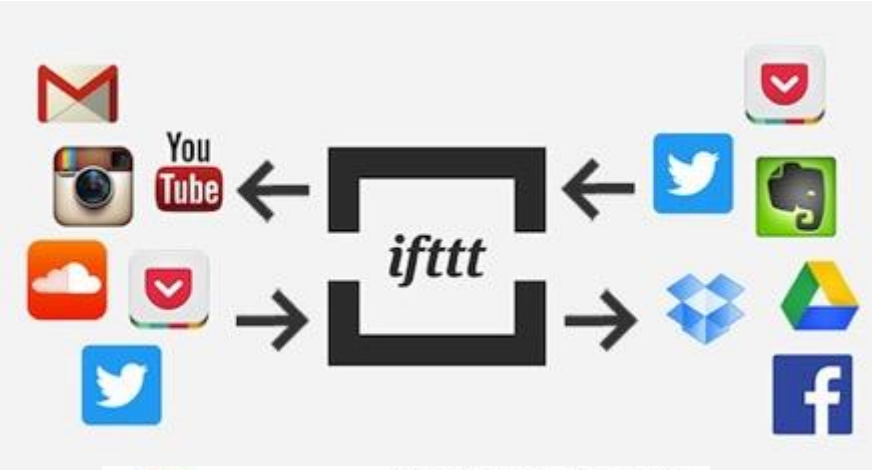
ここでは現在利用可能な IoT制御技術の例を示す。

IFTTT, Node.js, OpenJTalk, Julius, Blynk, iBeacon,
OpenHome Reemo, Mota SmartRing,DigitSole,Seosor Smart Alarm

IoTの制御プラットフォーム

＊IFTTT：家電制御＋音声認識＋音声合成＋α

facebook、twitter、YouTube、Evernote、instagram…等（「出来ること」「出来ないこと」）がバラバラのWebサービスを連結させて相互に情報のやり取りを可能にしたクラウドサービス



制御の基本的な振る舞いをそのまま記号化

例）

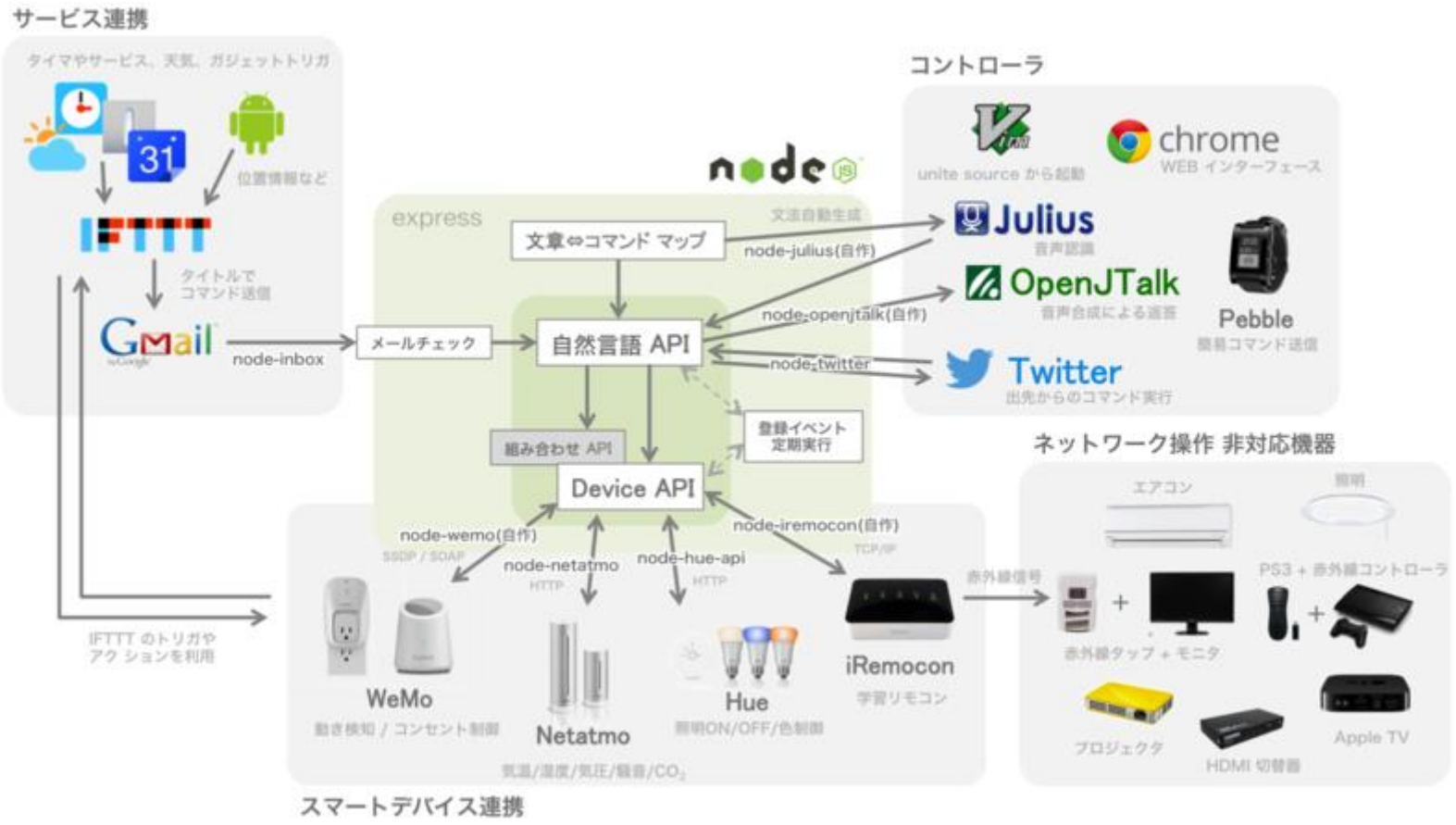
「twitter」サービスと「pocket」サービスを連結させるレシピ

twitter上で誰かのツイートが気になった時に「お気に入り」をクリックするだけで、自動的に自分が使っているpocket内にツイートが保存される

出典：http://hoomey.net/ifttt_study_1/

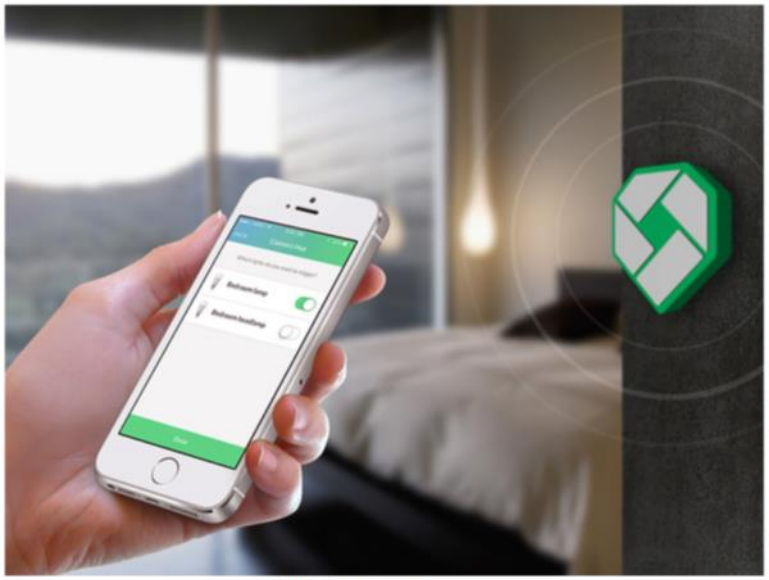
IoTの制御プラットフォーム

*IFTTT：家電制御＋音声認識＋音声合成＋α



出典：http://tips.hecomi.com/entry/2014/05/01/130105

IoTの制御プラットフォーム
＊ IFTTT：iBeacon



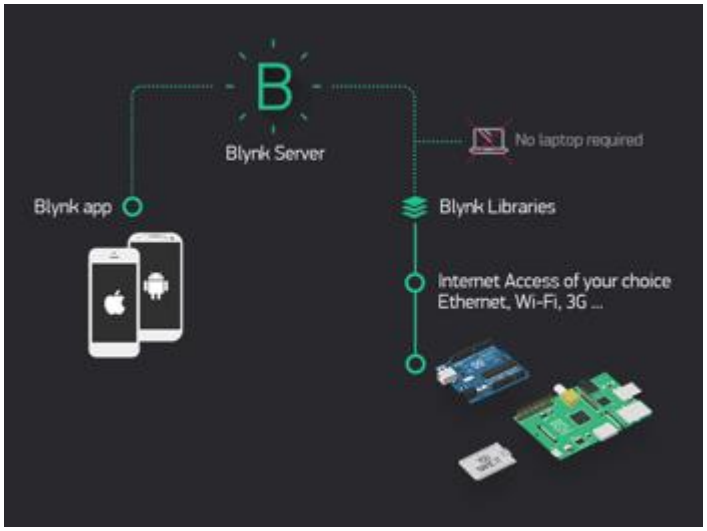
引用元：airfy Beacon

- 洗面所に入ると照明が自動で点き、出ると自動で消える
- 家を出る時にIFTTTで天気予報を通知する
- 寝るためにリビングを出ると、自動で照明やテレビが消える

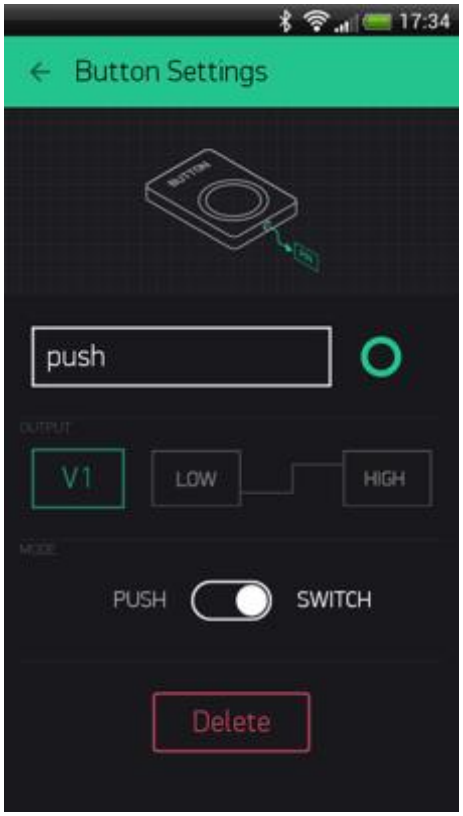
出典：http://o2o.abeja.asia/product/post-4193/

IoTの制御プラットフォーム
＊Blynk+ESP8266、Wake On WAN

•Blynk アプリ
Google Play / AppStore で公開中の専用アプリを使ってユーザが構成した制御用のアプリ
•IoT デバイス
専用の Blynk ライブラリを使ってユーザが作成したプログラムを導入ずみの制御対象の装置
•Blynk サーバ
Blynk アプリと IoT デバイスの連係を仲介するクラウドサービス（※オープンソースであり自前での構築も可能）



出典：http://dsas.blog.klab.org/archives/52229405.html



1.所定の PC を Wake On WANする
2.所定の PC へ ping を打つ
3.所定の AC 機器への給電を ON / OFF する
4.制御対象の IoT デバイスをリセットする

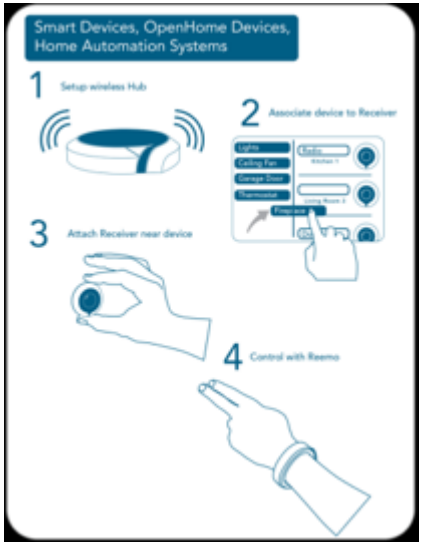
IoTの制御プラットフォームの例
＊OpenHome：Reemo

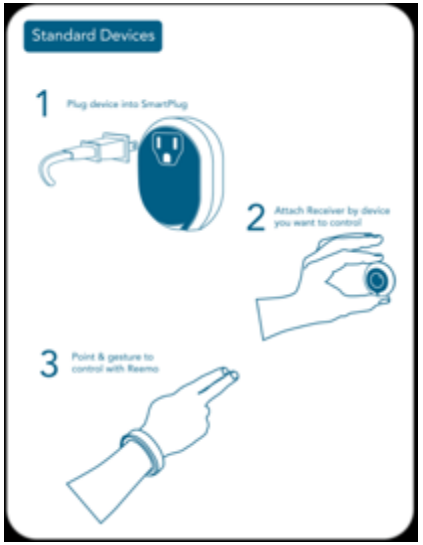
OpenHome 互換

ハンドジェスチャーで
照明をオフ

ハンドジェスチャーで
音楽をオン

その他、スプリンクラー、ガレージ扉の
ジェスチャー操作など





出典：https://www.youtube.com/watch?v=sYzTVuh9vXk

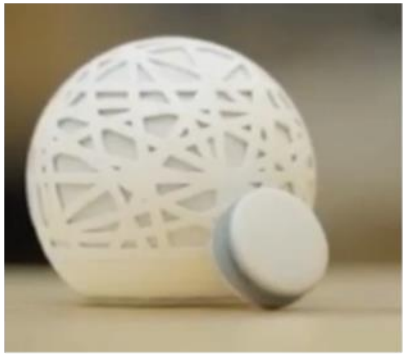
IoTのガジェット

＊Mota SmartRing、DigitSole、Seosor　Smart Alarm

SmartRing（リング状通信機）

DigitSole（無線式圧力センサー）

SensorSmartAlarm
（温湿度センサー利用の快眠グッズ）



出典：https://www.youtube.com/watch?v=sYzTVuh9vXk

2. IoT のセキュリティの現状

IoT はまだ生まれたての仕組みであるため、セキュリティよりも利便性や、利点を重視している。しかし、利用される主な技術についてはすでにセキュリティの検討が行われており、それらについて特徴的な事柄をかいつまんで解説することで、IoT のセキュリティ現状と課題を理解する助けとしたい。

2-1.セキュリティとプライバシー

2015年1月、ラスベガスで開催されたCESでは IoTビジネスの拡大を印象付ける一方で、セキュリティとプライバシーに関する懸念が FTC(Federal Trade Commission)の会長によって言及された。

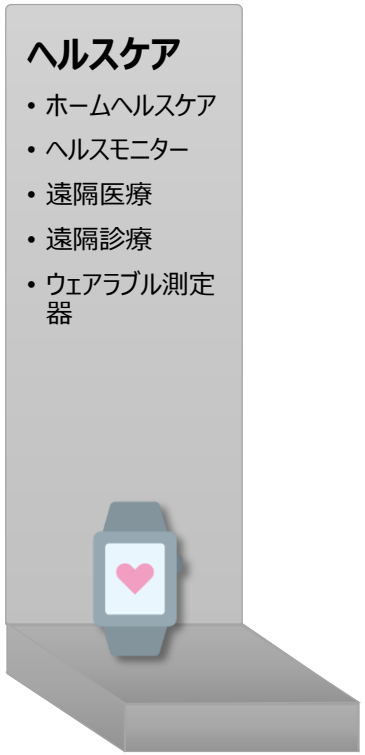
セキュリティとプライバシー

- IoT 機器やサービスでは個人や組織の各種情報を扱う
- たとえば、ヘルスケア機器であれば、個人の生体情報や血圧や血糖値など健康状態に関わる情報を個人、あるいはシステムとしては組織や特定の地域（たとえば自治体がヘルスケア機器を用いた遠隔診療などのサービスを提供する場合）の複数の情報を処理することになる（あるいは可能性がある）
- この情報は「プライバシー」情報であると同時に、これらの情報が漏えいしないか、漏えいしても読むことのできない暗号化された情報として処理できるような「セキュリティ」対策を施すことが望ましい（あるいは法令などによって義務付けられる）が、この二つの事柄は分けて考える必要がある
- 日本国内では「特定個人情報保護法」によって個人情報が保護されており、法制度に基づいた対策はこのガイドの中では扱わないこととするが、IoT-A におけるプライバシーについて参考として紹介するのみにとどめる
- 本ガイドで例示するのは、アプリケーション（機器ごとの）セキュリティ上の課題と想定される代表的な対策であり、扱う情報がプライバシーに属するものである場合の対処については扱わない
- 個人情報の扱いについてはIPAからガイドが提供されているので参照してほしい

参照：https://www.ipa.go.jp/security/kojinjoho/

- また、JNSAからも情報セキュリティポリシーのサンプルを提供している

参照：http://www.jnsa.org/policy/privacy_hyoujyun.pdf



2-2.デバイスとシステムのセキュリティ

デバイスとシステム（クラウドあるいはオンプレミス）のセキュリティのために利用されている技術の中で認証に伴う代表的なものを示す。

＊IFTTT Maker機能

(1) Trigger

IFFF上のアカウントに対応したProject（App）の識別子　APIの秘密鍵

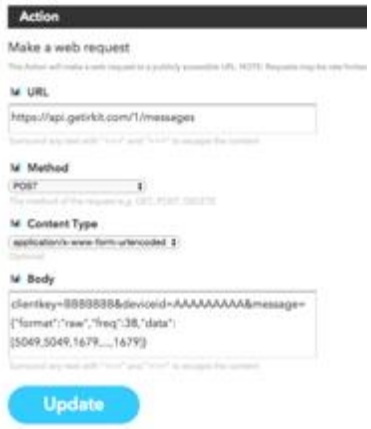
https://maker.ifttt.com/trigger/{**event**}/with/key/{**secret key**}

(2) Actions

JSON形式で3つまで変数を送ることができる。
{ "value1" : "", "value2" : "", "value3" : "" }

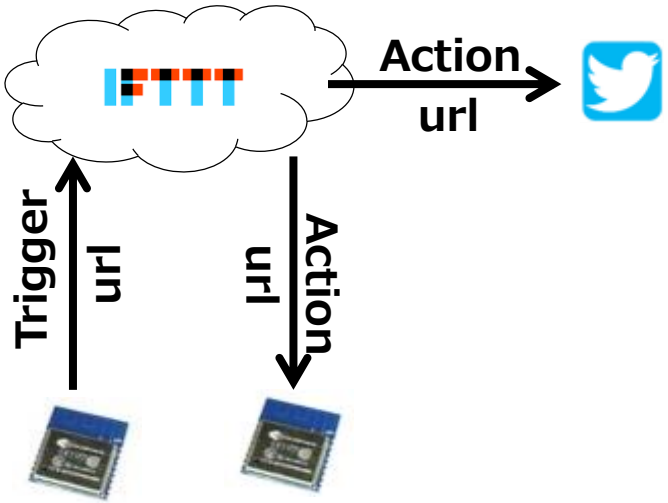
「＋α」は相手次第

http://URL



iRKitのようにクラウドサービスを持つ場合、対向にセキュリティの機能があれば認証付で
を送信できる

client_key =
device_id =



出典：http://senyoltw.hatenablog.jp/entry/2015/06/20/114005

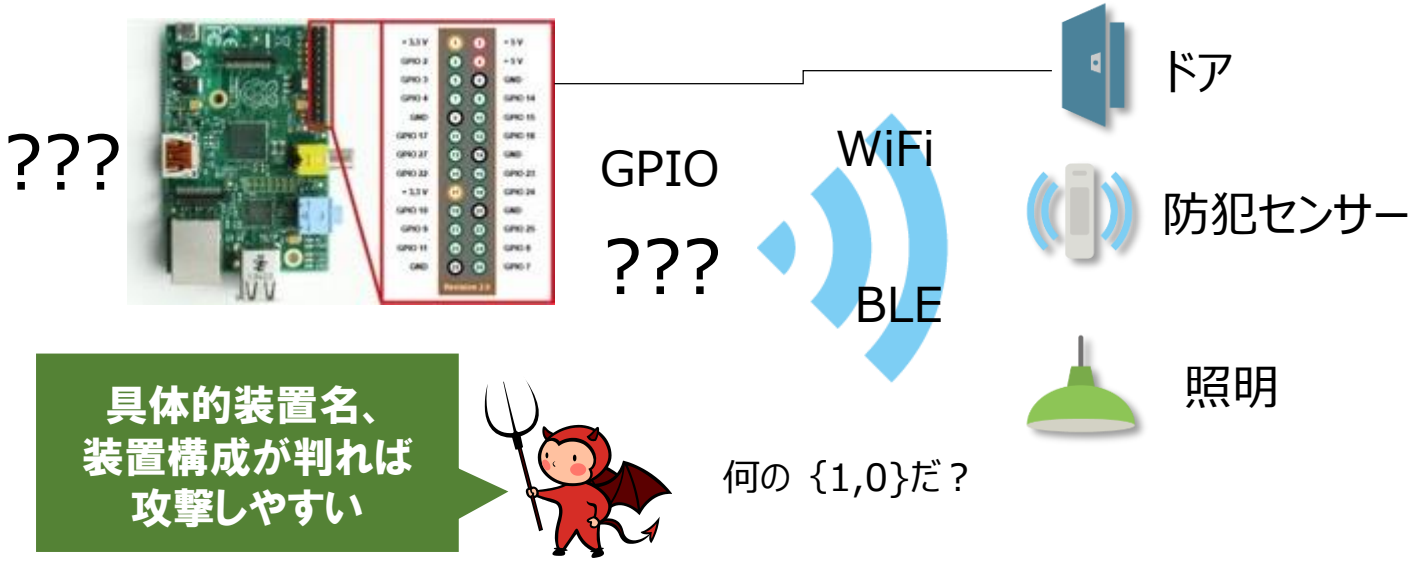
*API-Keyはセキュアか？

・デバイスの｛secret key｝がばれても｛login/password｝は漏れない（IFTTTはログイン・クレデンシャルを持たない）

（実は、Secret key 発行の手順を含めればOAuthの手順は踏んでいる・・・）

・デバイスが何か判らなければ “セキュア”と言えるのか？

GPIOの“先”、BLE、WiFiの先の具体的モノが“わからない”と言う事



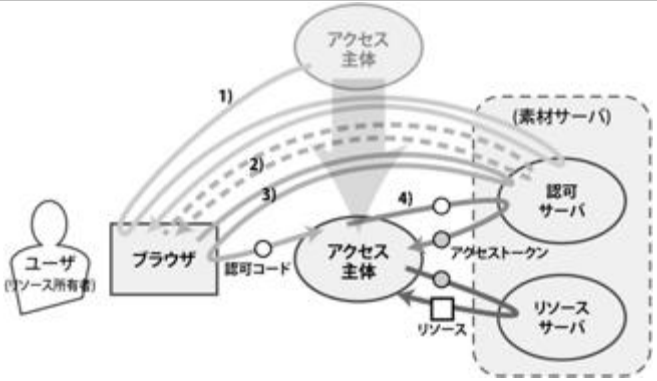
*API-Keyはセキュアか？

Question	Answer
「API key と パスワード」どちらがセキュアか？	・どちらも盗まれたら終わり （API Keyは盗まれることも考慮しないとならない）
「API key」の課題？	・乱用の可能性 （同じAPI keyを多用、流用してしまう、など）
OAuth2/OpenIDcで誰でも便利にセキュアに認証できる？	・「安全なサーバーかどうか」が課題 （バックドアなどがあれば意味がない、またトラフィック解析で「活動情報等」は抜かれ、（防犯ベルがOFFなど）推測される可能性はある）
その他？	・デバイス側でも設定課題がある・・・ （プロトコルよりも運用が課題）

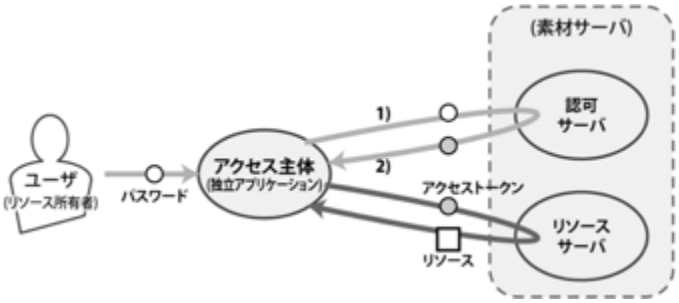
*REST APIへの攻撃

- インジェクション攻撃 (XSS, SQL, Xpath, Xquery)
- バッファオーバーフロー
- DDoS/DoS 攻撃
- XML 攻撃
- JSON 攻撃
- セッションハイジャック攻撃/ リクエスト強要（CSRF）
- 入出力の脅威を管理するためのAPI

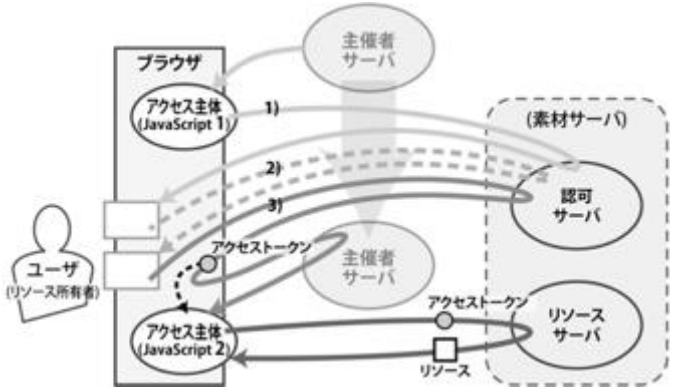
＊OAuth2



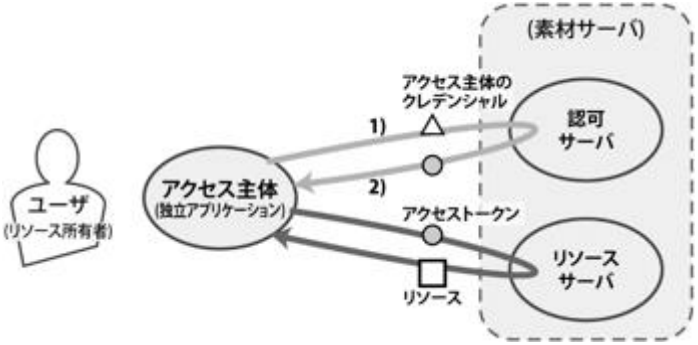
Authorization Code



Resource Owner Password Credentials



Implicit



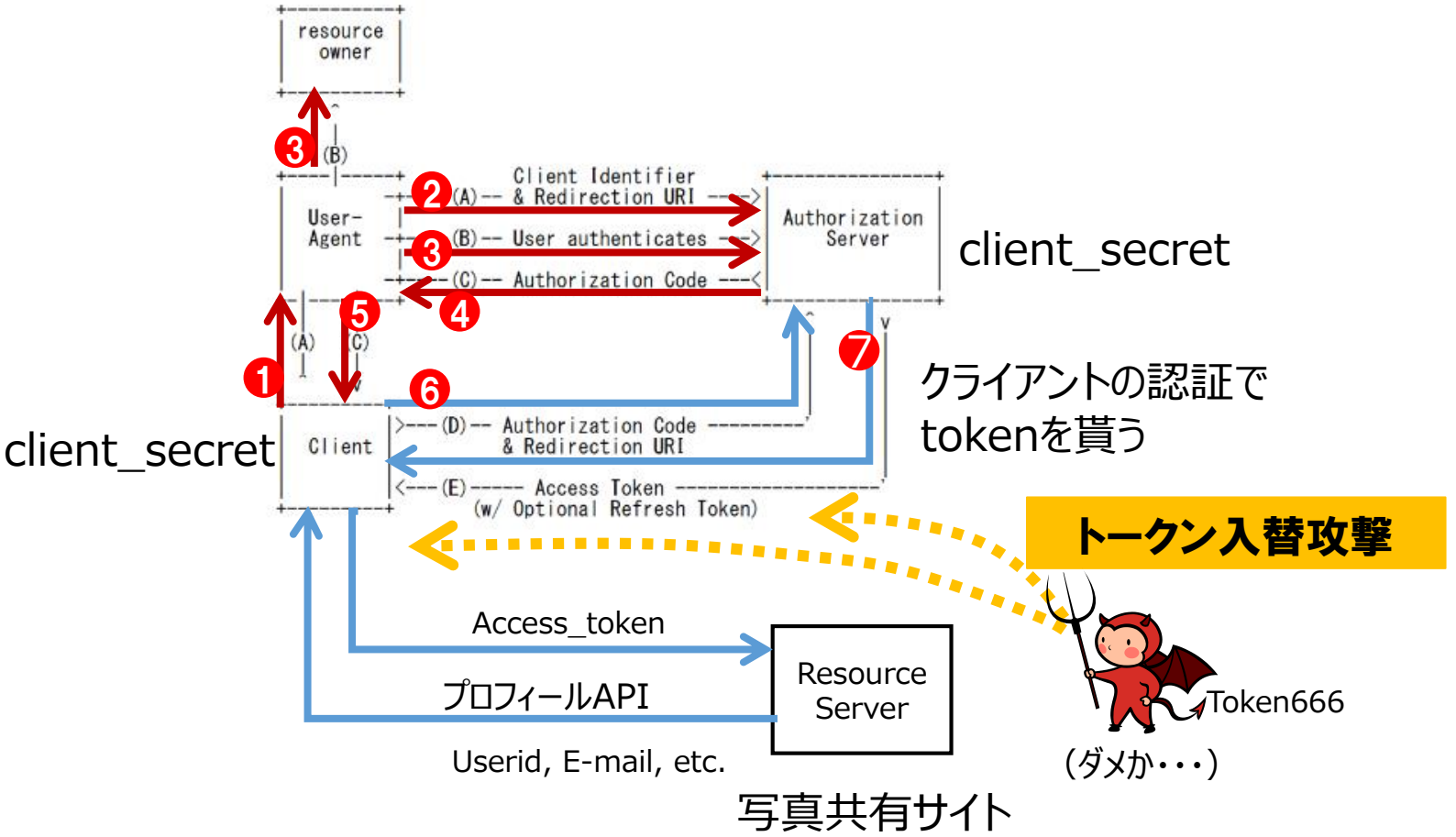
Client Credentials

Oauth：認可のみ（Authorization Code、Implicit、Resource Owner Password Credentials、Client Credentials）

出典：https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/709.html

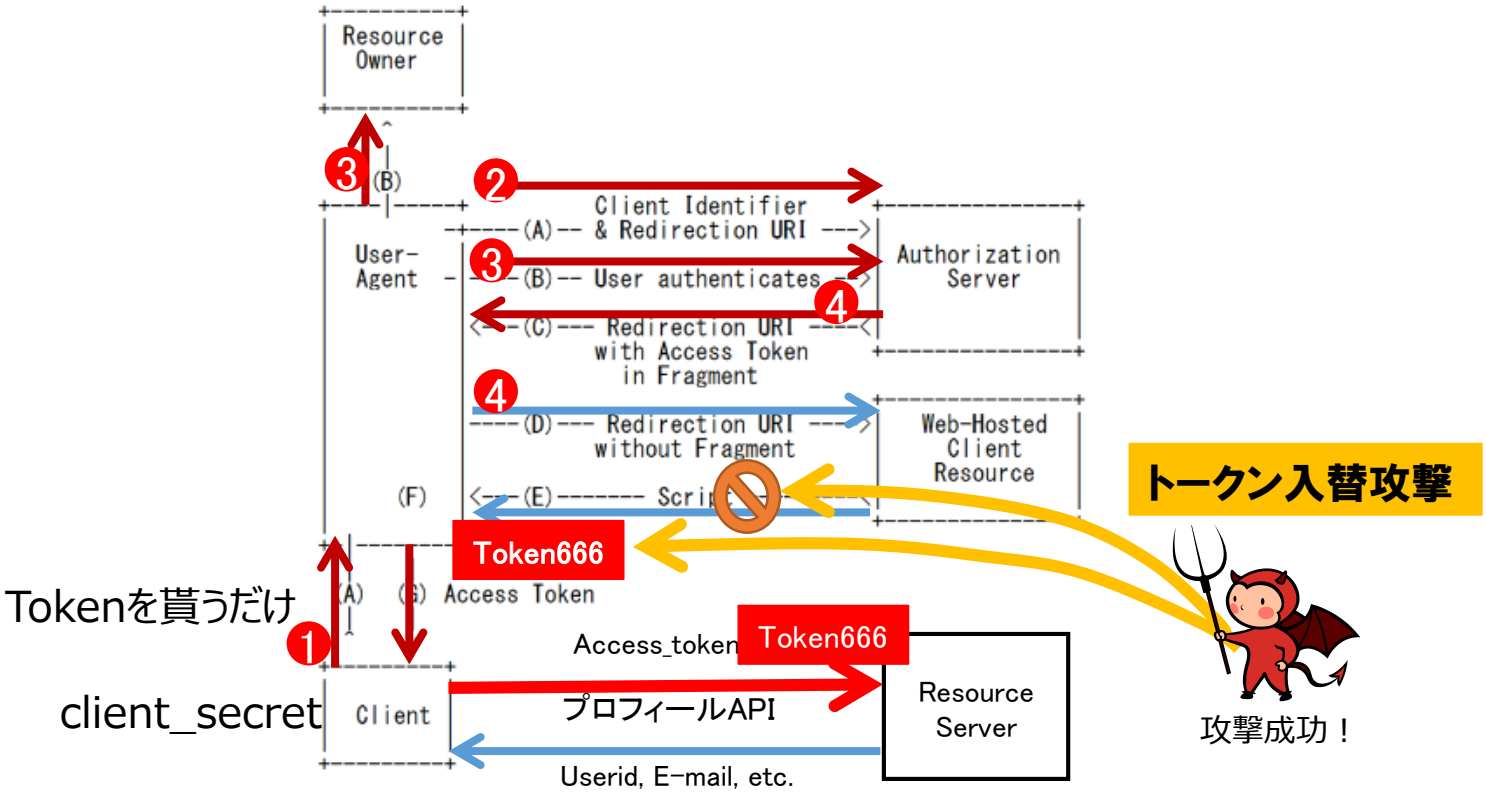
Client Secretを安全に保持することができる→Authorization Code
アプリケーションでの盗聴が可能→Implicit

*OAuth2 トークン入替攻撃



Client Secretのお陰で(6)のタイミングで「トークン入替攻撃」はできない

*OAuth2 トークン入替攻撃



「エンドユーザー (user_id)がクライアント (client_id)に対してリソース (scope) のアクセス権限委譲に同意した」という情報は得ない

写真共有サイト

Web-Hosted ClientにClient Secretが無いので「トークン入替」攻撃の可能性

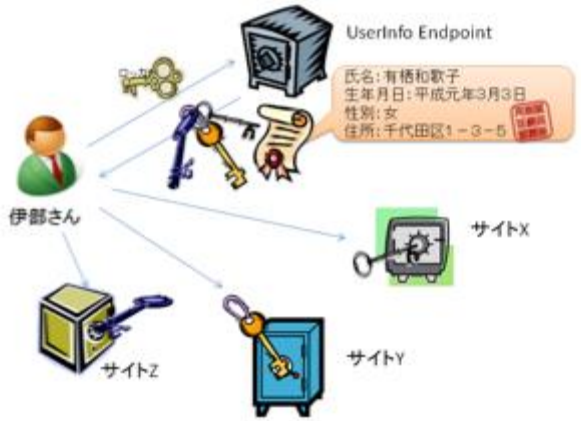
*OAuth, OpenID, OpenIDcの違い

図1　OpenID認証（身元確認）の場合

図2　OAuthで身元確認もどきをする場合

図3　OpenID Connectの場合

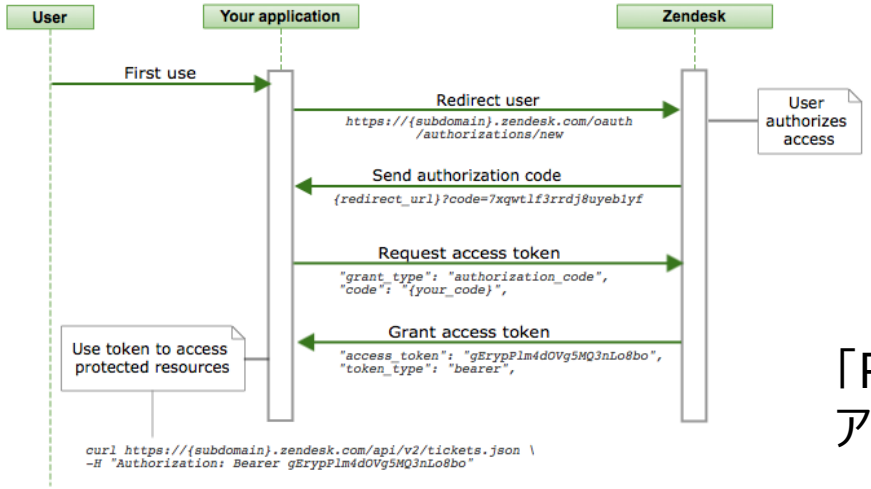
図4　OpenID Connectのクレーム集約、分散クレーム



出典：http://www.sakimura.org/2011/05/1087/

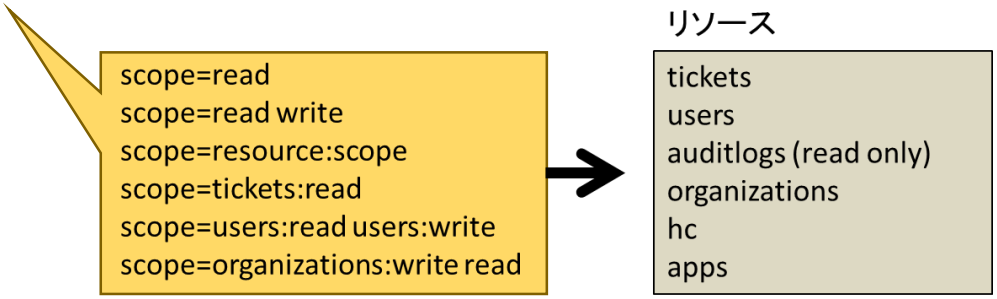
OAuthはあくまで認可のプロトコルで、身元確認で使うと問題
（身元確認でマンションの合鍵を渡すようなもの）→OpenID、OpenIDcを使う

＊OAuthのアクセス制御



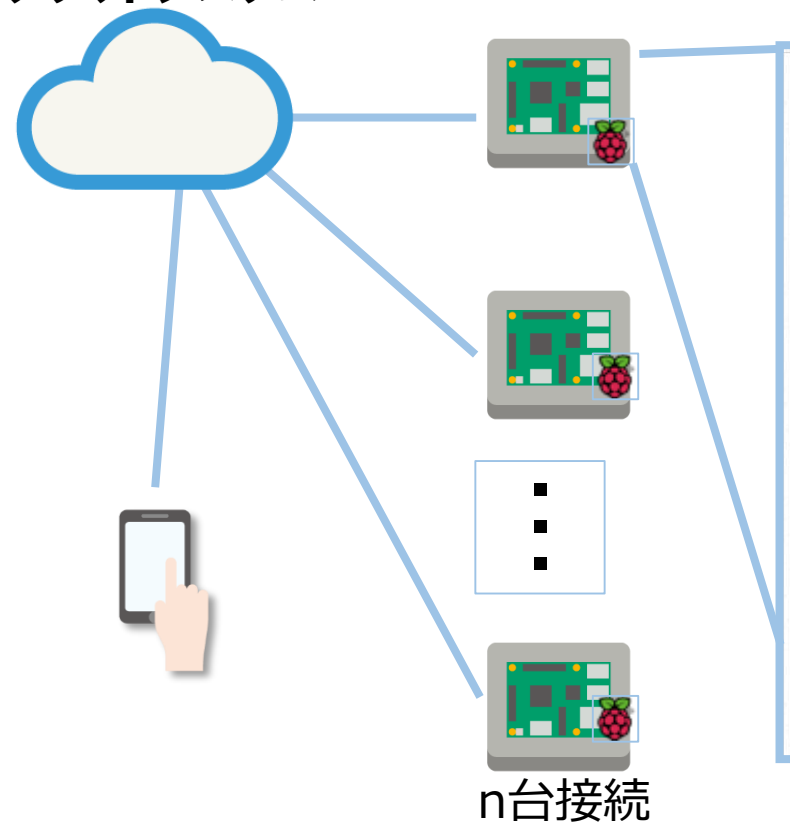
「Redirect Ｕｒｌ」でリソースへの
アクセス制御ができる

https://{subdomain}.zendesk.com/oauth/authorizations/new?response_type=code&redirect_uri={your_redirect_url}&client_id={your_unique_identifier}&scope=read%20write



出典：https://support.zendesk.com/hc/en-us/articles/203663836-Using-OAuth-authentication-with-your-application

*OAuth2 のアクセス制御

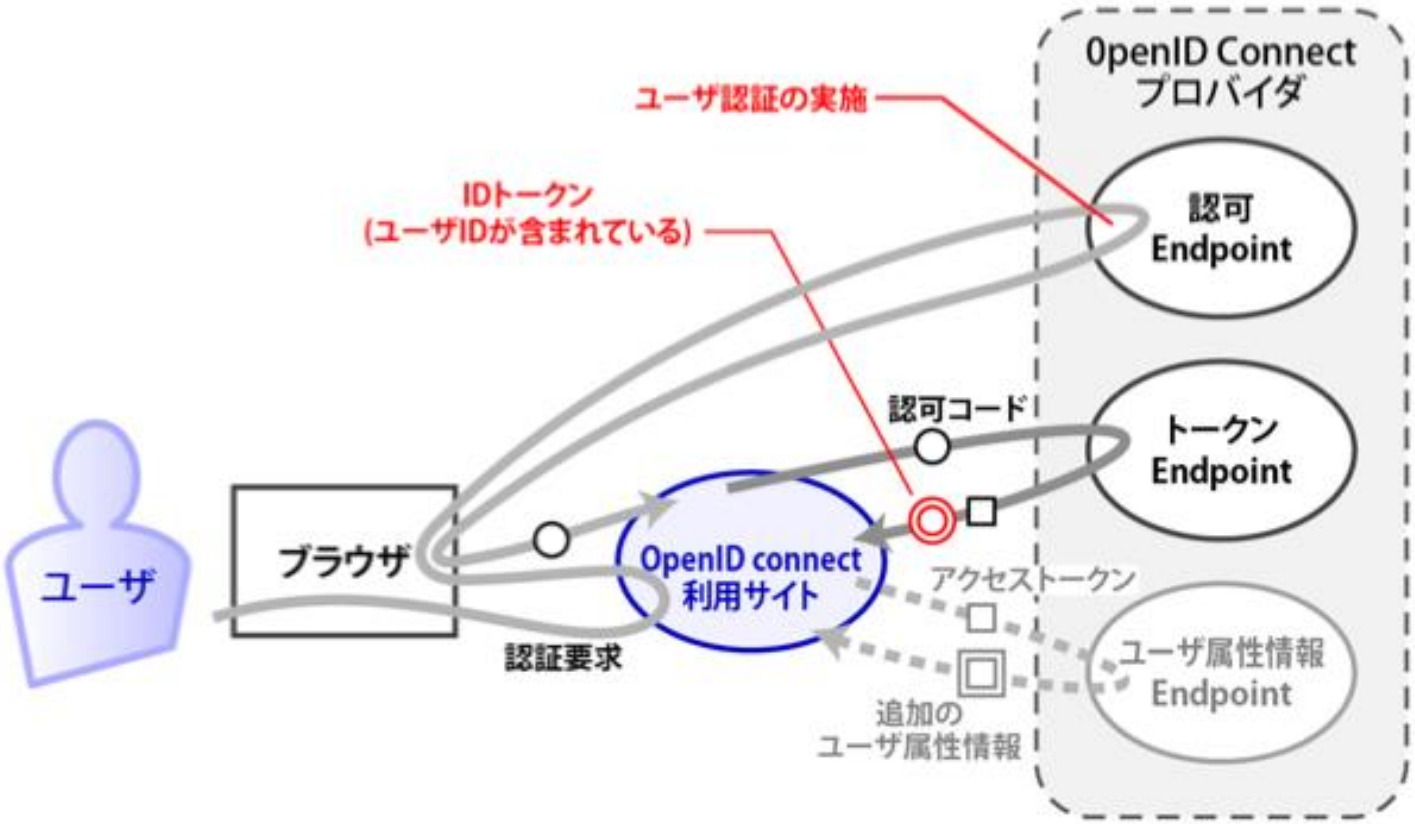



```
1  import gaugette.oauth
2  import datetime
3  import gdata.service
4  import sys
5
6  CLIENT_ID       = 'your client_id here'
7  CLIENT_SECRET   = 'your client secret here'
8  SPREADSHEET_KEY = 'your spreadsheet key here'
9
10 oauth = gaugette.oauth.OAuth(CLIENT_ID, CLIENT_SECRET)
11 if not oauth.has_token():
12     user_code = oauth.get_user_code()
13     print "Go to %s and enter the code %s" % (oauth.verification_url, user_code)
14     oauth.get_new_token()
15
16 gd_client = oauth.spreadsheet_service()
17 spreadsheet_id = SPREADSHEET_KEY
18 try:
19     worksheets_feed = gd_client.GetWorksheetsFeed(spreadsheet_id)
20 except gdata.service.RequestError as error:
21     if (error[0]['status'] == 401):
22         oauth.refresh_token()
23         gd_client = oauth.spreadsheet_service()
24         worksheets_feed = gd_client.GetWorksheetsFeed(spreadsheet_id)
```

出典：http://guy.carpenter.id.au/gaugette/2012/11/06/using-google-oauth2-for-devices/

場合により、n台の秘密鍵は「同一」となる可能性がある
（デバイス自体のハードウェアバックアップとしては都合が良いが・・・）

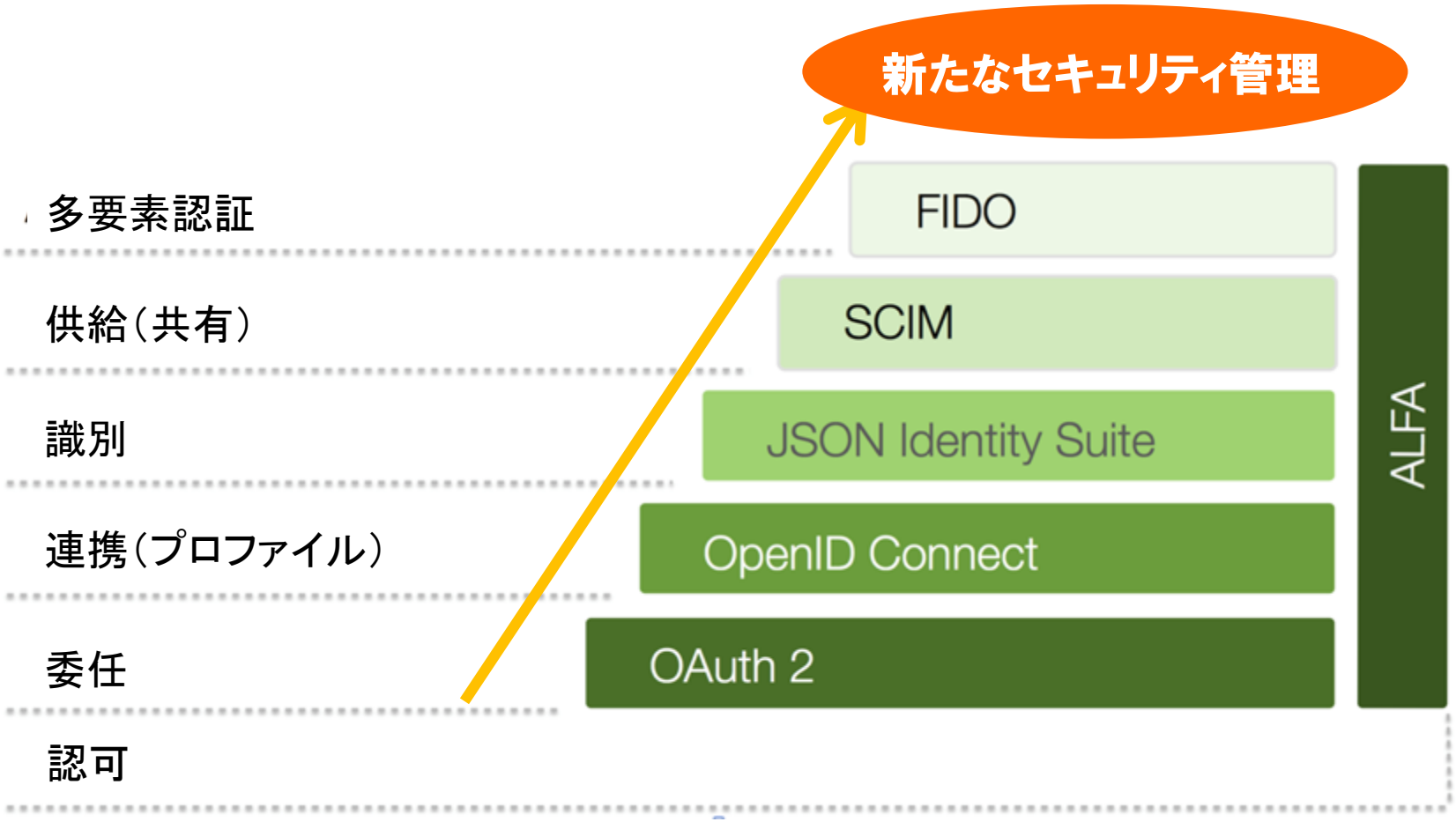
OpenID Connect
*OAuth2 ベースのアイデンティティ連携



出典：https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/104.html

OpenID Connect：認可＋認証＋属性取得

デバイスとシステムのセキュリティ
*SCIMから FIDOへ



出典：http://nordicapis.com/api-security-oauth-openid-connect-depth/

2-2-1. IoTのセキュリティ（組込み系）

組込みハードウェアに対する攻撃や解析について代表的な手法を示す

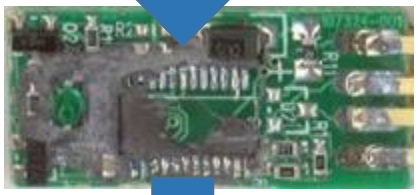
IoTのセキュリティ（組込み系）

＊ハードウェアセキュリティ（耐タンパー）

Before

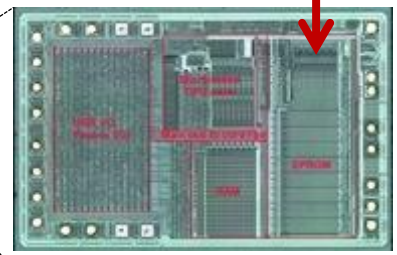
エポキシをニトロ系酸の薬剤で溶かす

After：



EEPROMの端子からデータを読出

EEPROM

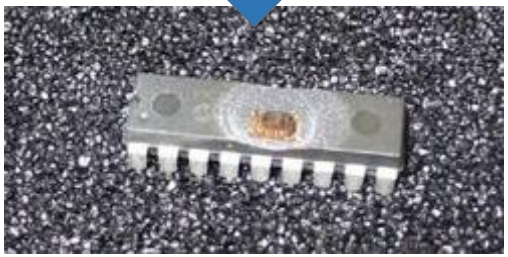


出典：http://blog.ioactive.com/2007/11/safenet-ikey-1000-in-depth-look-inside.html

Professional decapping devices

Nisene Jet Etch the gold standard in decapping.

プロ向けの“Decapping”装置が存在する・・・



出典：http://zacsblog.aperturelabs.com/

シールド系のハードウェアセキュリティは突破される可能性が高い

IoTのセキュリティ（組込み系）

＊Frozen　Attack

- 暗号鍵がメモリ中に一瞬現れる稼働中のSRAMのメモリを“凍らせ”てメモリを取り外し、専用の装置でSRAMから暗号鍵を取り出す

【対策】

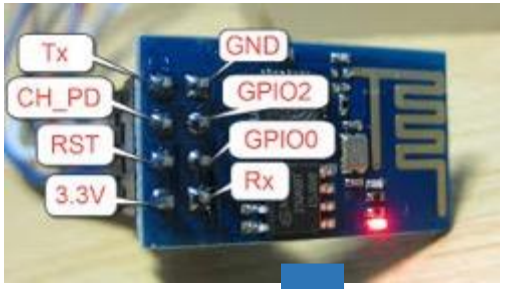
- TEASER：暗号鍵をセパレートに管理するLinuxのパッチが存在
- TPMはメモリ内で暗号化しない仕組みだが、一方でCPU内にセキュリティの機構が求められる

出典：http://hackaday.com/2009/01/18/use-the-cpu-cache-to-prevent-cold-boot-no/

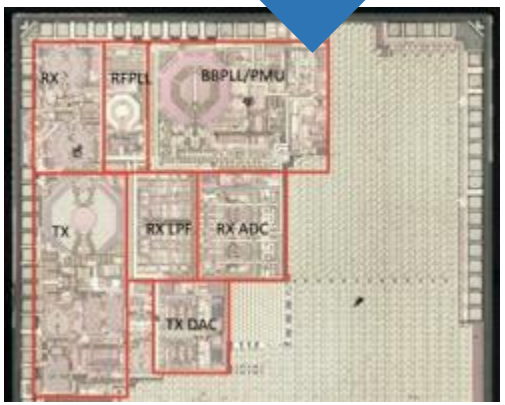
メモリを読まれないようにする対策が重要となっている

IoTのセキュリティ（組込み系）

＊ESP8266のDecapping



Decapping(内部構造を確認する)



- 一方で esptoolのコマンドから内部のファームウェアを読み込み可能
（ファームウェアは書換え可能）
- Linuxが動作するハードウェアで対策されたものも存在する
- 組込みでもリソースの豊富なデバイスでは、TrustZone、TPMなどで鍵のセキュアな保管が可能、セキュアブート（改ざん防止のみ）など保護対策が可能

出典：http://hackaday.com/2015/03/18/how-to-directly-program-an-inexpensive-esp8266-wifi-module/

RTOSレベルの動作を期待するハードウェアではセキュリティ対策がなされてない事が多い
（セキュリティ対策の不十分なルーター、防犯装置等のハードウェアの“オープン化”）

IoTのセキュリティ（組込み系）

*オープン開発とIP保護

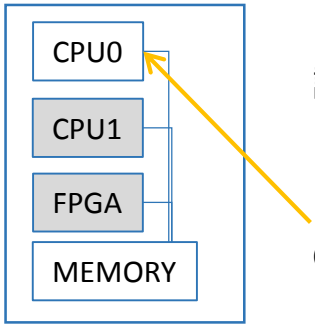
- OpenCV（カメラ）で物体認識
- ハンドジェスチャ操作
- 笛で操作

東大、自律型飛行ロボ「Phenox」がKickstarterで出資者を募集（850ドル、500台）

出典：http://gigazine.net/news/20140512-phenox/

Zynq-7000 Soc：
Linux 部分はオープンソース

CPU0 は“飛ぶ”、“カメラで撮る”、“特徴点を検出”等抽象的なライブラリーを提供、ユーザーが利用できる。CPU1とFPGAはクローズド



PKI を使ったセキュアブートの保護機能有り

CPU0 をオープン化

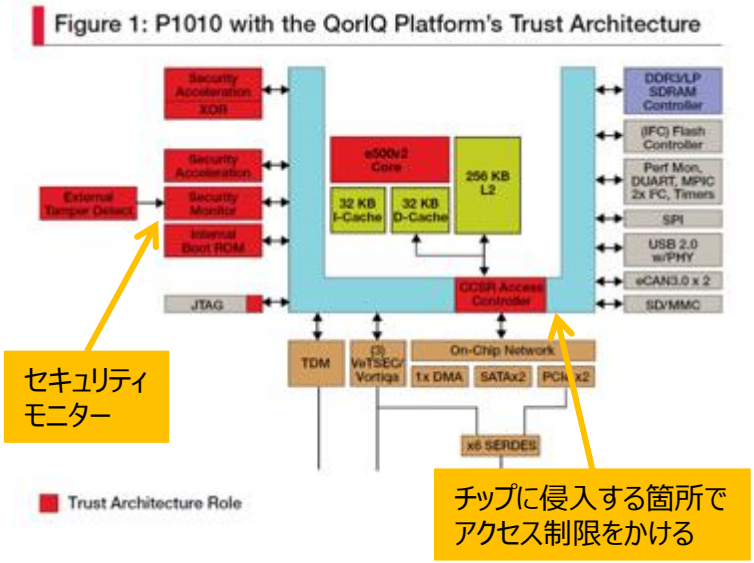
出典：http://weekly.ascii.jp/elem/000/000/317/317119/

オープン化（CPU0は開発者に使わせる）とクローズ化（FPGAに守りたい知財を隠す）

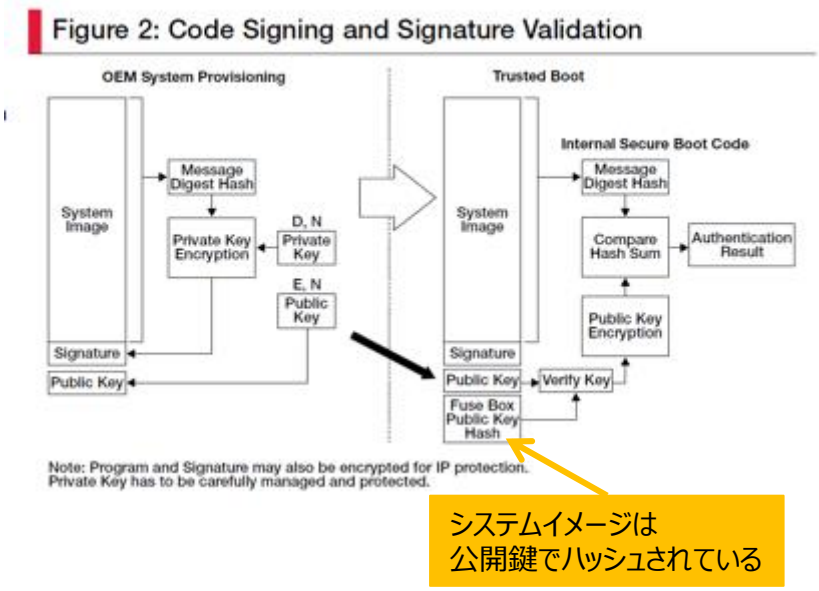
IoTのセキュリティ（組込み系）

*セキュアブートとコードサイニング証明書

●セキュアブート：



●コードサイニング証明書：



出典：http://cache.nxp.com/files/32bit/doc/brochure/PWRARBYNDBITSTA.pdf

セキュアブートはシステム（OS）の改ざんを防ぐ
コードサイニング証明書はアプリケーションの改ざんを防ぐ

2-2-2. IoTのセキュリティ（無線系）

　無線センサーネットワーク（Wireless Sensor Network）で利用される攻撃手法について例示する。

無線センサーネットワークへの攻撃

＊代表的な攻撃手法

複製ノード攻撃	不正取得したノードを大量に複製してネットワークにばら撒くことにより ネットワークに多大な影響を与える攻撃
ワームホール攻撃	悪意を持つノードが経路情報を 偽装して通信を誘導し情報を搾取
DoS 攻撃 ・Denial-of-Sleep （電力消耗攻撃）	サーバなどのコンピュータやネットワークリソース（資源）がサービスを提 供できない状態にする
リレー攻撃	無線通信を中継することで、所有者が離れていても動作させる
IP 偽装攻撃	IP通信において、送信者の IP アドレスを詐称して別のIPアドレスに 「なりすまし」（英：spoofing）を行う

IoTのセキュリティ（無線系）

＊RFIDへの攻撃

3～5mの距離で
チェック可能

その人の分析が
可能

その人の動態の
追跡が可能

出典：http://www.iot-a.eu/public

[1]	「ブロッカータグ」、「RFIDガーディアン」によるAnti-collision protocol（Singulation* Protocol）への妨害。 （ユーザーのプライバシー保護→検索妨害（DoS））
[2]	RFIDリーダーとRFIDカードへの「ジャミング」 （高出力のRFトランスミッターでシステムHaltに追い込む）
[3]	「ファラデーケージ」（金属の鳥かご、電波のアクセスを遮蔽）

IoT のセキュリティ（無線系）

*RFID のリレー攻撃

【リレー攻撃】（使用者に気づかれにくい）

→「スイッチオフ」できる RFID は現在存在しない→守りにくい

（使用者の意図しないところで起きる可能性）

→リレー中に信号を変更も可能

⇒NFC 付き携帯が使える

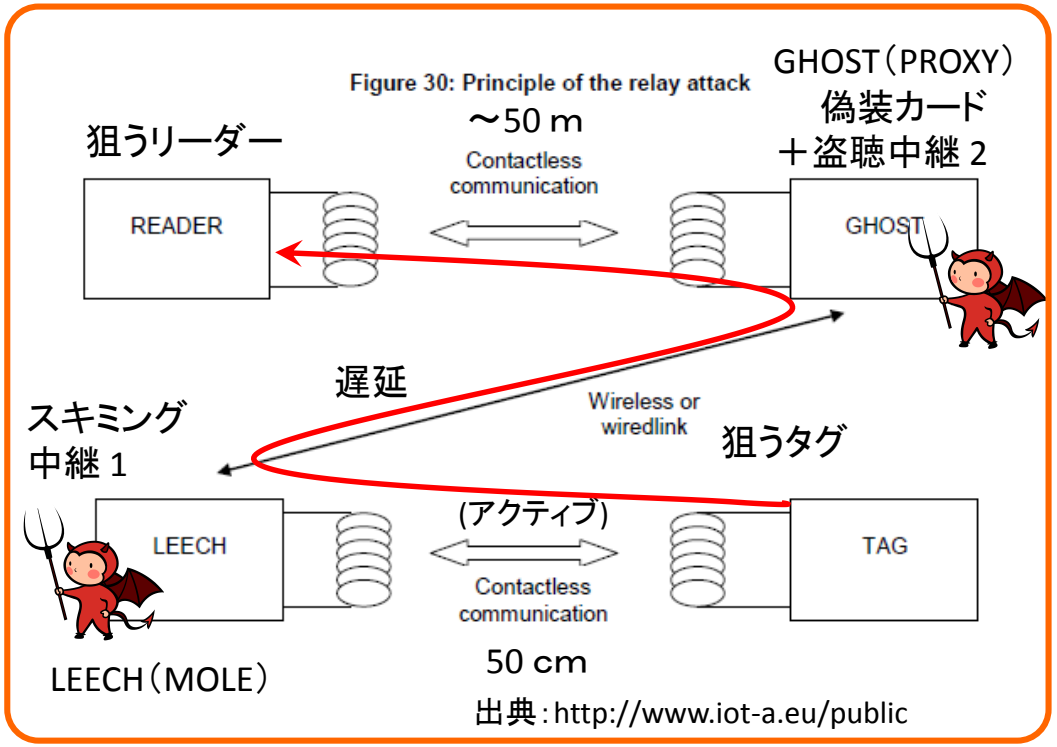
（コストは約200€、有線なら低コスト）

【問題】

→リレーによる遅延

（ISO 14443-3 規定タイミング

FWT＝5s 以内？など制限有）



2-3. IoT のプライバシー

IoT のアーキテクチャを検討する欧州の IoT-A プロジェクトにおいて、セキュリティのみならずプライバシーの問題について整理されているのでこれを参照、例示する。日本国内では IoT の仕組みに基づいたプライバシーの課題について整理しきれておらず、既存の個人情報保護法に則った対策が求められる。具体的な課題を明確にし、既存の法制度では対処できない事柄について意識していただくことを目的とする。

IoTのプライバシー

＊個人情報保護法

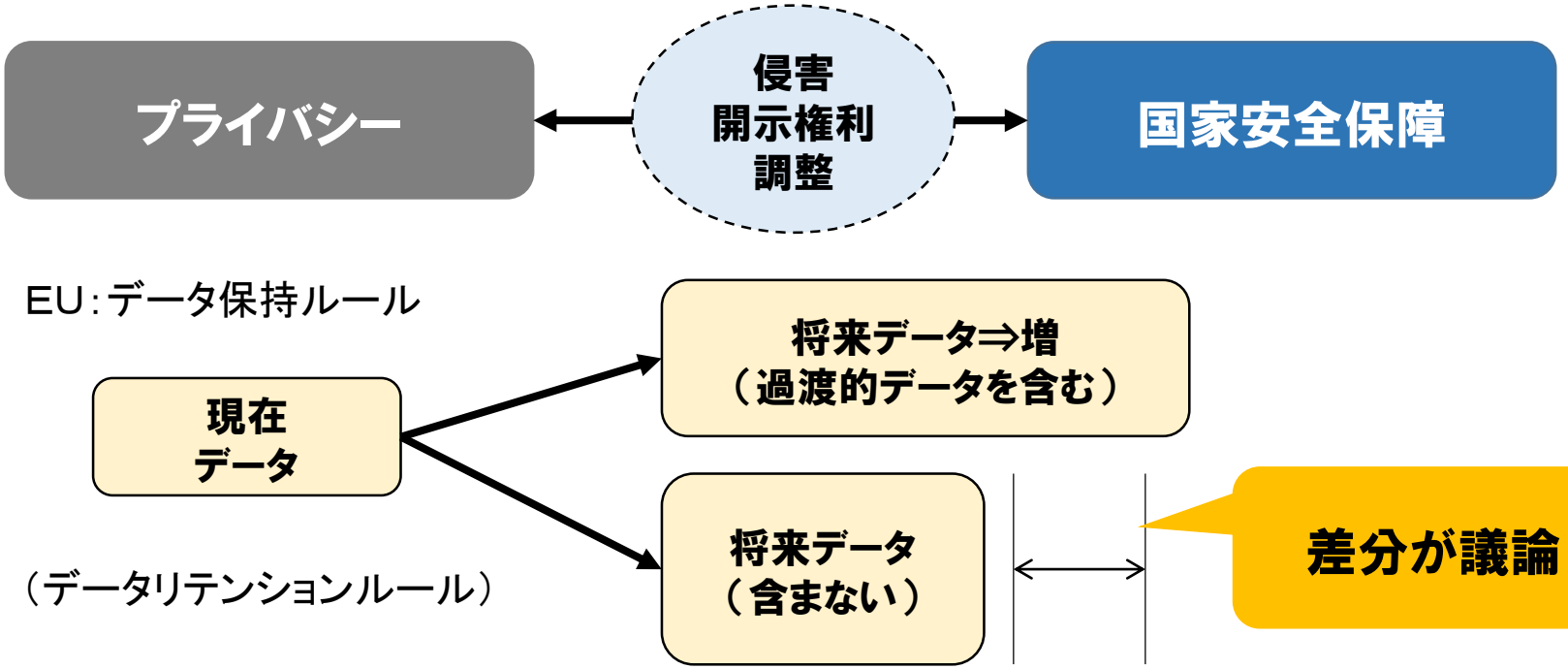
項目	分類	情報の内容	法律
個人情報	要配慮個人情報（センシティブデータ）	人種、信条、社会的身分等・・・	本人の同意を得ないで、要配慮個人情報を取得してはならない
			不当な差別・偏見が生じないように取り扱いに配慮する
			本人の同意のない第三者提供の特例 （オプトアウトからの除外）
	身体的特性に関する情報	指紋認識、顔認識データ等・・・	・特定の個人を識別できるもの ・他の情報と容易に照合でき、特定個人を識別できるもの （第三者に条件付で提供可能）
	個人または個人の使用する機器等に関する情報	名前、住所等・・・ 旅券番号、端末ID等・・・	

参考：http://www.mhlw.go.jp/file/05-Shingikai-10601000-Daijinkanboukouseikagakuka-Kouseikagakuka/151117_tf1_s4.pdf

「個人情報」か？「要配慮個人情報」か？を明確化する必要

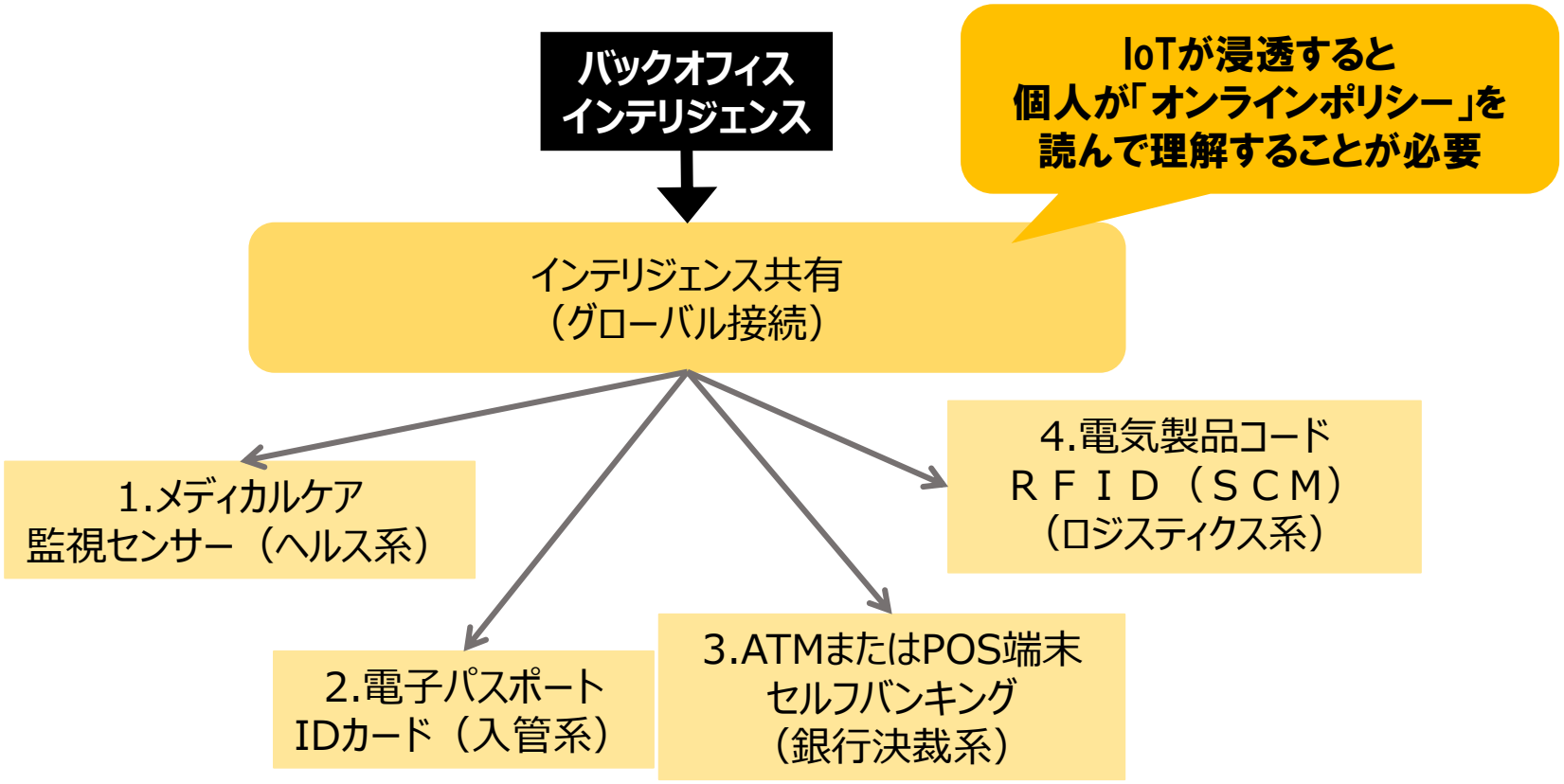
IoTのプライバシー
＊欧州標準（IoTA）の紹介

IoT-A (Internet of Things - Architecture)　：6章セキュリティとプライバシー



欧州は「対米国」を意識して「プライバシー」を重視している
だが「個人情報の利活用」は積極的に行う方向である

IoTのプライバシー
＊欧州標準（IoTA）の紹介



欧州がターゲットとする上記事業分野（１から４）ではプライバシー配慮の反面、インテリジェンス共有において現状の「ポリシー承諾」は非現実的

2-4. 誰でも作れる IoT

IoT は誰でも作れる時代で、廉価なマイコンボード（ラズパイなど）を利用すればプログラミングやハードウェアの詳しい知識がなくとも作れるようになったが、そこにはサイバーセキュリティ対策などが行われず、管理されていない「野良」と言うべきものが増え続けている。当然、プライバシーについても課題があり、画像認識技術の利用の際には留意すべき点がある。

誰でも作れる IoT
*インターネットラジオを作ってみる

1.秋葉原でPi＋LCDとボリュームつまみ（ロータリーエンコーダー）購入

Raspberry Pi 2　＋　**LCD　16x2**　＋　**RGB-LED付つまみ**



2.ハードウェアの組立て
→GPIOの配線と半田での接着

3.インターネットラジオのインストール
→mpc/mpdを用いる（他に、XBMCを用いる方法もある）

4.プログラミング
→ここで発見・・・（セキュリティの実態）

誰でも作れる IoT
*インターネットラジオに画像音声認識機能を追加

PiCamera
カメラモジュール

SG90
サーボモーター

MPL1152A
気圧センサー

OSRB38C9AA
赤外線リモコン

SB612A
赤外線センサー

USBオーディオ変換

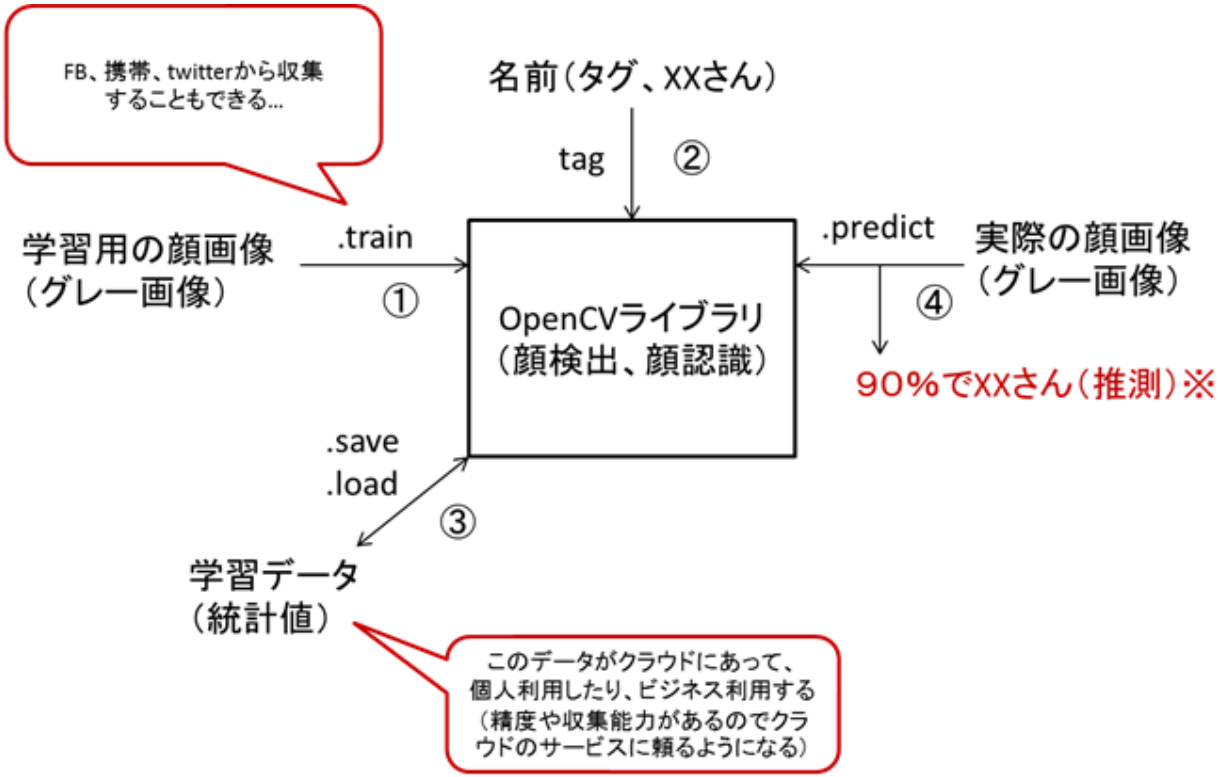
画像音声認識
インターネットラジオ

誰でも作れる IoT
＊オープンソースの画像音声認識機能の課題

- **PiCamera と OpenCV による物体認識**
  カスケード分類器（*.xml）を改ざんすることで物体認識のすり替えが可能
  例：バナナを人の顔として認識する
- **Open JTalk での音声合成**
  勝手に喋られる可能性
  ./jsay “在宅中です” のコマンドの引数である文字列を書き換えることで情報を改ざん、不在なのに在宅と喋らせる
- **Julius による音声認識**
  サーバー側で音声認識を行うと、通信ソケットが晒され、異なる音声実行を行うことが可能
  ＃julius -C xxx.jconf –module （起動する）
  ＃jcontrol IP address

誰でも作れる IoT

＊顔画像処理時のプライバシーの問題



改正個人情報保護法で、顔画像は保存せず一時利用する必要あり
学習の過程で個人情報を使う必要がある

誰でも作れる IoT

*プライバシーの問題と匿名化

機能	技術	データ	情報の分類	匿名加工
顔・物体認識 （顔認証）	OpenCV	顔認識テンプレート （グレイ画像テンプレート） 「ｘｘさんの顔」自体 または統計的情報をもつ カスケードデータ	個人情報	・目視での判別不可にするだけで良いか？ ・数学的に個人を特定できるデータは個人特定性か？
音声認識 （声紋認識）	Ju l ius	固有名詞（文言）などのデータ （声紋データ） 「ｘｘさんからの声」		・相手に名前を言わせるは個人特定性か？
音声合成 （会話での認証）	OpenJTalk	固有名詞（文言）などのデータ 「ｘｘさんの声がけ」		・地域内で人が分る表現は個人特定性か？ ・名前を言って応答を待つ、文言から顔画像や名前が特定できるなら、個人特定性か？

オープンで実績ある「匿名加工技術」が少ない
k-匿名化法はデータが多数あって成立するためデータが必要

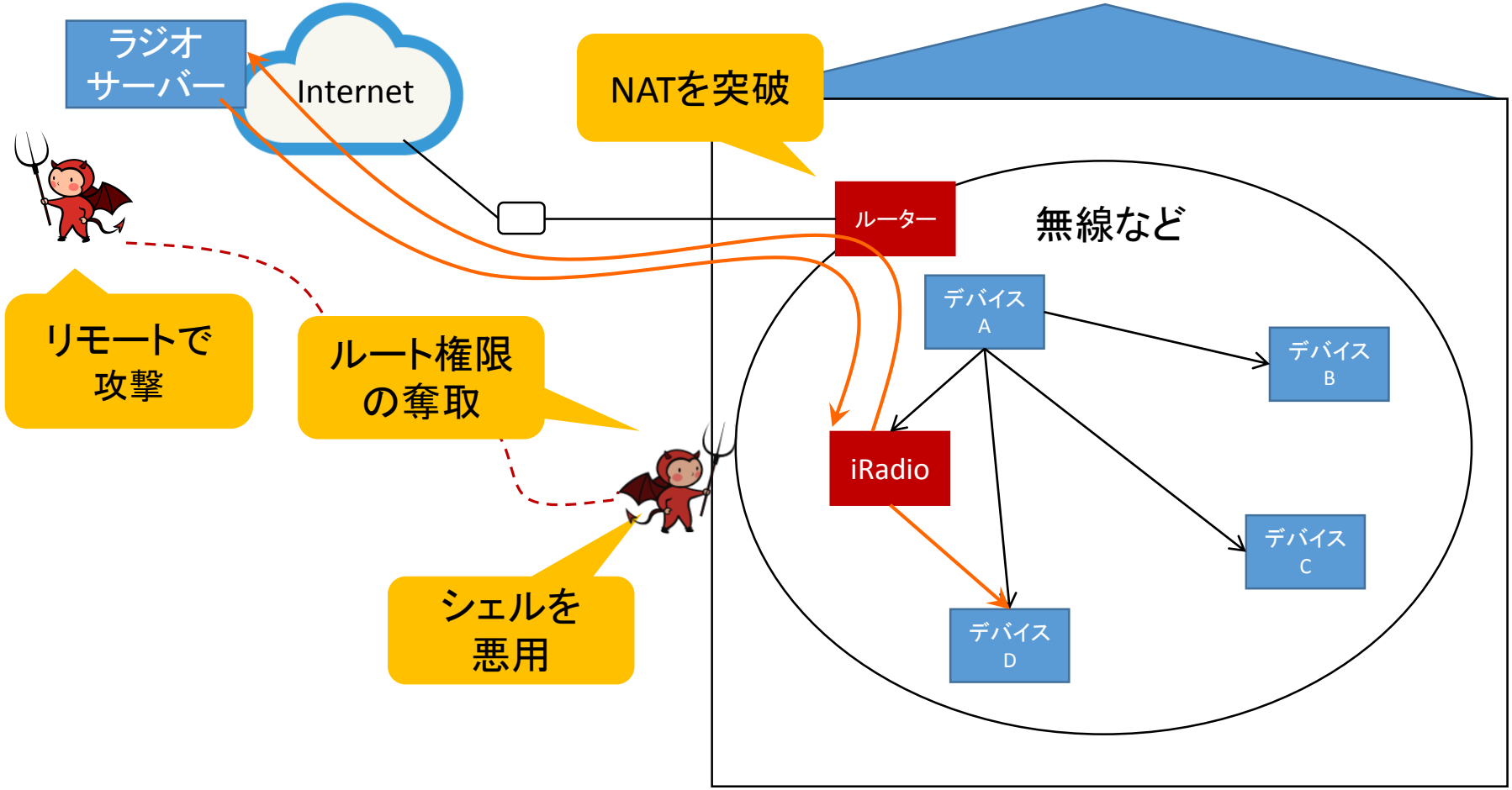
誰でも作れる IoT
＊セキュリティの問題とルート権限

- ラズパイなどで利用可能なホビー用のOSやミドルウェア、アプリケーションは「ルート権限の固まり」
  - sudo python iradio.py
    インターネットラジオのモジュール（mpc）をシェルを呼び出し、
    Pythonのsubprocess モジュールの Popen にて、「shell=True」、
    「stdout=PIPE 」を使う

一般に入手可能なアプリケーションが複数あり、組み合わせることで便利
しかし、セキュリティ上は管理者（ルート）権限で動作するため危険

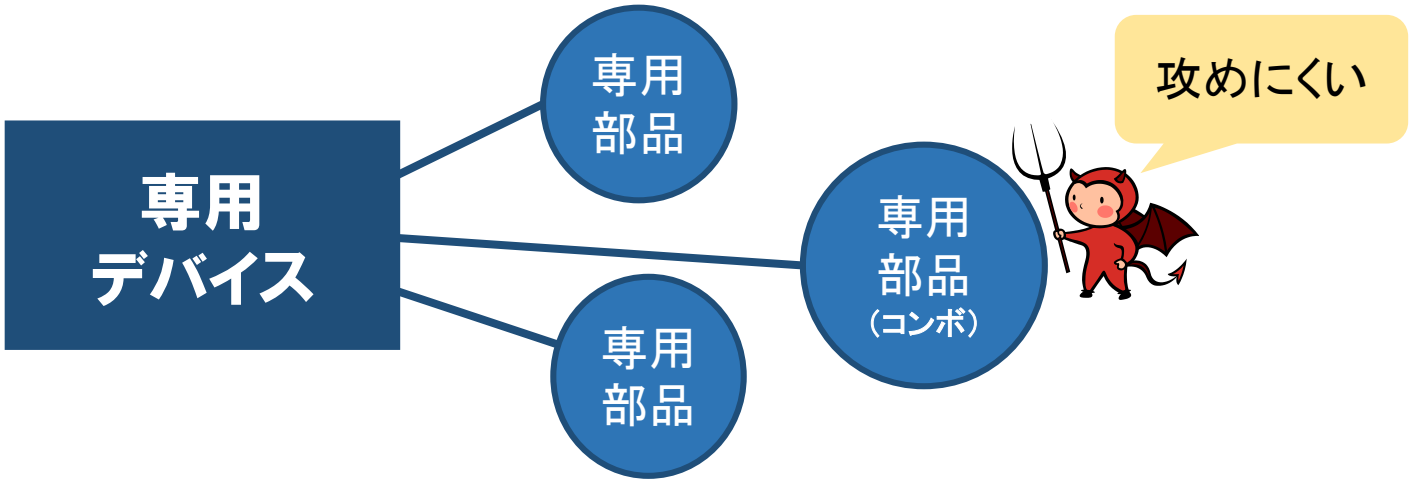
誰でも作れる IoT

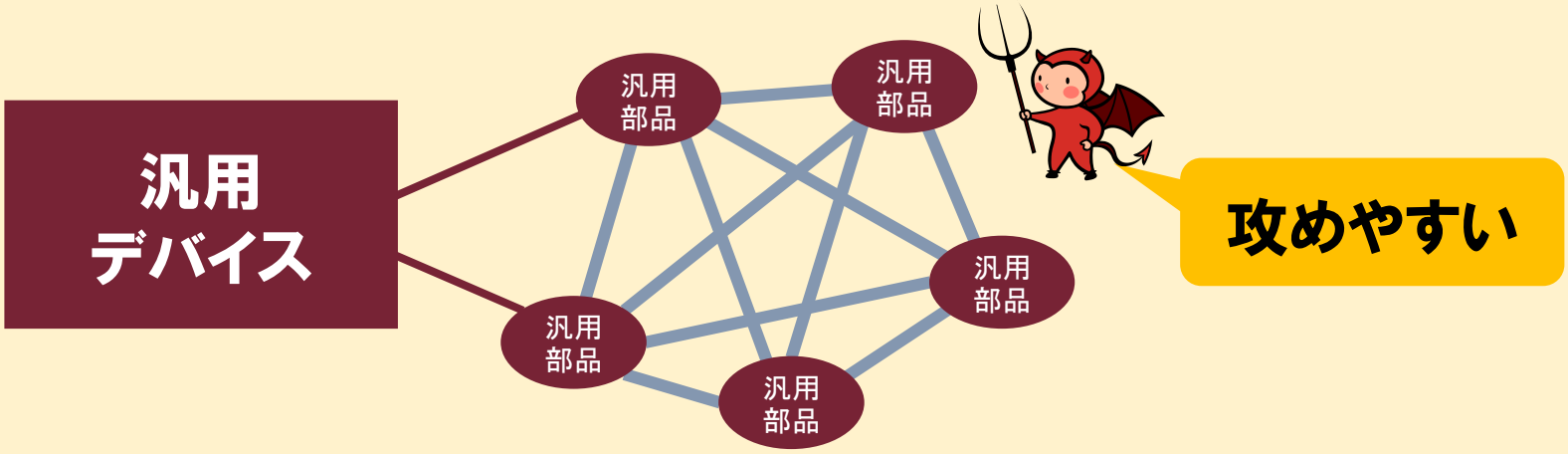
*セキュリティの問題とルート権限



誰でも作れる IoT

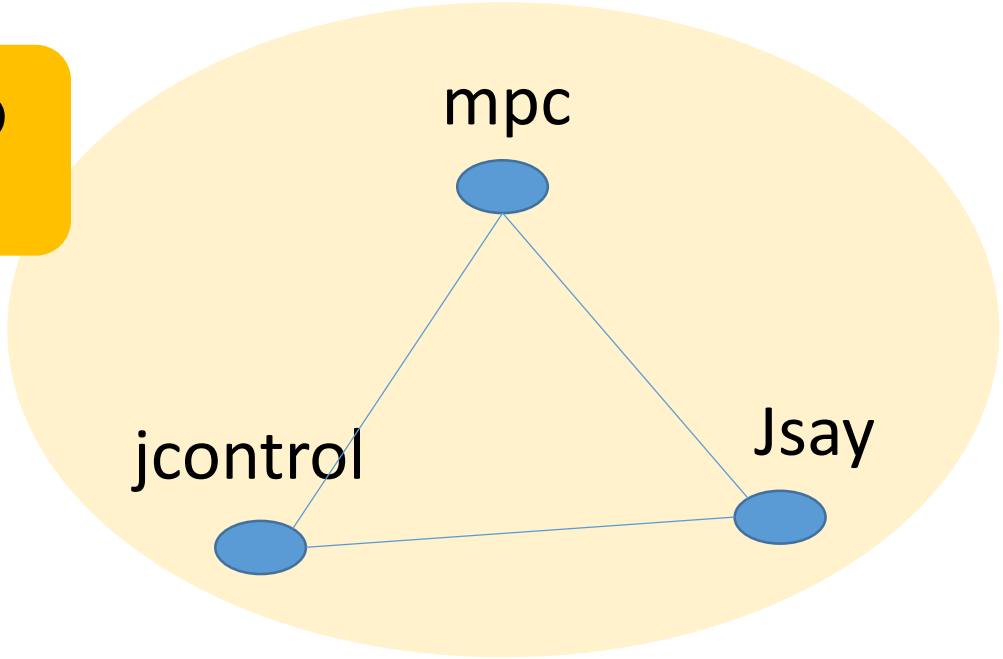
*セキュリティの問題と汎用デバイス





誰でも作れる IoT
*セキュリティの問題とコマンド

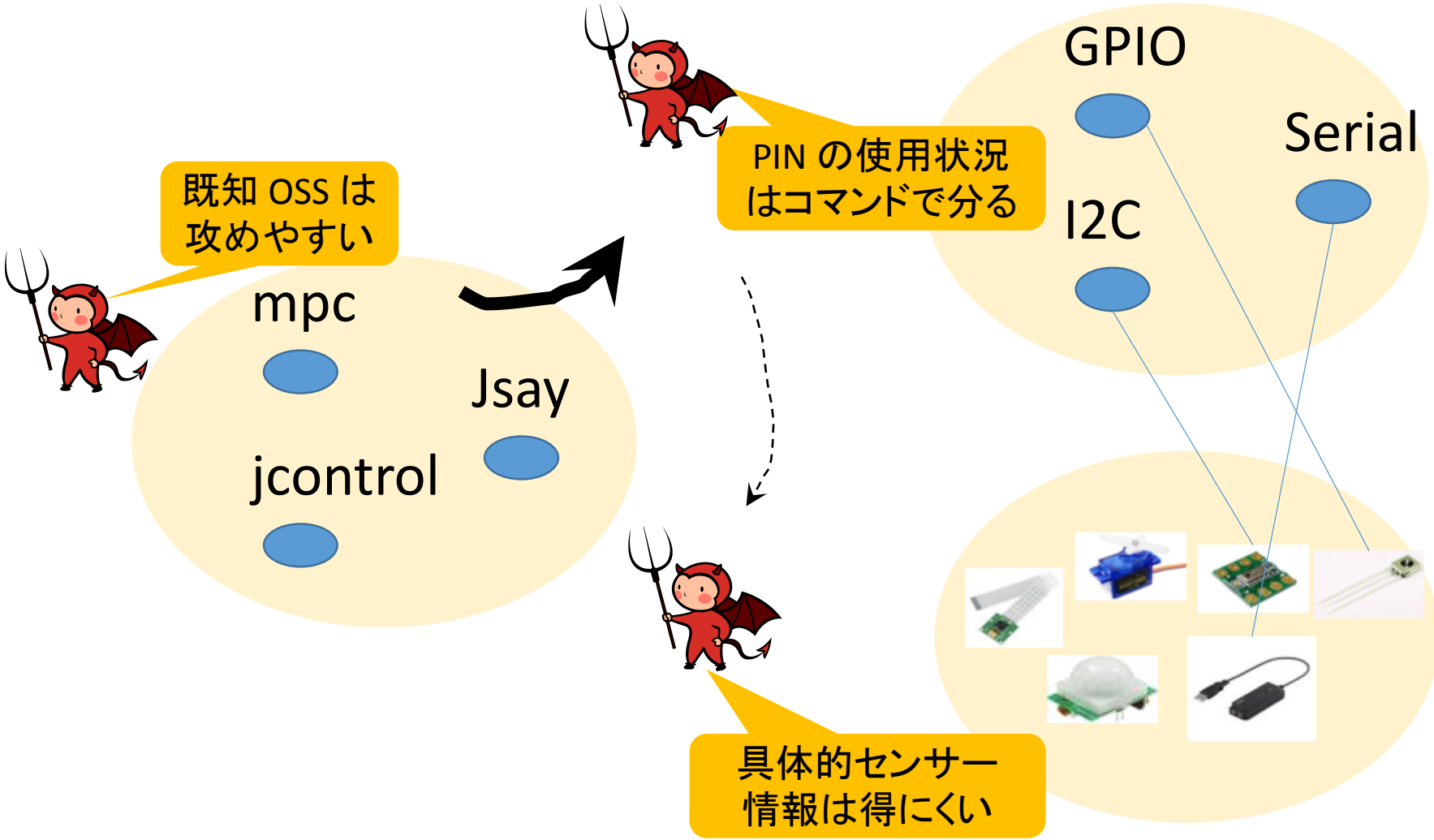
いずれかのコマンドの脆弱性を突けばよい



command = bin/bash mpc play | jsay

誰でも作れる IoT

*セキュリティの問題とシステムの把握



誰でも作れる IoT
＊セキュリティ上考慮すべき事柄

- **ファイルの範囲を特定のディレクトリ下に制限**
  - Chrootなどの利用
- **プロセス、リソース、ユーザーに対する制限**
  - SE Linuxなどの利用
- **セキュリティbyデザイン、プライバシーbyデザインが重要**
  - OpenIDc、OAuth2など、パスワードレス（認可、委任）技術の利用
  - ｋ-匿名化法の利用
- **物体情報の「紐付き」解消（プライバシー）**
  - 個人と物体情報（ナンバープレート等）が「紐づく」場合、等
- **野良IoTデバイスのセキュリティについて**
  - 汎用コマンドのカスタマイズの危険性の認知
    （簡単保護モード：「一発」で鍵を閉めるような、簡素な仕組みが必要）

など

3. ベンダーとして IoT デバイスを提供する際に検討すべきこと

ベンダー（提供者）は IoT の仕組みや構造について詳細を理解していないユーザー（利用者）が IoT 製品やサービスを安全に利用するために考慮すべき事柄がある。この章では、サイバーセキュリティの観点から企画・開発から製品・サービスの提供にわたり、どのようなことを考慮し、ユーザーに伝えるべきか例示する。

ライフサイクルについて

＊ベンダーの製品提供と保証

製品保証期間 → セキュリティ更新の提供期間

- 個人向け IoTデバイスは、任意の利用目的で所有、利用するものであるため、製品の保証期間をベンダーが定めたとしても実際に稼働する期間を厳密に定義することはできない
- このため、セキュリティ含め、安全に利用することのできる期間を設定する必要がある
- 上記の「製品保証期間」は製品の保証を提供する期間で、製品の不具合（ハードウェアの材質上や製造上の瑕疵など）について保証を提供する期間は、通常1年程度とされる
- 「セキュリティ更新の提供期間」とは、製品保証期間を過ぎてもユーザーが使い続けることを想定し、製品に対するセキュリティの更新を提供する期間である
- この期間を過ぎた場合ユーザーには「廃棄」することを勧めるなどの対応が望ましいと考えられる

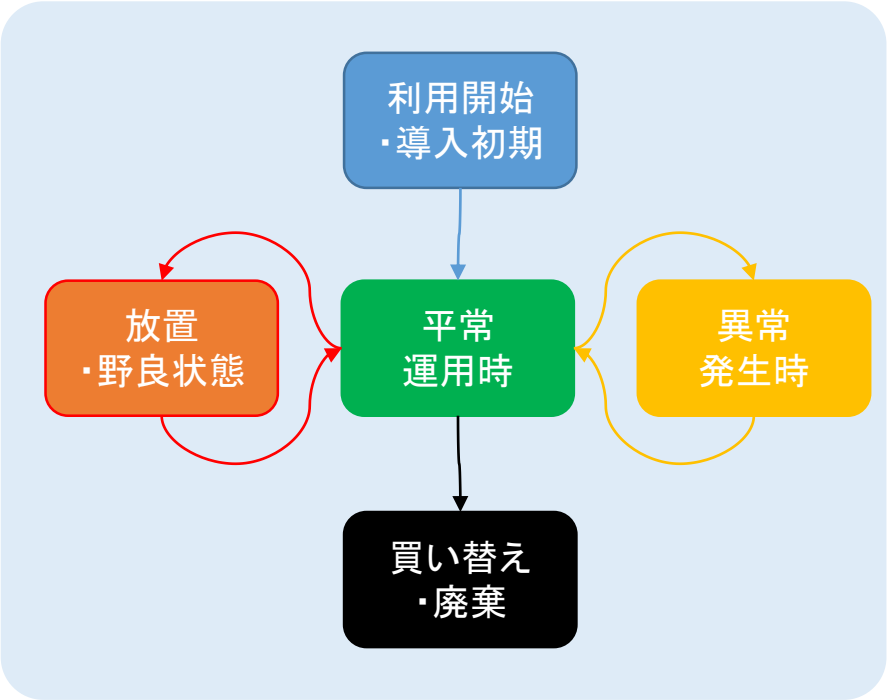
※経済産業省ではベンダー（事業者）に対して「製品安全に関する事業者ハンドブック 」を発行している

http://www.meti.go.jp/product_safety/producer/jigyouhandbook.pdf

ライフサイクルについて

＊ユーザーによる製品の利用

- 利用開始の際に、デバイスの導入設定がユーザーにとって複雑でなく、初期設定に必要な情報などを第三者が再利用することのできない仕組みを提供することが望ましい。
- 利用を開始した後、デバイスに異常が発生した場合、異常を解消して復旧する必要がある
- 利用開始後、長期間にわたって使用せずに稼働させたまま放置することで第三者がデバイスにアクセスすることが可能な状態を「野良」と呼ぶが、セキュリティ上は好ましくない。
- デバイスが不要となる場合には、記録・保存されたデータの消去や初期化についての手順が準備され、ユーザーが対処するか、ユーザーが対処せずともよいような仕組みがあることが望ましい



3-1. デバイスの構成と想定される脅威

個人や家庭での利用を想定した IoT 機器は用途によってネットワークや外部機器との接続、アプリケーションや OS の更新の仕組みが異なる。それぞれの代表的な機器（スマート家電、汎用マイコンボード（ラズパイなど）、ウェアラブルデバイス、スマートウォッチ、webカメラ（見守り用））について、そのシステムの構成と想定される脅威とを想定することで、具体的な対策を機器側、システム側について検討する。

3章と4章の違い

- 3章はベンダーが IoT 機器やサービスを開発する際に考慮すべきサイバーセキュリティ上の脅威を列挙し、想定される対策例を示す
- 4章では3章で提示したベンダー向けのガイドとは視点を変え、専門知識のないユーザーに対してベンダーや開発者が安全な仕組みを提示するのに必要な観点を示す
- ベンダーは IoT デバイスの企画・開発、販売に際して、 IoT デバイスおよびデバイスで利用するインターネット上のサービスに対し、サイバーセキュリティ対策を施し、ユーザーが行なう必要のある操作や作業を特定して適切なガイドを行なう必要がある
- ユーザーに適切なセキュリティ機能を提示することは、ベンダーのサポートやインシデント対応コストを下げることにもつながる

サイバーセキュリティとは何か？

IoTの時代を迎え、情報システムだけでなく多種多様な機器やセンサーなどが接続された複雑なシステム全体についてのセキュリティを指すのが「サイバーセキュリティ」。つまり、サイバーセキュリティという場合には、システムに接続されたこれらの機器やセンサーを含めた仕組み全体のセキュリティである。

IoTあるいはそれに類する製品やサービスについて過去に明らかになったリスクを例示する。

- 会話するバービー人形のプライバシー侵害リスク：2015/12/01: AFPBB (www.afpbb.com/articles/-/3068650)
- クライスラー、ハッキング対策で 140万台リコール：2015/07/25: 日経 (www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/)
- スマートエントリー車をハックする窃盗団の手口：2015/04/19: WIRED(wired.jp/2015/04/19/new-york-times-columnist-falls-prey-to-signal-repeater-car-burglary/)
- ５歳の「ハッカー」、父のゲーム機に侵入：2014/04/07: CNN(www.cnn.co.jp/tech/35046195.html)
- 中国から輸入したアイロンに無線LAN経由でスパム攻撃をするチップが発見される：2013/10/29: Gigazine (gigazine.net/news/20131029-spam-chips-hidden-in-iron/)
- スマートテレビに脆弱性、カメラで「のぞき見」される恐れも：2013/08/02: CNN（www.cnn.co.jp/tech/35035482.html）
- 子ども部屋から不審な声、男がカメラ乗っ取り罵言：2013/08/16: CNN(www.cnn.co.jp/tech/35036051.html)

リスクがどのような「脅威」によって現実化する恐れがあるかについて検討する際に本ガイドを参照してほしい。

想定される脅威について

本ガイドでは、IPAが発行した「自動車の情報セキュリティへの 取組みガイド 」を元に、IoT デバイスへの脅威を以下のように定義した。これを異なるデバイスに当てはめて脅威分析を行う。
*http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf

- 利用者による操作に起因する脅威
  1. 操作ミス　デバイスやシステムを誤動作させられてしまう
  2. ウィルス感染　デバイスやシステムが有する情報やデータが漏れるか誤動作させられてしまう
- 攻撃者による干渉に起因する脅威
  3. 盗難　デバイスが盗まれてしまう
  4. 破壊　デバイスが破壊されてしまう
  5. 盗聴　通信内容を他人に知られてしまう
  6. 情報漏えい　知られたくない情報を盗まれてしまう
  7. 不正利用　他人にシステム、デバイス、ネットワークを使用されてしまう
  8. 不正設定　他人にシステム、デバイス、ネットワークを設定変更されてしまう
  9. 不正中継　無線や近接による通信内容を傍受されるか、書き換えられてしまう
  10. DoS攻撃　システム、デバイスの機能やサービスが利用できなくなる
  11. 偽メッセージ　偽メッセージによるシステム、デバイスが誤動作してしまう
  12. ログ喪失　動作履歴が無いため、問題発生時に対処方法がわからなくなる

脅威一覧表の目的と使いかた

- 本章で扱う「4種の IoT 機器」は、それぞれユースケースが異なるため、前出の「12種類の想定される脅威」を縦軸、5つの状態で示されるライフサイクルを横軸とし、各脅威の各状態において取り得る対策の例を列挙している
- 例えば、「スマートテレビ」が「平常運用時」において「盗難」にあった場合、「スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる」という対策を例示する
- 「ウェアラブル」が「平常運用時」において「盗難」にあった場合、「GPSなどを利用してデバイスの位置を把握することができるようにする」および「リモートワイプできるようにする」が付け加えられる

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• N/A	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• N/A

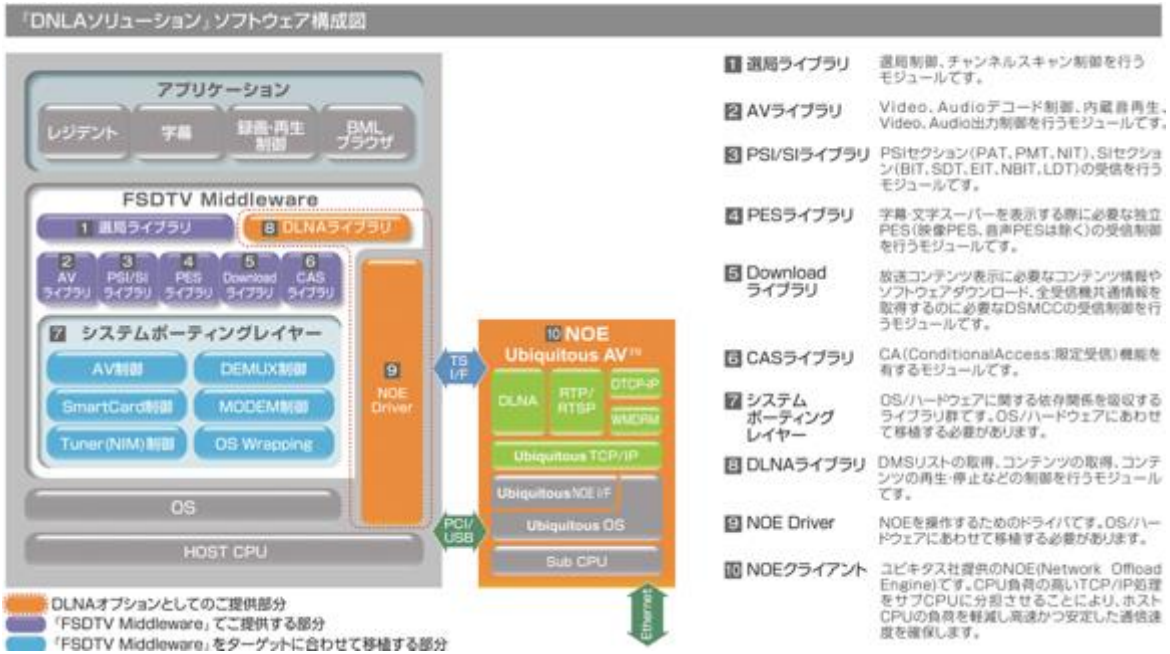
- なお、テレビ、ウェアラブルデバイスおよびネットワークカメラは、製品を開発提供するベンダーに対するガイドを提供するが、汎用マイコンボードは、ボードを利用してシステムを開発するユーザーに対するガイドを提供するものとする

スマートテレビ：システム構成

スマートテレビについて

- スマートテレビとは、インターネット接続機能を持っており、Youtubeなどのコンテンツを検索、再生でき、ハードディスクを増設することで録画容量を増やすことができ、インターネット経由で番組予約を行うなどができるテレビあるいはセットトップボックスを指すものとする
- 地上波デジタル放送の再生や、周辺機器との接続やコンテンツの共有、ウェブブラウザーやYoutubeの視聴など、機能の多くはソフトウェアによって実現され、Linuxなどの汎用OS上に汎用のアプリケーションをインストールして構成されている

例：地上波デジタルテレビのソフトウェアコンポーネント（富士ソフト）http://www.fsi.co.jp/dtv/dlna/img/FSDTV_DLNA.pdf



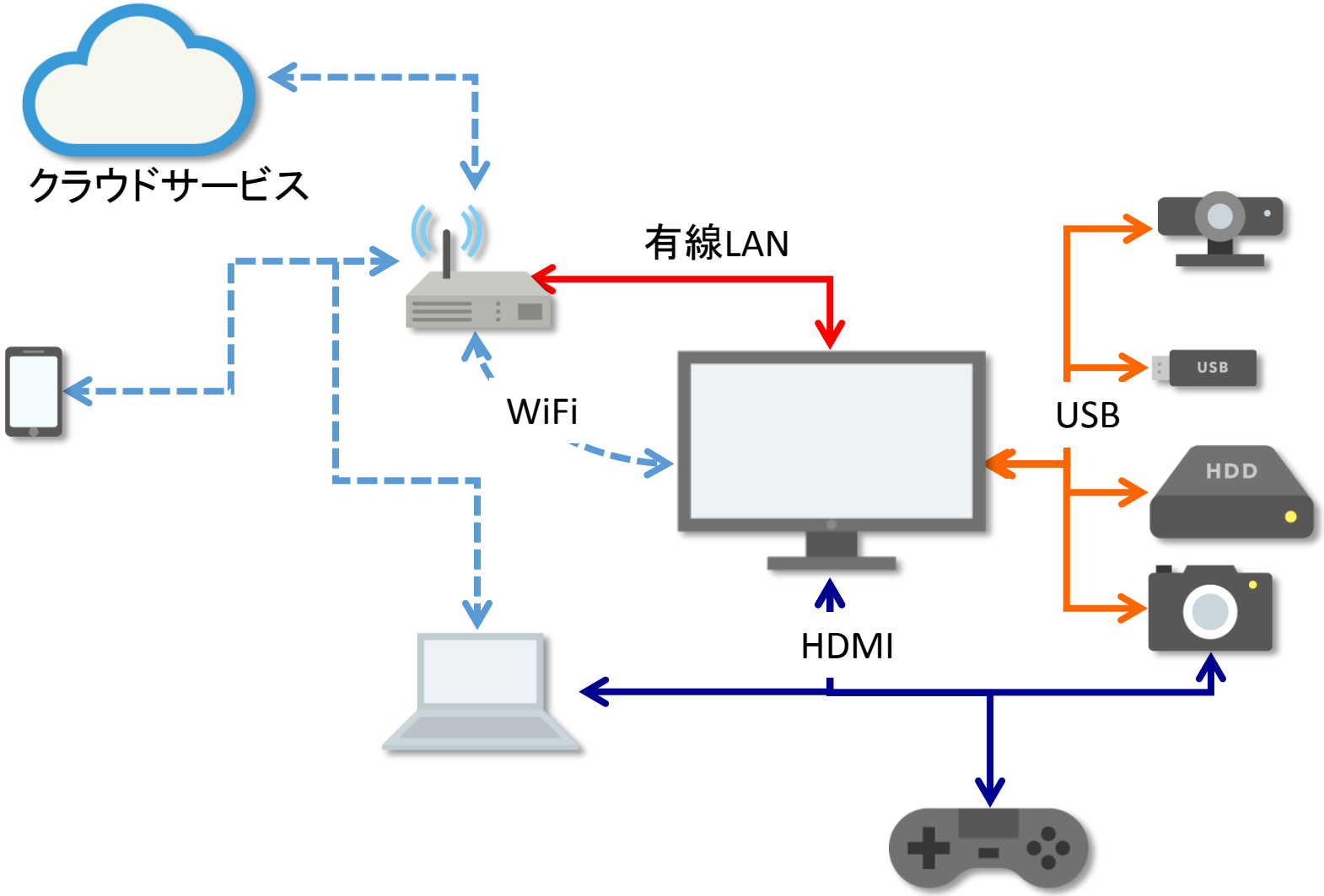
スマートテレビ：システム構成

例：ソニー BRAVIA X9300Cシリーズ

http://www.sony.jp/bravia/products/KJ-X9300C/

- Android TV（音声検索、Google Cast ：スマートフォンとの接続、Android TV アプリ：ゲームなど、TV Side View：スマートフォンをリモコンや番組予約などに）
- 有線LAN、無線LAN、Wi-Fi Direct
- ハイブリッドキャスト対応
- ブラウザ機能
- ホームネットワーク機能
- ブラビアリンク
- 外付けHDD録画

スマートテレビ：システム構成



想定される脅威：スマートテレビ

表 1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策の為の機能およびサービス				
脅威	• 説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoTデバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	• パスワードを変更しないと利用開始できない • アプリケーションなどが最新の状態であることの確認と、更新作業 • ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 • テスト（試行）モードでの通信の確認	• ネットワークカメラの接続先と自機の証明書の更新 • 定期的なパスワードの更新を要求、更新しないと利用できなくなる	• サポートセンターとの連絡方法を表示させる	• 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	• 設定の初期化（SkypeやYouTubeなどのアカウントからデバイスを削除なども含む） • 廃棄時は物理的に読み出し不可にする • 連携先に廃棄を連絡、廃棄通知は電話連絡先シールを添付
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフト ウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• パスワードを変更しないと利用開始できない • 製造元の信頼性の確認 • 接続可能な外部記憶装置（DLNA）の指定時に可能であればウィルススキャン • スマートテレビをつなげようとしているネットワークが感染していないか確認	• 定期的なウィルスチェック • 製造元からの脆弱性情報のチェックとアプリケーションなどが最新の状態であることの確認と、更新作業	• 不定期のウィルスチェック • 製造元からの脆弱性情報のチェックとアプリケーションなどが最新の状態であることの確認と、更新作業 • サポートセンターとの連絡方法を表示させる	• 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる • 一定期間、ウィルススキャンを行っていない場合利用できなくなる	• 設定の初期化（SkypeやYouTubeなどのアカウントからデバイスを削除なども含む） • 廃棄時は物理的に読み出し不可にする • 連携先に廃棄を連絡、廃棄通知は電話連絡先シールを添付

想定される脅威：スマートテレビ

表 2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• N/A	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• N/A
破壊	• IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 • IoTデバイスが潰される、あるいは燃やされるなどにより使用できなくなる、等	• N/A	• 破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する	• 破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する	• 破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する	• N/A
盗聴	• IoTデバイス内部やIoTデバイス同士の通信や、IoTデバイスと周辺システムとの通信を権利を有しない第三者に盗み見られる脅威 • センサーノードなどから得られた気温や湿度、放射線量などの情報が途中経路で盗聴される、等	• 通信の暗号化でコンテンツを保護 • 相互認証方法の確認 • Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する		• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 記録保存するコンテンツや聴取・録画予約記録などを暗号化する • 通信の暗号化 • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする

想定される脅威：スマートテレビ

表3：情報漏洩、不正利用

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
情報漏えい	• IoTシステムにおいて保護すべき情報が、許可のされていない者に入手される脅威 • 蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	• アプリケーションなどが最新の状態であることの確認と、更新作業 • ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 • 相互認証方法の確認 • Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	• 記録保存するコンテンツや聴取・録画予約記録などを暗号化する • 通信の暗号化 • アプリケーションなどが最新の状態であることの確認と、更新作業	• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 記録保存するコンテンツや聴取・録画予約記録などを暗号化する • 通信の暗号化 • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる • 動作監視（モニタリング）使用状の記録と監視をメーカーのサービスとして提供	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする
不正利用	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの機能などを利用される脅威 • 認証用の通信をなりすます事により、サービスを不正に利用する、等	• アプリケーションなどが最新の状態であることの確認と、更新作業 • ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 • 相互認証方法の確認 • Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	• 認証情報の定期的な変更と変更時に専用のモードで行う（ペアリング、二段階認証など） • 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） • デバイスそのものの偽者などはベンダー側のデバイスID管理などで実現	• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 認証情報の定期的な変更と変更時に専用のモードで行う（ペアリング、二段階認証など） • 動作監視（モニタリング）使用状の記録と監視をメーカーのサービスとして提供	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする

想定される脅威：スマートテレビ

表4：不正設定、不正中継、DoS攻撃

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正設定	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの設定値を不正に変更される脅威 • ネットワーク設定を変更し、正常な通信ができないようにする等	• ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 • 相互認証方法の確認 • Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	• 動作・使用状態のログ取得と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 動作監視（モニタリング）使用状態の記録と監視をメーカーのサービスとして提供 • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする
不正中継	• 通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 • NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等、近接通信であるから安全とした前提を利用するもの	• N/A	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 動作監視（モニタリング）使用状の記録と監視をメーカーのサービスとして提供 • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする
DoS 攻撃	• 不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威 • IoTデバイスやサービスゲートウェイに過剰な通信を実施し、利用者の要求（エアコンの遠隔制御など）をできなくさせる、等	• N/A	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 動作監視（モニタリング）使用状の記録と監視をメーカーのサービスとして提供 • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	• N/A

想定される脅威：スマートテレビ

表5：偽メッセージ、ログ喪失（証跡）

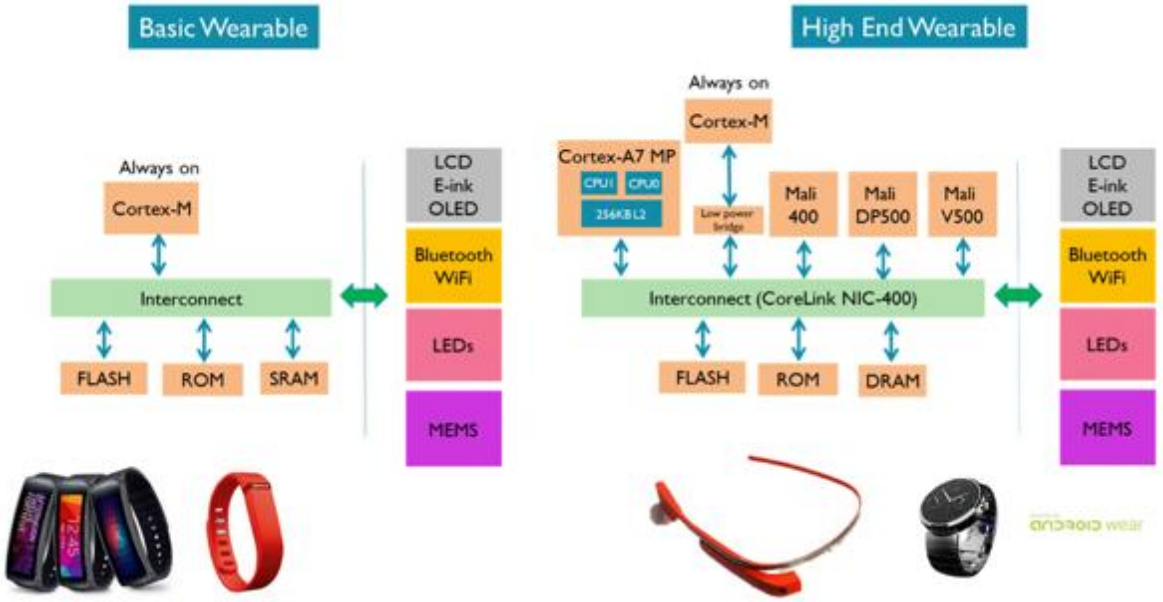
攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
偽メッセージ	• 攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 • エアコンの遠隔操作のメッセージを改ざんし、設定温度を高くする、等	• 相互認証方法の確認 • Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） • 異常発生を検知し、ユーザーに通知し、利用できなくなる	• 通信の暗号化 • 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） • 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる •	• N/A
ログ喪失（証跡）	• 操作履歴等を消去または改ざんし、後から確認できなくする脅威 • 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	• 物理的に読み出し不可にする • 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする

ウェアラブルデバイス：システム構成

ウェアラブルデバイスについて

- 「身につける（着る）コンピュータ（デバイス）」を指し、腕時計やリストバンド、指輪、メガネ、衣服など、以前から我々が身に着けていたモノの形態を踏襲し、より自然にコンピュータを利用できるようにするためのインタフェースとして誕生したものである。ハードウェアにより近いベーシックな構成の場合ではシンプルなRTOSによる動作するものから、Android OSにより動作するハイエンドレベルの構成まで多種多様な実装形式があるのも特徴である
- 近年はリストバンド形式のものにセンサを組み込むことによってライフログをとり、健康管理に役立てるような機器（Activity Monitor）への関心が強い

ARM technology driving the wearable trend
https://community.arm.com/groups/embedded/blog/2014/4/29/arm-technology-driving-the-wearable-trend



ウェアラブルデバイス：システム構成

ウェアラブルデバイスの装着部位と主な用途および製品

- **オムニチャネル時代にウェアラブル端末普及のきっかけとなるコア技術とは**
  http://o2o.abeja.asia/product/post-2064/
  図1：ウェアラブルデバイスの装着部位まとめ より

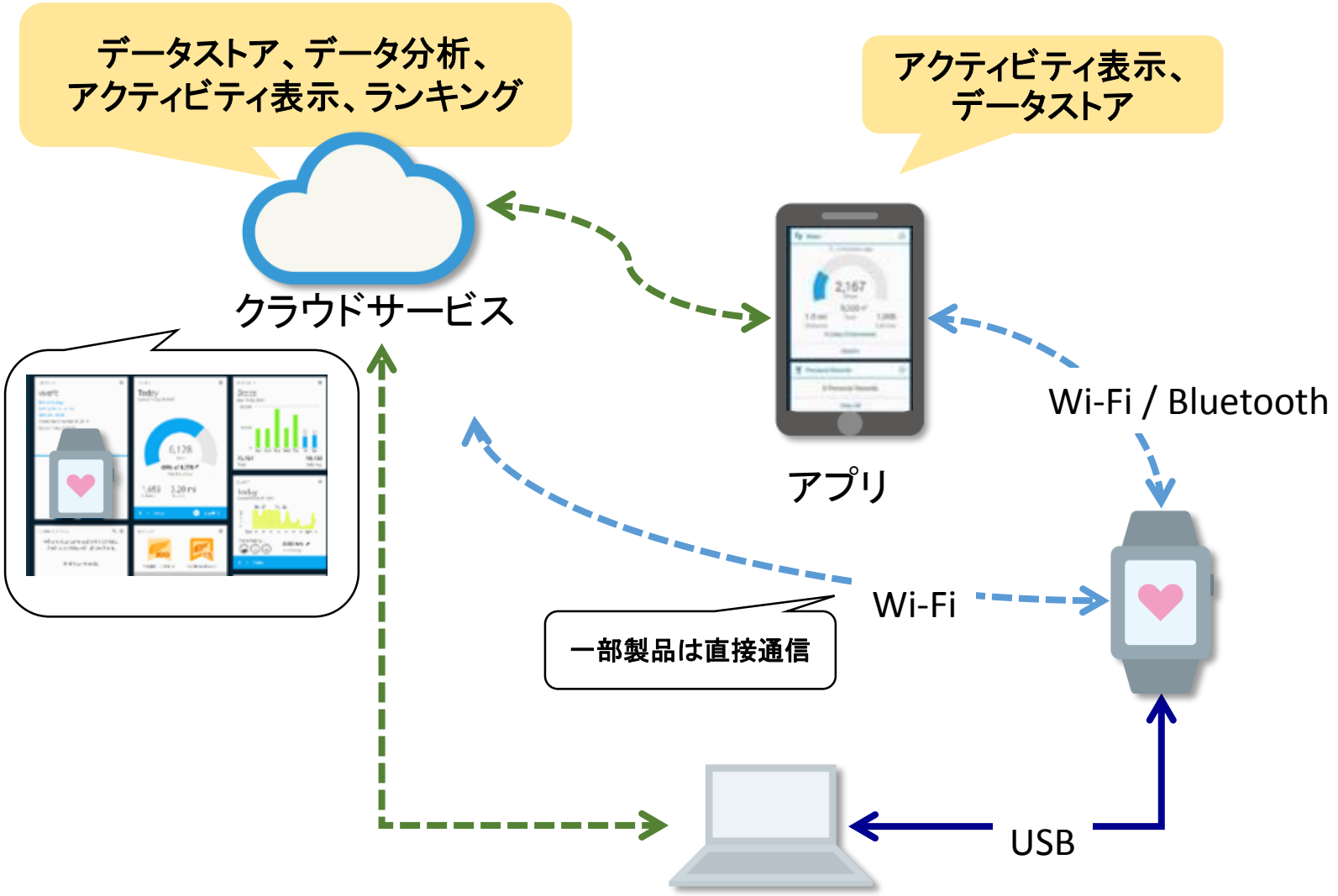
例：Fitbit/surge

https://www.fitbit.com/jp/surge#specs

GPS追跡	距離、ペース、登った高度を表示し、ルートとスプリットタイムを確認
PurePulse™ 心拍計	継続的、自動的に、リストベースの心拍数と単純化された心拍数ゾーンを把握
通知＋ミュージックコントロール	着信およびメッセージ通知をタッチスクリーンに表示
毎日のアクティビティ	歩数、距離、消費カロリー、登った階数、アクティブな時間を記録
自動睡眠監視＋アラーム	睡眠を監視し、バイブ目覚ましで起床
マルチスポーツ	ランニング、クロストレーニング、有酸素ワークアウトを記録し、ワークアウトサマリーを表示
ワイヤレス同期	主要スマートフォンやコンピューターでワイヤレスかつ自動的にデータを同期

【センサーおよびコンポーネント】
GPS、3 軸加速度計、3 軸ジャイロスコープ、デジタルコンパス、光学心拍数モニター、高度計、環境光センサー、バイブレーションモーター、ディスプレイ、タッチスクリーン、モノクロ LCD、バックライト搭載（暗所対応）

ウェアラブルデバイス：システム構成



想定される脅威：ウェアラブルデバイス

表1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoTデバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	• ペアリング先や通信先の確認ができるようにする • ペアリング先で必要な連携アプリケーションのアクセス権限の確認ができるようにする • インターネットへの接続はデフォルトでOFFにする	• ペアリング先や通信先の確認ができるようにする • 通信連携に必要なアクセス権限の確認ができるようにする • 連携アプリケーションのアクセス権限の確認ができるようにする • アクセス制御ができるようにする	• 確認ダイアログを表示する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• ペアリング状態や通信状態の確認ができるようにする • インストールされているアプリケーションの確認ができるようにする • 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • スマホやPC内の連携アプリケーションや設定の初期化ができるようにする • 連携先クラウドサービスからのデータ削除ができるようにする
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフトウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• インストールされるソフトウエアの確認ができるようにする	• 定期的なペアリング先や通信状態の確認ができるようにする • ファイアーウォール等でアクセス制御ができるようにする	• デバイスが完全に停止することができるようにする • 記録したデータを削除することができるようにする	• 製造元からの脆弱性情報のチェックができるようにする • 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • 母艦内の連携アプリケーションや設定の初期化ができるようにする • 連携先クラウドサービスからのデータ削除ができるようにする

想定される脅威：ウェアラブルデバイス

表2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• 利用者情報の登録（ペアリング先、利用するネットワークなどの情報）に対して耐タンパ性を持たせる	• デバイスがネットワーク（ペアリング含む）から切断されたことを検知し、ユーザーに通知することができるようにする • GPSなどを利用してデバイスの位置を把握することができるようにする • リモートワイプできるようにする	• N/A	• デバイスがネットワーク（ペアリング含む）から切断されたことを検知し、ユーザーに通知することができるようにする • GPSなどを利用してデバイスの位置を把握することができるようにする • リモートワイプできるようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする
破壊	• IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 • IoTデバイスが潰される、あるいは燃やされるなどにより使用できなくなる、等	• N/A	• 破壊されることで デバイスがネットワーク（ペアリング含む）から切断されたことを検知し、ユーザーに通知することができるようにする	• N/A	• 破壊されることでデバイスがネットワーク（ペアリング含む）から切断されたことを検知し、ユーザーに通知することができるようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする
盗聴	• IoTデバイス内部やIoTデバイス同士の通信や、IoTデバイスと周辺システムとの通信を権利を有しない第三者に盗み見られる脅威 • センサーノードなどから得られた気温や湿度、放射線量などの情報が途中経路で盗聴される、等	• ペアリング先、通信先や通信経路が確認できるようにする • 通信の暗号化ができるようにする • 相互認証ができるようにする	• ペアリング先や通信状態、動作の監視（モニタリング）ができるようにする • 設定変更されていないことが確認できるようにする • 通信の暗号化ができるようにする • 構成変更時に通知するようにする	• N/A	• ペアリング先や通信状態、動作の監視（モニタリング）ができるようにする • 設定変更されていないことが確認できるようにする • 通信の暗号化ができるようにする • 構成変更時に通知するようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする

想定される脅威：ウェアラブルデバイス

表3：情報漏洩、不正利用

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
情報漏えい	• IoT システムにおいて保護すべき情報が、許可のされていない者に入手される脅威 • 蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	• デバイス上のデータへのアクセス制御設定ができるようにする • 脆弱性チェックを実施（ベンダー保証）する • 通信の暗号化ができるようにする	• 動作監視（モニタリング）ができるようにする • 使用状況が分かるようにする • 設定変更時の通知ができるようにする • 認証情報の定期的な変更ができるようにする • 通信の暗号化ができるようにする	• N/A	• 動作監視（モニタリング）ができるようにする • 使用状況が分かるようにする • 設定変更時の通知ができるようにする • 認証情報の定期的な変更ができるようにする • 通信の暗号化ができるようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする
不正利用	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの機能などを利用される脅威 • 認証用の通信をなりすます事により、サービスを不正に利用する、等	• デバイス側とスマフォ側の両方で認証機能を使えるようにする • 認証情報がデフォルトから変更できるようにする • 認証情報に有効期限を設ける • 脆弱性チェックを実施している（ベンダー保証） • 無防備な外部IFを実装しないようにする	• 認証情報の定期的な変更ができるようにする • 変更時には専用のモードで行うようにする（ペアリングのような） • 動作監視（モニタリング）や使用状況の報告ができるようにする • ベンダー側のデバイスID管理などにより偽のデバイスかどうかを判定する仕組みを用意しておく • （デバイスそのものの偽者などはベンダー側のデバイスID管理などで検知する）	• 問題発生時の問い合わせ先が分かるようにする • 完全停止できるようにする • 完全停止がわかるようにする	• 認証情報の定期的な変更ができるようにする • 変更時には専用のモードで行うようにする（ペアリングのような） • 動作監視（モニタリング）や使用状況の報告ができるようにする • ベンダー側のデバイスID管理などにより偽のデバイスかどうかを判定する仕組みを用意しておく（デバイスそのものの偽者などはベンダー側のデバイスID管理などで検知する）	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする

想定される脅威：ウェアラブルデバイス
表4：不正設定、不正中継

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正設定	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの設定値を不正に変更される脅威 • ネットワーク設定を変更し、正常な通信ができないようにする、等	• デバイス側とスマフォ側の両方で認証機能を使えるようにする • 認証情報がデフォルトから変更できるようにする • 認証情報に有効期限を設ける • 脆弱性チェックを実施している（ベンダー保証） • 無防備な外部IFを実装しないようにする	• 動作監視（モニタリング）ができるようにする • 使用状況が分かるようにする • 設定変更時の通知ができるようにする • 認証情報の定期的な変更ができるようにする • 通信の暗号化ができるようにする	• 設定に問題があることがわかるようにする • 設定のロールバックができるようにする • 問題発生時の問い合わせ先が分かるようにする	• 動作監視（モニタリング）ができるようにする • 使用状況の報告ができるようにする • 設定変更時の通知ができるようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする
不正中継	• 通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 • NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等 • 近接通信であるから安全とした前提を利用するもの	• 読み取り防止機能が使えるようにする • 使わないときにOFFにすることができる（追加操作をつける、単に近くにいてONにはならないなど）	• 動作監視（モニタリング）として、次のことができるようにする • 設定変更されていないことが確認できるようにする • ペアリング先や通信先への不正な通信の検知ができるようにする • ペアリング先や通信先の通信相手が正しいことを常にモニターできるようにする • 通信遅延の検知（ベンダー側）をする	• 完全停止できるようにする • 完全停止がわかるようにする	• 動作監視（モニタリング）ができるようにする • 設定変更されていないことが確認できるようにする • 通信遅延の検知（ベンダー側）をする	• 廃棄時は物理的に読み出し不可にする • SDカードなどのローカルの記憶媒体は取り出すようにガイドする

想定される脅威：ウェアラブルデバイス

表5：DoS攻撃、偽メッセージ、ログ喪失（証跡）

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
DoS 攻撃	• 不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威 • IoTデバイスやサービスゲートウェイに過剰な通信を実施し、利用者の要求（エアコンの遠隔制御など）をできなくさせる、等	• セッションタイムアウトの設定ができるようにする • 通信機能以外は予備リソースで動作できるようにする • DoSを受けても、基本機能は動く仕様とする	• コマンド受付間隔を調整して、過剰な接続要求が来ても受け付けないようにする	• 再起動による即時回復ができるようにする • サービス不能期間のデータのバッファリングと再送ができるようにする • データが来なくてもダウンしない機能を実装する	• N/A	• N/A
偽メッセージ	• 攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 • エアコンの遠隔操作のメッセージを改ざんし、設定温度を高くする、等	• メッセージの認証ができるようにする • ペアリング先や通信先の確認ができるようにする • 認証方式そのものの安全性確認が取られている • メッセージ内容の承認ができるようにする • 相互認証ができるようにする	• 動作監視（モニタリング）ができるようにする • 設定変更されていないことが確認できるようにする • ペアリング先や通信先への不正な通信の検知ができるようにする • 通信相手と相互認証ができるようにする	• 完全停止できるようにする • 完全停止がわかるようにする • 問題発生時の問い合わせ先分かるようにする	• 動作監視（モニタリング）ができるようにする • 設定変更されていないことの確認ができるようにする • ペアリング先や通信先への不正な通信の検知ができるようにする • 通信相手と相互認証ができるようにする	• N/A
ログ喪失（証跡）	• 操作履歴等を消去または改ざんし、後から確認できなくする脅威 • 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	• 管理者権限とユーザ権限を分離する	• アクセスログの取得が出来るようにする • 定期通知が出来るようにする	• 設定に問題があることがわかるようにする • 設定のロールバックが出来るようにする • 問題発生時の問い合わせ先が分かるようにする	• N/A	• N/A

ネットワークカメラ

ネットワークカメラについて

- ネットワークカメラとは、カメラが捉える映像をインターネットなどネットワークで携帯端末・パソコン・スマートフォン経由で視聴できる機能を提供する
- Webカメラとの違いとしては、カメラ自体がIPアドレスを持ち単独で機能することである

（WebカメラはUSB経由でパソコンと接続しない限り機能しない）

- 代表的なIoT機器の一つと言える
- 過去にセキュリティの不備が問題になったことがあるため、実装は進んでいるが、適切に使用されているとは言い切れない
- 最近の商品については、設定変更権限のある管理者と、画像視聴のみができる一般ユーザーの権限分離や、インターネット経由でのカメラ画像へのアクセスを制御機能が実装されている。マニュアルにはデフォルトパスワードの変更操作方法が記載されていることが多い

  参考) http://www.itmedia.co.jp/pcuser/articles/1408/27/news051.html

- 価格帯　6000円台～

  アクシス
  パナソニック
  SONY
  CANON
  VIVOTEK
  JVC
  コロナ産業　他

ネットワークカメラ：システム構成

- OS　専用ファームウエアと記載されているが実際はLinuxであることが多い
- 有線LAN、無線LAN、Wi-Fi Direct
- 音声対応機能（マイク・スピーカー）
- 動作検知センサー
- 録画機能　（SD、外付けHDD、NAS）
- 録画視聴機能

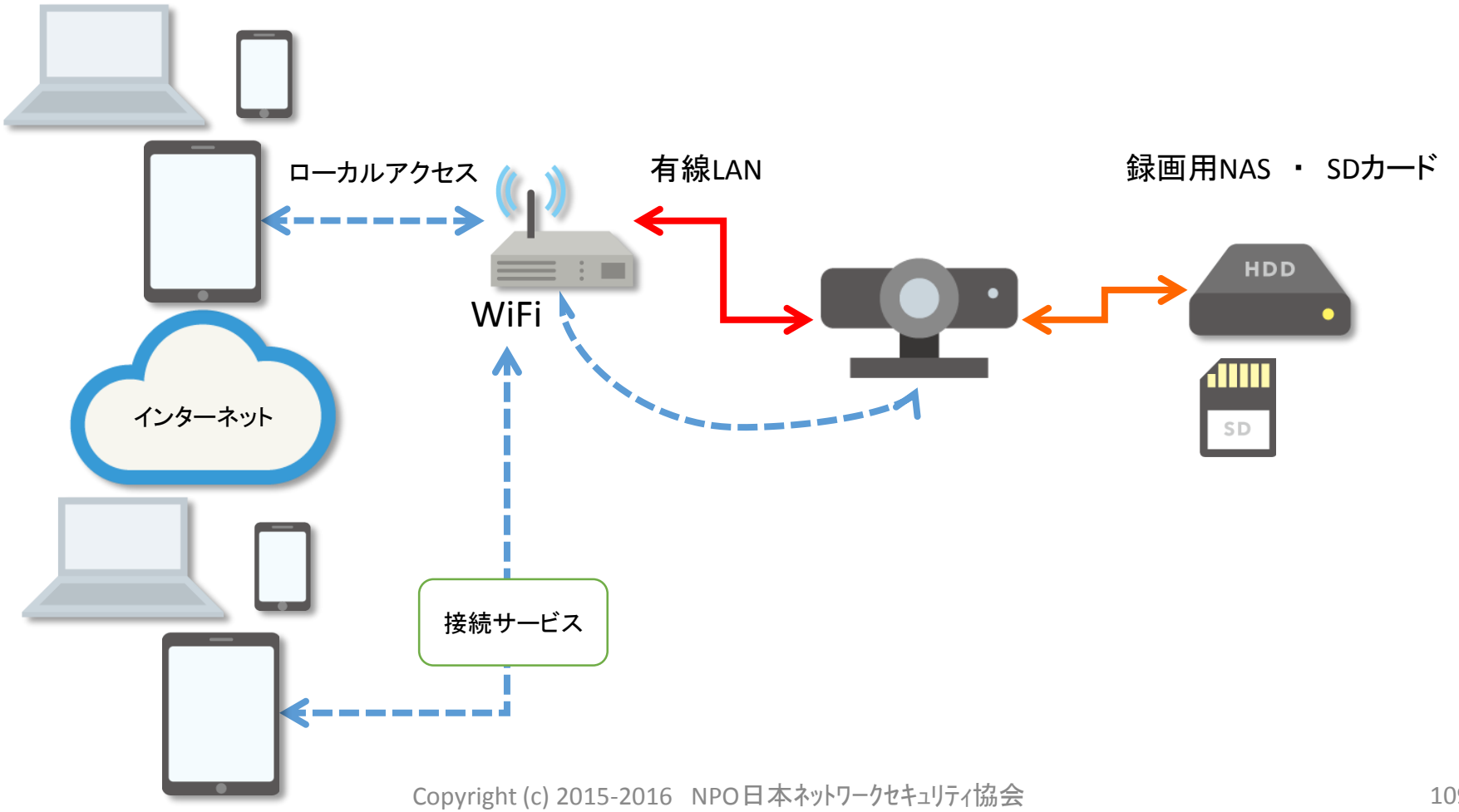
  （ブラウザーでAcitveXを動かす、専用のサイト経由で見る、スマホアプリを使う）

参考）

- 機能パン（首振り機能）有無、画像品質、暗視機能有無、　LAN給電
  などの差がある

ネットワークカメラ：システム構成

PC・タブレット・スマートフォン



想定される脅威：ネットワークカメラ

表1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoT デバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	• カメラへのアクセス時のユーザー認証機能を有効にする • 工場出荷時の認証情報を全製品共通にしない（MACアドレスなど） • インターネットへの公開はデフォルトOFFにする • 映像を転送する場合は転送先設定が正しいことを確認できるようにする • 転送先でデータへのアクセス制御機能があることを確認できる	• 定期的な認証情報の更新がきる • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など）	• 通信先などの異常を自動検知してメール等で通知する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • 映像転送先サーバーからのデータ削除ができるようにする
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフト ウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoT デバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• インストールされるソフトウエアの確認ができるようにする	• ファイアーウォールによるアクセス制御ができるようにする • 転送先の定期的な確認ができるようにする • 製造元から脆弱性情報を配信する	• デバイスが完全に停止することができるようにする • 記録したデータを削除することができるようにする	• 認証情報に有効期限を設ける	• 同上

想定される脅威：ネットワークカメラ

表2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoT デバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoT デバイスを誰かが持ち去る、等	• 解析されることで不正利用されないように耐タンパ性を持たせる • 利用者情報の登録ができる	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知できるようにする あるいは映像から盗難を検知する	• N/A	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知するできるようにする	• 廃棄時は物理的に読み出し不可にする • SDカードなどローカルの記憶媒体は取り出すようにガイドする
破壊	• IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 • IoTデバイスが潰される、あるいは燃やされるなどにより使用できなくなる、等	• N/A	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。 あるいは映像から破壊を検知する	• N/A	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。	• 同上
盗聴	• IoTデバイス内部やIoTデバイス同士の通信や、IoTデバイスと周辺システムとの通信を権利を有しない第三者に盗み見られる脅威 • センサーノードなどから得られた気温や湿度、放射線量などの情報が途中経路で盗聴される、等	• 通信経路の確認ができるようにする • カメラ側Webサーバーへアクセスするなどのデバイスの認証や制限	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など）	• N/A	• 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など）	• 同上

想定される脅威：ネットワークカメラ

表3：情報漏洩、不正利用

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置・野良状態	買い替え・廃棄時
情報漏えい	• IoT システムにおいて保護すべき情報が、許可のされていない者に入手される脅威 • 蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	• カメラ側Webサーバーへのアクセス制御設定ができ（ユーザー認証・権限分離） • 脆弱性チェックを実施する（ベンダー） • 通信が暗号化できるようにする	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知な不正な通信の遮断・検知（Firewallなど） • 通信相手が正しいことを常にモニターできる	• N/A	• 動作監視（モニタリング）機能 不正な通信の遮断・検知（Firewallなど） • 通信相手が正しいことを常にモニターできる	• 廃棄時は物理的に読み出し不可にする • SDカードなどローカルの記憶媒体は取り出すようにガイドする
不正利用	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に IoT システムの機能などを利用される脅威 • 認証用の通信をなりすます事により、サービスを不正に利用する、等	• ユーザー認証機能を有効にする • カメラ側Webサーバーへのアクセス制御設定ができ（ユーザー認証・権限分離）になっている • 認証情報の有効期限を設ける • 無防備な外部IFを設けない • 脆弱性チェックを実施する（ベンダー）	• 認証情報の定期的な変更ができるようにする • 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など） • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	• 問題発生時の問い合わせ先を明示する • デバイスが完全停止できるようにする • 完全停止がわかるようにする	• 認証情報の定期的な変更ができるようにする • 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	• 同上

想定される脅威：ネットワークカメラ

表4：不正設定、不正中継、DoS 攻撃

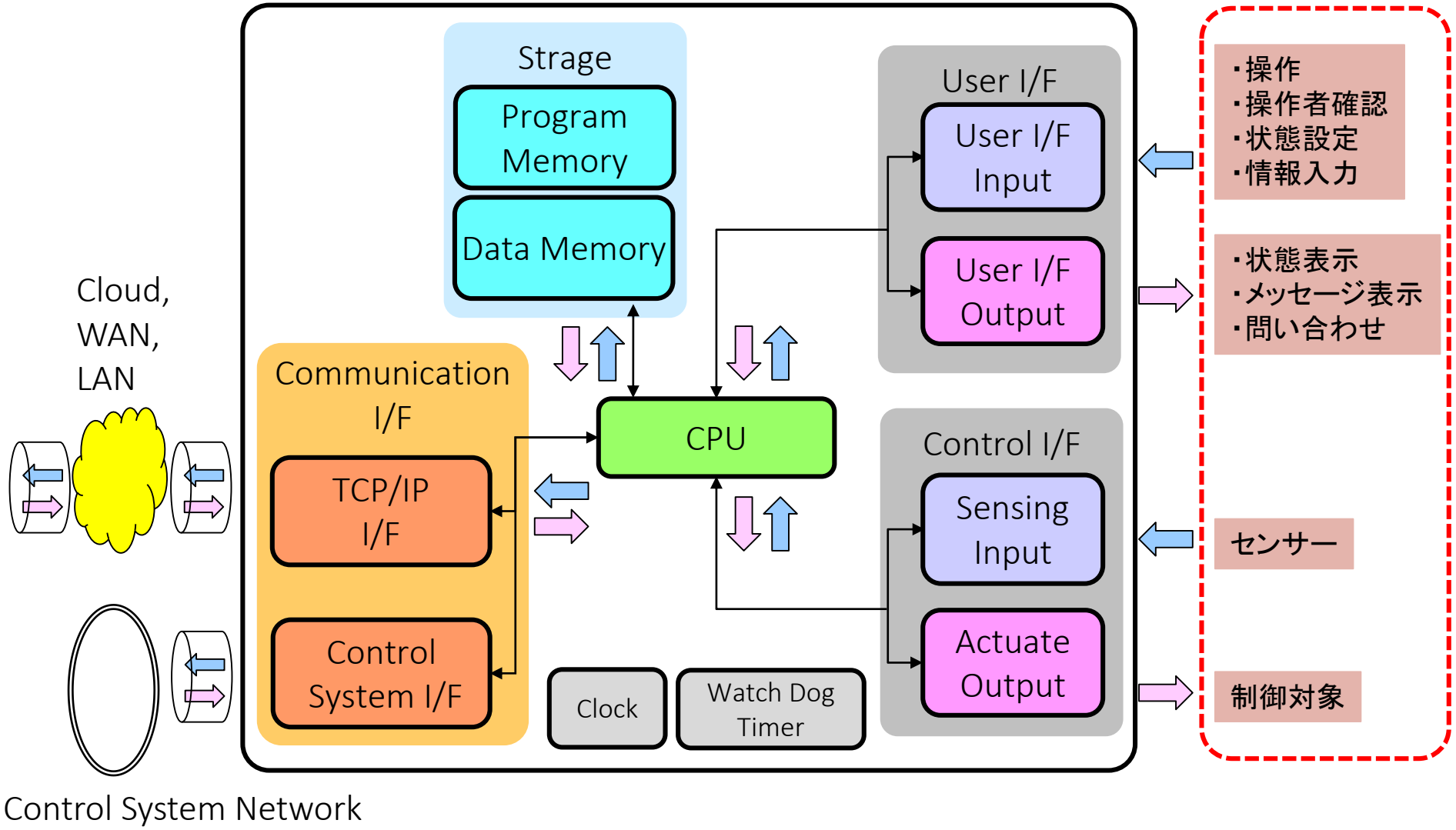
攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正設定	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの設定値を不正に変更される脅威 • ネットワーク設定を変更し、正常な通信ができないようにする、等	• ユーザー認証機能を有効にする • カメラ側Webサーバーへのアクセス制御設定ができる（ユーザー認証・権限分離） • 認証情報の有効期限を設ける • 無防備な外部IFを設けない	• 認証情報の定期的な変更ができるようにする • 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく • 管理者と一般ユーザーを分けて運用し管理者の認証情報管理をより厳格にできるようにする	• 通信先などの異常を自動検知してメール等で通知する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	• 廃棄時は物理的に読み出し不可にする • SDカードなどローカルの記憶媒体は取り出すようにガイドする
不正中継	• 通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 • NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等 • 近接通信であるから安全とした前提を利用するもの	• N/A	• N/A	• N/A	• N/A	• N/A
DoS 攻撃	• 不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威 • IoTデバイスやサービスゲートウェイに過剰な通信を実施し、利用者の要求（エアコンの遠隔制御など）をできなくさせる、等	• セッションタイムアウトの設定ができるようにする • DoSを受けた場合、画像はローカルに保管する	• コマンド受付間隔を調整して、過剰な接続要求が来ても受け付けないようにする	• 再起動による即時回復ができる	• N/A	• N/A

想定される脅威：ネットワークカメラ

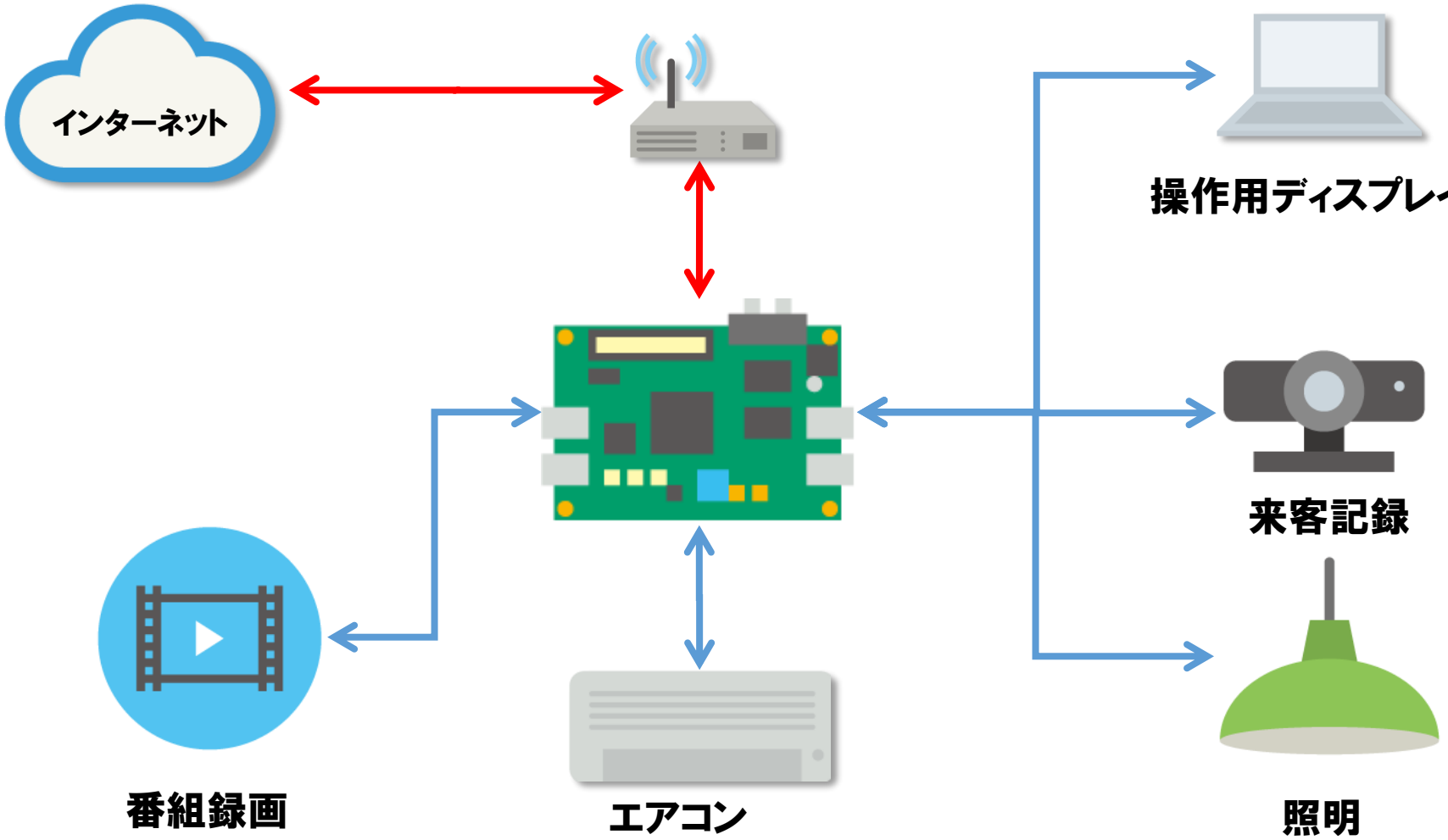
表5：偽メッセージ、ログ喪失（証跡）

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
偽メッセージ	• 攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 • エアコンの遠隔操作のメッセージを改ざんし、設定温度を高くする、等	• 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離する • カメラ側Webサーバーへアクセスするなどのデバイスの認証やアクセス制限を行うことができる	• カメラ側Webサーバーへアクセスするなどのデバイスの認証やアクセス制限を行うことができる • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	• 完全停止できる・完全停止がわかるようにする • 問題発生時の問い合わせ先を明示する	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • ベンダー側のデバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく • 通信の暗号化ができる	• N/A
ログ喪失（証跡）	• 操作履歴等を消去または改ざんし、後から確認できなくする脅威 • 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	• 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離す（画像の編集権限の分離）	• アクセスログの取得と定期通知ができる	• 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• N/A	• N/A

汎用マイコンボード：システム構成



汎用マイコンボード：システム構成



想定される脅威：汎用マイコンボード

表1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoT デバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	• ID、パスワード、通信先などデフォルト設定の確認・変更機能を実装する • 通信の暗号化機能はデフォルトONにする（特にroot権限やコマンド、レスポンスのやりとり） • テスト（試行）による動作確認を実装する	• 定期的な認証情報の更新がきる • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ログの取得による不正動作の検知ができるようにする	• 通信先などの異常を自動検知してメール等で通知する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• 動作監視（モニタリング） - ランプ - 遠隔通知 • 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • 廃棄時は物理的に読み出し不可にするようガイドする • ラベルや注意書き等、システムの構成や制御内容、取扱うデータ、管理者などが類推可能となるおそれのある情報を削除するようガイドする • 連携先に廃棄を連絡するガイドまたは機能を実装する
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフト ウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• ボード購入元の信頼性を確認する（ウィルスが仕込まれていないか） • ネットワークなど安全な環境下で設定を行うようガイドする • 実際のシステムに接続する前にセキュリティの設定が行われるようにする • ・最新のセキュリティパッチを適用されるようにする	• ・定期的なウィルスチェックができるようにする ・製造元からの脆弱性情報を配信する • ・ログの取得による不正動作の検知ができるようにする	• 動作状況のわかりやすい表示 • 安全なシーケンスで再起動を実行するようにする • 安全な停止、入出力やネットワークの切り離しができるようにする	• 定期的なウィルスチェックができるようにする	

想定される脅威：汎用マイコンボード

表2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• ユースケースに応じた損害の算定をする	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知できるようにする • 盗難を検地した場合には起動しないよう実装する	• ・盗難を検出した倍には自ら機能を停止する • ・重要なデータはあらかじめ適当なタイミングでバックアップをとれるようにする	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知するできるようにする	• N/A
破壊	• IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 • IoTデバイスが潰される、あるいは燃やされるなどにより使用できなくなる、等	• ユースケースに応じた損害の算定をする	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。	• ・重要なデータはあらかじめ適当なタイミングでバックアップをとる	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。	• N/A
盗聴	• IoTデバイス内部やIoTデバイス同士の通信や、IoTデバイスと周辺システムとの通信を権利を有しない第三者に盗み見られる脅威 • センサーノードなどから得られた気温や湿度、放射線量などの情報が途中経路で盗聴される、等	• 通信経路の確認ができるようにする • 通信の暗号化ができるようにする • 相互認証機能を利用する • Firewallや、侵入検知機能のあるネットワークの利用をガイドする	• 動動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • 定期的な暗号化鍵の変更を可能にする	• N/A	• 動動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など） • 定期的な暗号化鍵の変更を可能にする	• 耐タンパ性を持つ製品を使用する

想定される脅威：汎用マイコンボード

表3：情報漏洩、不正利用

攻撃者による干渉に起因する脅威		対策				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
情報漏えい	• IoT システムにおいて保護すべき情報が、許可のされていない者に入手される脅威 • 蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	• アクセス制御設定ができ（ユーザー認証・権限分離）設定 • 脆弱性チェックの実施 • 脆弱性チェック済みデバイスの使用 • 通信が暗号化できるようにする • 重要なシステムはFirewallや、侵入検知機能のあるネットワークを利用する	• ・動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • 通信の暗号化ができるようにする • 不正な通信の遮断・検（Firewallなど） • 通信相手が正しいことを常にモニターできる • ・ログが取得できるようにする（正常ログ、異常ログ）	• N/A	• 動作監視（モニタリング）機能がある • 通信の暗号化ができるようにする • 不正な通信の遮断・検知（Firewallなど） • 通信相手が正しいことを常にモニターできる	• 耐タンパ性を持つ製品を使用する
不正利用	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの機能などを利用される脅威 • 認証用の通信をなりすます事により、サービスを不正に利用する、等	• 認証情報をデフォルト値から変更する ・脆弱性チェックの実施 • ・脆弱性チェック済みデバイスの使用	• 認証情報の定期的な変更 • 変更時には安全なモードで行う（ペアリングのような） • 動作監視（モニタリング） • デバイスの認証（デバイスID管理などの偽物対策） • ログを取得できるようにする（正常ログ、異常ログ）	• 不正利用を検出した場合に動作を停止させる	• 認証情報の定期的な変更ができるようにする • 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • デバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	

想定される脅威：汎用マイコンボード

表4：不正設定、不正中継、DoS 攻撃

攻撃者による干渉に起因する脅威		対策				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正設定	• ・なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの設定値を不正に変更される脅威 • ネットワーク設定を変更し、正常な通信ができないようにする等	• 認証機能を有効にする（IoT側とサーバー側の両方） • 認証情報をデフォルト値から変更する • 脆弱性チェックの実施 • 脆弱性チェック済みデバイスの使用 • ・	• 認証情報の定期的な変更 • 変更時には安全なモードで行う（ペアリングのような） • 動作監視（モニタリング） • デバイスの認証（デバイスID管理などの偽物対策） • ログを取得できるようにする（正常ログ、異常ログ）	• 不正設定を検出した場合に動作を停止させる	• 動動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある （構成情報更新時にメール通知など） • 不正な通信の遮断・検知（Firewallなど） • 通信相手が正しいことを常にモニターできる	• 耐タンパ性を持つ製品を使用する
不正中継	• 通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 • NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等 • 近接通信であるから安全とした前提を利用するもの	• 読み取り防止機能の追加 • 使わないときにはOFFとなる機能を設ける（単に近くにいるだけでONにはしない機能）	• ・動作監視（モニタリング） ・設定変更されていないことの確認 • 通信遅延の検知（ベンダー側） • ログの取得（正常ログ、異常ログ）	• 完全停止する • 停止したことがシステム側で判断出来る	• 動作監視（モニタリング） • 設定変更時の通知機能 • 不正な通信／アクセスの検知（※どこまで出来る？） • 通信相手が正しいことのモニタできる	
DoS 攻撃	• 不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威 • IoTデバイスやサービスゲートウェイに過剰な通信を実施し、利用者の要求（エアコンの遠隔制御など）をできなくさせる、等	• コネクションフラッド、SYNフラッド、UDPフラッドに耐えるシステム構造 • セッションタイムアウトの設定 • DoSを受けI/F部分が麻痺しても基本機能は動く構造	• ログの取得（正常ログ、異常ログ）	• DoS攻撃が終わったら速やかに機能回復できる • 再起動による回復 • サービス不能期間のデータのバッファリングと再送機能 • データが来なくてもダウンしない機能がある	• N/A	• N/A

想定される脅威：汎用マイコンボード

表5：偽メッセージ、ログ喪失（証跡）

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
偽メッセージ	• 攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 • エアコンの遠隔操作のメッセージを改ざんし、設定温度を高くする、等	• 認証機能の利用（IoT側とサーバー側の両方） • 認証情報をデフォルト値から変更できる • 脆弱性チェックの実施 • 脆弱性チェック済みデバイスの使用 • データの安全な暗号化機能がある • 安全な暗号を用いたプロトコルの利用 • メッセージ値の正常範囲の確認　（例：エアコンの温度が常識的な範囲） • 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離する	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • ログの取得（正常ログ、異常ログ）	• 偽メッセージを検出した場合に動作を停止させる	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） •	• N/A
ログ喪失（証跡）	• 操作履歴等が消去または改ざんされ、後から確認できなくなる脅威 • 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	• ログ情報の保護 • バックアップ機能を持つ（安全な場所） • 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離する	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • ログファイルへのアクセスの検知、記録 • ログの取得（正常ログ、異常ログ）	• バックアップから復帰可能な機能	• 動作監視（モニタリング）機能がある • ログファイルへのアクセスの検知、記録	• 耐タンパ性を持たせる

4. ベンダーが、ユーザーの IoT の利用に際して考慮すべきこと

ユーザー（利用者）は IoT の仕組みや構造について詳細を理解していなくてもベンダー（提供者）が提供する情報から個々の IoT 製品やサービスについて安全に利用できる必要がある。この章では、サイバーセキュリティの観点からユーザーに対してベンダーが配慮すべき項目を解説する。

4. ベンダーがユーザーの IoT の利用に際して考慮すべきこと

4章の概要

- 4章では3章で提示したベンダー向けのガイドと視点を変え、ベンダーや開発者が専門知識のないユーザーに対して安全な仕組みを提示できるようにすることを目的とする
- ベンダーはIoTデバイスの企画・開発、販売に際して、IoTデバイスおよびデバイスで利用するインターネット上のサービスに対し、サイバーセキュリティ対策を施し、ユーザーが行なう必要のある操作や作業を特定して適切なガイドを行なう必要がある
- ユーザーに適切なセキュリティ機能を提示することは、ベンダーのインシデント対応コストを下げることにもつながる

● 要諦は以下の三点

1. デフォルト設定をセキュアに！
2. 問題発生を想定する
3. 廃棄まで責任を持つ

デフォルト設定をセキュアに！

- **デフォルトの設定はセキュリティの高い方を採用する**

  ユーザーが設定変更を正しく実施できるスキルを持つとは限らない

  設定変更ができない場合でも一定のセキュリティが保たれるようにする

  （例）インターネットからのアクセスを不可の設定にして出荷

  共通ID・共通パスワードは使わず、デバイス個々に設定する

  Well－Knownポートはひとまず閉じておく

- **デフォルト設定を変更せざるを得ない手順を作る**

  デフォルト設定をセキュアにすると動作に支障が出て、不良品と勘違いするエンドユーザーが多くなりそうな場合の次善の策

  面倒だからと、マニュアルにあっても自主的な設定変更をしないユーザー対策

  （例）初期設定画面で、デフォルトパスワードを変更しないと次のステップに進めなくする

  管理者がログインするとパスワードの変更を強制される

  初回起動時に設定変更チェックを走らせ、メッセージを出す

問題発生を想定する

- **インシデント発生時の受付窓口を設ける**
  おかしいと思っても連絡する先がないと被害は拡大する
- **問題発生を検知する手段を考える**
  ユーザーが気づくきっかけを作る
  （例）重要な構成変更が行われたらメールで通知
  何かソフトウエアがインストールされたらPopUp表示
- **非常停止機能を作る**
  簡単な操作で被害を止める手段が必要
  （例）リセット・データワイプボタン
  無線通信停止ボタン

廃棄まで責任を持つ

- **デバイスが放置される可能性を考える**
  安価なIoTは、紛失・盗難・放置される可能性がある
  そのまま稼動を続けると、プライバシー侵害・BOTの温床になる
  例）
  有効期限を持つパラメータを仕込み、必ず停止させる
  ベンダーからのリモートワイプ

IoT Security WG Report 2015

●レポート執筆メンバー(社名五十音順)

WGリーダー:松岡 正人 (株式会社カスペルスキー)

WGメンバー:玉木　誠 (SCSK株式会社)
阿部 真吾 (JPCERTコーディネーションセンター)
洞田 慎一 (JPCERTコーディネーションセンター)
酒井 美香 (日本IBMシステムズ・エンジニアリング株式会社)
杉浦　昌 (日本電気株式会社)
福田 尚弘 (パナソニック株式会社)

兜森 清忠 (オブザーバ)
桐山 隼人 (オブザーバ)

IoTセキュリティワーキンググループメンバー

名前	会社名	名前	会社名	名前	会社名
松岡　正人 *リーダー	（株）カスペルスキー	阿部　真吾	JPCERTコーディネーションセンター	三池　聖史	ユニアデックス（株）
武田　洋介	（株）アイピーキューブ	洞田　慎一	JPCERTコーディネーションセンター	荒川　一之	ユニアデックス（株）
中原　歌織	アドソル日進（株）	細田　将	セコム株式会社	東海林　昌幸	（株）ラック
高木　昌彦	（株）アピリッツ	鈴木　和之	綜合警備保障（株）	山下　勇太	（株）ラック
作本　直樹	アライドテレシス（株）	藤川　真樹	綜合警備保障（株）	川上　昌俊	（株）ラック
和田　弘之	アライドテレシス（株）	相原　弘明	（株）ソリトンシステムズ	篠原　崇宏	（株）ラック
二木　真明	アルテア・セキュリティ・コンサルティング	半田　富己男	大日本印刷（株）	鈴木　翔	（株）ラック
手塚　信之	SCSK（株）	中村　亮大	大日本印刷（株）	又江原　泰彦	（株）ラック
境　　稔	SCSK（株）	林　　憲明	トレンドマイクロ（株）	鵜山　通夫	サブスクライバ
玉木　誠	SCSK（株）	酒井　美香	日本IBMシステムズ・エンジニアリング（株）	古城　隆	サブスクライバ
亀田　勇歩	SCSK（株）	杉浦　昌	日本電気（株）	兜森　清忠	オブザーバ
小川　朝也	NTTソフトウェア（株）	島　　成佳	日本電気（株）	桐山　隼人	オブザーバ
戸田　勝之	NTTデータ先端技術（株）	関　　徳男	日本電気（株）		
近藤　伸明	（株）神戸デジタル・ラボ	長坂　啓司	日本プロセス（株）		
松本　悦宜	（株）神戸デジタル・ラボ	瀬田　晃彦	日本ユニシス（株）		
久保　智夫	（株）サーバーワークス	福田　尚弘	パナソニック（株）		
高橋　大成	（株）サーバーワークス	堀部　千壽	パナソニック（株）		
有村　浩一	JPCERTコーディネーションセンター	武田　一城	（株）日立ソリューションズ		
満永　拓邦	JPCERTコーディネーションセンター	尾崎　誠	ユニアデックス（株）		

注意事項

*本レポート中で引用している写真・図版や各種情報などの引用元と著作権はそれぞれの引用元を参照のこと
*本レポートを引用する際には日本ネットワークセキュリティ協会に事前に通知をすること

＜お問い合せ＞
*本報告書に関する引用・内容についてのご質問等は JNSA ウェブサイト上の引用連絡およびお問合せフォームからご連絡下さい。
*引用のご連絡に対する承諾通知は、ご返信しておりませんのでご了承下さい。
*また報告書についての FAQ もございますので、引用・お問合せの際はご参照下さい。
http://www.jnsa.org/faq/incident.html

■お問い合わせフォーム
引用連絡および問合せフォーム
URL： https://www.jnsa.org/aboutus/quote.html