

一般財団法人
草の根サイバーセキュリティ運動全国連絡会(Grafsec-J)
第二回全国大会 講演資料

「IoTって何？」

～マイナンバー、IoT時代に向けたサイバー
セキュリティと情報モラル～

2016年2月16日

日本スマートフォンセキュリティ協会(JSSEC)
利用部会 部会長 後藤 悦夫(株式会社 ラック)
(本日の内容はJSSECメンバーとしての個人的な考え方です)

自己紹介



後藤 悦夫

- 一般社団法人 日本スマートフォンセキュリティ協会
利用部会 部会長
- 株式会社 ラック
サイバー・グリッド・ジャパン
サイバークリッド研究所 客員研究員
etsuo.goto@lac.co.jp

<経歴>

～2015/3 トヨタ自動車株式会社 情報部門
・情報セキュリティのポリシーやルールの
策定、働き方変革の推進などを担当

- ・2011年よりスマートフォンのルール
(JSSECの利用ガイドラインWGに参加)
- ・2014年よりモバイルワークのルール

ワークライフバランスとりながら

2015/4～ 株式会社 ラックの客員研究員
・JSSEC活動やIoTの調査・研究を担当



名古屋グリーンテニスクラブ

一般社団法人 日本スマートフォンセキュリティ協会

会員:132社 + 25法人(特別会員、オブザーバー)

<2015年7月現在>

スマートフォンの**安全な利活用を図り普及を促進する**ために、2011年5月に任意団体としてスタートし、2012年4月より一般社団法人として活動

利用部会

利用者の視点
で活動

技術部会

提供者の視点
で活動

啓発事業部会

ジュニア層への
啓発活動

PR部会

JSSECの
PR活動

主な成果物

利用部会:スマートフォン&タブレットの業務利用に関するセキュリティガイドライン

技術部会:Androidアプリのセキュア設計・セキュアコーディングガイド

◆ <http://www.jssec.org/> ⇒ 部会・WGからの報告 / 成果物からダウンロード可能

利用部会
部会長：後藤 悦夫

利用ガイドラインWG
・企業向けのガイドライン

事例研究WG
・各社利用事例調査

IoT調査・研究TF
新規活動開始



**「スマートフォン&タブレットの
業務利用に関する
セキュリティガイドライン」**

- ・2015/7 調査研究スタート
- ・利用分野
- ・利用形態
- ・脅威や課題
- 企業セキュリティへの影響など、今後の活動の方向を議論

https://www.jssec.org/dl/guidelines_v2.pdf

はじめに

■啓発活動の大切さと難しさ

- ・製造業で最も重要な啓発活動は「安全作業」
- ・サイバー空間は目に見えないため、伝えるのが難しい

	現場における安全作業	サイバー安全の課題
知らない	何が危険か知らない！ → 具体的な危険事例を教える	<ul style="list-style-type: none">・サイバーは見えない、分かり難い・使われ方が人それぞれ・危険が変化（攻撃者の悪意に左右）
出来ない	安全な作業が出来ない！ → 安全な作業手順を訓練する	<ul style="list-style-type: none">・安全な使い方（手順）が定義出来ない・使われ方が人それぞれ・危険が変化（攻撃者の悪意に左右）
やらない	安全な作業手順を知っていても、やらない！ → しつけ、手順の改善	<ul style="list-style-type: none">・しつけにも限界・安全な使い方（手順）が定義出来ない・個人の意識に依存

本日の概要

- 2020年のオリンピックと一緒にやってくるIoT
 - ・世の中の動きは
 - ・なぜ今IoTなのか
- IoTってななに
 - ・IoTでなにが変わるのか
 - ・IoTの事例
- IoT時代のサイバーセキュリティとは
 - ・PCやスマートフォンと何が違うか
 - ・最近の事故事例
 - ・啓発活動にどう影響するのか

■ オリンピックと一緒にやってくるIoT

2012年に開催された**ロンドンオリンピック**

- 期間中に延べ2億件を上回るサイバー攻撃が行われた

2020年の**東京オリンピック**の際も、

- オリンピックへの直接的なもののみならず、社会インフラやあらゆる経済社会活動に向けた攻撃が行われる可能性・・・

出展: IPA(独立行政法人情報処理推進機構) <https://www.ipa.go.jp/about/press/20140117.html>



2012年 **ロンドンオリンピック**時の環境

- ・インターネット(Web)を使った情報システムが活躍していた
- ・iPhone4sなどスマートフォンが広まり始めた

2020年 **東京オリンピック**時の環境

- ・スマートフォン+インターネット(LTEやWiFiなど)が普及
- ・IoT(**Internet of Things**:あらゆるモノが繋がる)が普及

■ オリンピックと一緒にやってくるIoT



NISC
内閣官房：
内閣
サイバー
セキュリティ
センター

2015.9.4
**「サイバーセキュ
リティ戦略」**
が閣議決定

「サイバーセキュリティ2015(案)」の概要について

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上 及び持続的発展 ～ 費用から投資へ ～	国民が安全で安心して暮らせる 社会の実現 ～ 2020年・その後に向けた基盤形成 ～	国際社会の平和・安定及び 我が国の安全保障 ～ サイバー空間における積極的平和主義 ～
<p>■ 安全なIoTシステムの創出</p> <ul style="list-style-type: none"> ▶ IoTに係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】 ▶ M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】 ▶ エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【経済産業省】 <p>■ セキュリティマインドを持った企業経営の推進</p> <ul style="list-style-type: none"> ▶ サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】 ▶ 経営ガイドラインの策定【経済産業省】 ▶ 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】 ▶ ISACを活用した情報共有体制の拡充【総務省】 <p>■ セキュリティに係るビジネス環境の整備</p> <ul style="list-style-type: none"> ▶ 政府系ファンド等の活用検討【経済産業省】 ▶ 著作権法におけるリバースエンジニアリングに関する適法性を明確化【文科科学省】 ▶ 制御システムセキュリティ認証の拡大【経済産業省】 	<p>■ 国民・社会を守るための取組</p> <ul style="list-style-type: none"> ▶ マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】 ▶ 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】 ▶ 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】 <p>■ 重要インフラを守るための取組</p> <ul style="list-style-type: none"> ▶ オリンピック・パラリンピック東京大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】 ▶ マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】 <p>■ 政府機関を守るための取組</p> <ul style="list-style-type: none"> ▶ 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】 ▶ 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【内閣官房】 	<p>■ 我が国の安全の確保</p> <ul style="list-style-type: none"> ▶ 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】 ▶ カウンターインテリジェンスに係る取組の推進【内閣官房】 ▶ サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】 ▶ 部外インフラ等、関係主体との連携強化【防衛省】 <p>■ 国際社会の平和・安定</p> <ul style="list-style-type: none"> ▶ 二国間協議や多国間協議に参画し、国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映【内閣官房及び外務省】 ▶ 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】 ▶ 各国における能力構築を支援【内閣官房 他】 <p>■ 世界各国との協力連携</p> <ul style="list-style-type: none"> ▶ ASEAN諸国との連携を強化【内閣官房 他】 ▶ インターネットエコノミーに関する日米政策協力対話にて一致した、米国との情報共有を強化【総務省】 ▶ 包括的な日米サイバー防衛の連携【防衛省】
<p>横断的 施策</p> <p>■ 研究開発の推進</p> <ul style="list-style-type: none"> ▶ 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】 ▶ 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】 ▶ 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】 	<p>■ 人材の育成・確保</p> <ul style="list-style-type: none"> ▶ 高度なITの知識と経営などその他の領域における専門知識を併せもつ人材の育成【文科科学省及び経済産業省】 ▶ 初等中等教育に携わる教員等を対象とした研修、情報交換【文科科学省】 ▶ 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】 ▶ サイバー防衛演習を通じた実践的セキュリティ人材の育成【総務省】 	
<p>推進体制 ▶ 伊勢志摩サミットにおけるサイバーセキュリティの確保やオリンピック・パラリンピック東京大会に向けた対策の検討【内閣官房】</p>		

出展：
NISC(内閣官房内閣サイバーセキュリティセンター) <http://www.nisc.go.jp/active/kihon/pdf/cyber-security2015-gaiyo.pdf>



一般社団法人日本スマートフォンセキュリティ協会
-スマートフォンを安心して利用出来る社会へ-

■ オリンピックと一緒にやってくるIoT

■ 2020年までに起こる、だれも予期しなかった変革

ガートナーによると、2020年までに半数以上の主要な新規事業プロセスと新システムが、何らかの形でIoTに結び付くという。

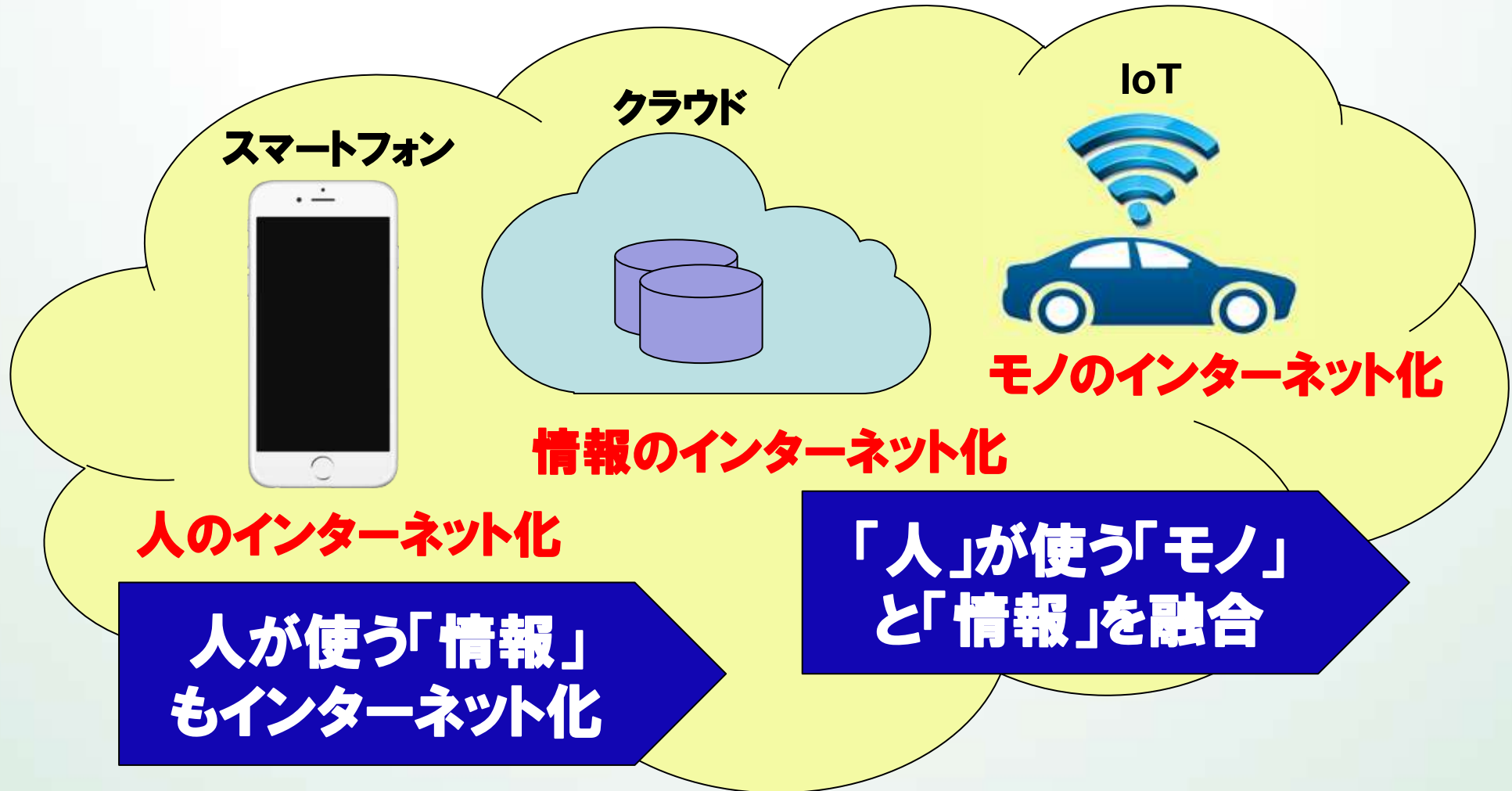
センサーの付いた物理的なモノがツールと化し、それらをデバイス、システム、人などにつなげるコストが減少するにつれ、消費者と企業に対するIoTの影響は急速に拡大していくと指摘する。



出典:ビジネス+ITプレミアム <<http://www.sbbit.jp/article/cont1/30647>>

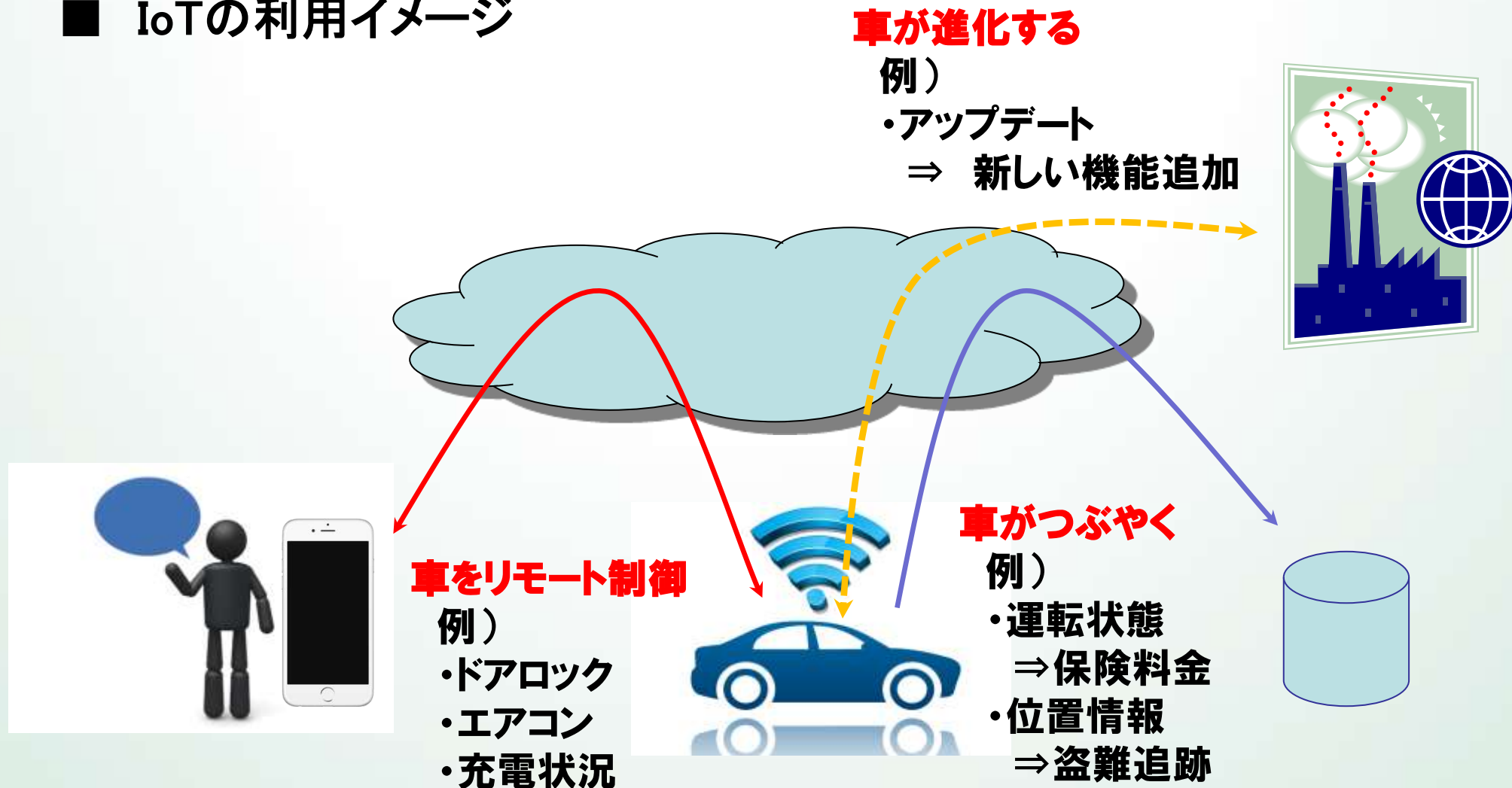
■ オリンピックと一緒にやってくるIoT

■ なぜ今IoTなのか(進化と深化の過程)



IoTってななに

IoTの利用イメージ



■IoTの事例

■ IoTごみ箱、東海大に登場

携帯電話網を利用し、ごみの蓄積状況をリアルタイムでモバイル端末などに発信する。

収集頻度や人員配置、ごみ箱配置の最適化——など、
収集作業の効率化によるコスト削減を見込む。



出典:ITmedia <<http://www.itmedia.co.jp/news/articles/1601/21/news140.html>>

IoTの事例

■ 家電リモコンやスピーカーフォンになる多機能照明

LEDシーリングライトにスピーカーやマイク、IR発光部、WiFi接続、人感センサや温度湿度センサを搭載して、スマートフォンアプリからエアコンやテレビの操作、音楽再生、スピーカーフォンとしての会話などができる製品です。

スピーカーのほかにマイク、IRリモコン、人感センサや温度湿度センサなどを組み合わせた多機能が特徴。

WiFi経由でネットワークにつながり、家でも出先でもリモコンアプリから操作できるため、音楽用のスピーカーとして使うほかにも、出先からテレビやエアコンを操作したり、照明を点けたり消したり、部屋に居る人と会話までができます。



出典: Engadget Japan <<http://japanese.engadget.com/2016/01/13/sony/>>

■IoTの事例

■ Google Nowが搭載されたスマート鏡

グーグルのソフトウェアエンジニアMax Braunさんが自作したこの鏡、Google Nowが搭載されたスマート鏡なのです。

Amazon Fire TV StickとAndroid APIを使って鏡に表示している情報は、時刻や天気予報、APニュースヘッドラインなど。まさに朝に欲しいちょっとした情報が、朝必ず目にする鏡に映し出されています。「スマート、スマート」、「IoT、IoT」って何でも言うけれど、今はまだこれくらいがちょうどいいの。



出典: GIZMODO <http://www.gizmodo.jp/2016/02/iotgoogle_now.html>

IoTの事例

トヨタが“ビッグデータセンター”新設

トヨタがIoT時代を見据え、クルマの「つながる」化を推進。車載通信機の搭載率を高め、仕様もグローバルで統一する。膨大なデータ処理やサービス展開に注力するため、ITインフラを強化し、専門機関を新設する。

2017年以降のモデル切り替えから、米国市場を皮切りに車載通信機(DCM:データコミュニケーションモジュール)の搭載率を高めるとしている。

現状では「レクサス」など高級車を中心に搭載されているが、これをより多くの車種へと展開していく。現在、国や地域ごとに異なる仕様を、2019年までにグローバルで共通化する予定だ。



出典:ITmedia <<http://www.itmedia.co.jp/enterprise/articles/1601/05/news124.html>>

■IoTの事例(使ってみました)

IoTテニスラケット(Babolat Play Pure Drive)

●ラケットを使う為に、充電と設定が必要

A screenshot of a smartphone's profile page titled 'プロフィール'. The page shows a profile picture placeholder and a registration form with the following fields:

性別	男性 ▼
名字	
名前	生年月日 必須 ×
生年月日	郵便番号 必須 ×
郵便番号	市区 必須 ×
市区	国 必須 ×
国	
利き手	右利き ▼
アカウントタイプ	プレーヤー ▼

IoTの事例(使ってみました)



**●見える化は
楽しい！
役立つかは？**



■ IoT時代のサイバーセキュリティとは

〈なになが起こるか〉

■ ネットを通じ制御される

- ・ 機密を守るから動作(制御)を守る
- ・ 守るものが情報から社会機能へ

◎ 提供者に求められる事 → Security by Design

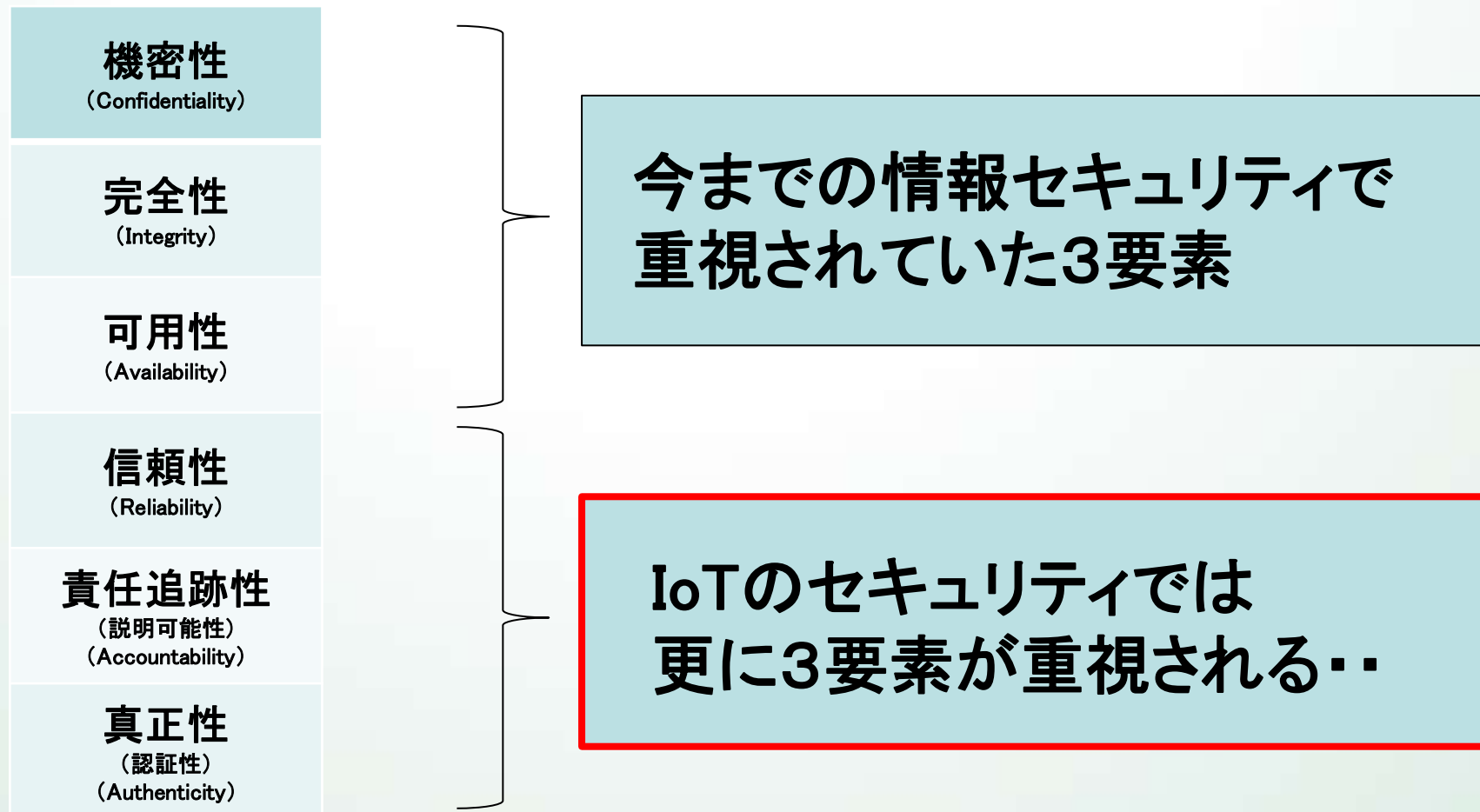
■ モノがつぶやく

- ・ 自分の情報(位置、身体など)が集められる

◎ 提供者に求められる事 → Privacy by Design

IoT時代のサイバーセキュリティとは

＜PCやスマートフォンのセキュリティと何が違うか＞



■ IoT時代のサイバーセキュリティとは

<最近の事件事例>

日本の監視カメラ、6000台もの映像が見られてる

問題となっているのはロシアのウェブサイト。

このサイトでは、街中や店内、自宅玄関など、世界120か国の監視カメラが撮影している映像を、リアルタイムで見れてしまいます。

日本国内の監視カメラもおよそ6000か所。デパートやコーヒーショップ、歯医者やホテルなど、顔がくっきり映っているものまであるそうです。これらの映像は、購入時のまま変更せず初期パスワードを使っているカメラの映像ということだそうです。



出典:iMedi <<http://imedi.jp/archives/22504>>

■ IoT時代のサイバーセキュリティとは

- 何に注意すればよいか(これからの検討課題)
 - ・なんでも、かんでもネットに繋がらない
 - ・信頼出来るブランドやモノを選ぶ
 - ・初期状態のまま使わない(特にパスワード)
 - ・使わなくなったら、ネットから切り離す

→ サイバーセキュリティの啓発活動にも影響

- オリンピックに向けたサイバーセキュリティ
 - ・安心・安全が最高のおもてなし
 - ・サイバーの安全が社会の安全の基本(IoT時代の治安)
 - ・いよいよ、リオ終了の2016年9月から本格的準備に

→ サイバーセキュリティのボランティア活動も重要

ご清聴ありがとうございました。

