野村総合研究所

資料WG3－5

IoT利活用を促進する取組動向

2016年03月08日

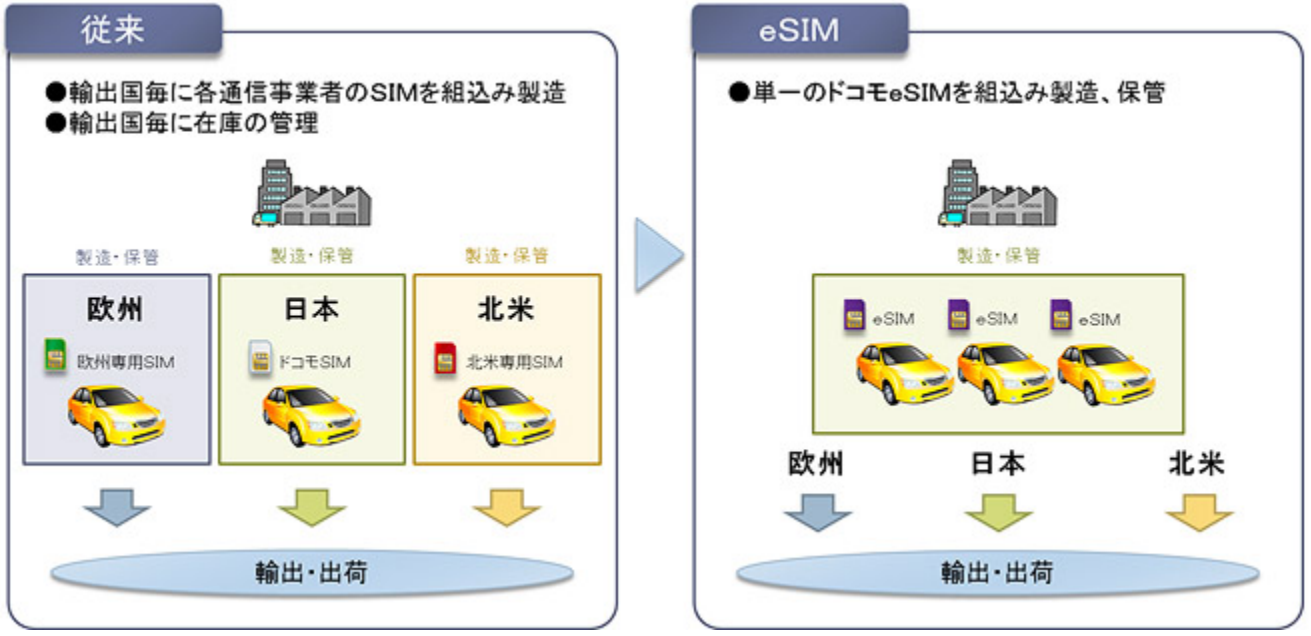
株式会社野村総合研究所
コンサルティング事業本部
ICT・メディア産業コンサルティング部

主席コンサルタント
桑津浩太郎

〒100-0005
東京都千代田区丸の内1-6-5 丸の内北口ビル

e-sim　SIMのソフト化によるグローバルオペレーションの円滑化

■IoT向けには、対象機器やネットワーク機器の海外展開に際して、現地オペレータSIMへの対応負担を軽減できる。



出所：NTTドコモ

■2016年頃に、本格提供の可能性が出ている。

●消費者向けは、出張時や海外旅行時に、現地の通信事業者との契約(=これまでのSIMの物理的な入れ替え)負担を軽減できる。

サービス開始、初期セッティング等の負荷を軽減できる。
全体システムとしての効率化、コストダウンが期待できる。

LPWA (Low Power Wide Area)
・低速、低コスト向けIoT代替網をめぐる動き。

■2.4GHz、900MHz等。多くの企業はアンライセンス帯域かつ広域エリアを想定。

■NB-LTE等との競合が予想される。

■Ingenu

- ●プライベートネットワークから、IoT向けパブリックネットワークへ転換。専用ASICのRandom Phase Multiple Accessを用いて、低コスト、大容量収容。
- ●主に技術提供。網構築はローカル事業者へ。
  オーストラリア、中国、フィリピン、南アフリカ、対等の18カ国で実績あり。
  顧客はキャリアではなく、バックホール事業者、タワープロバイダー、SI事業者等。

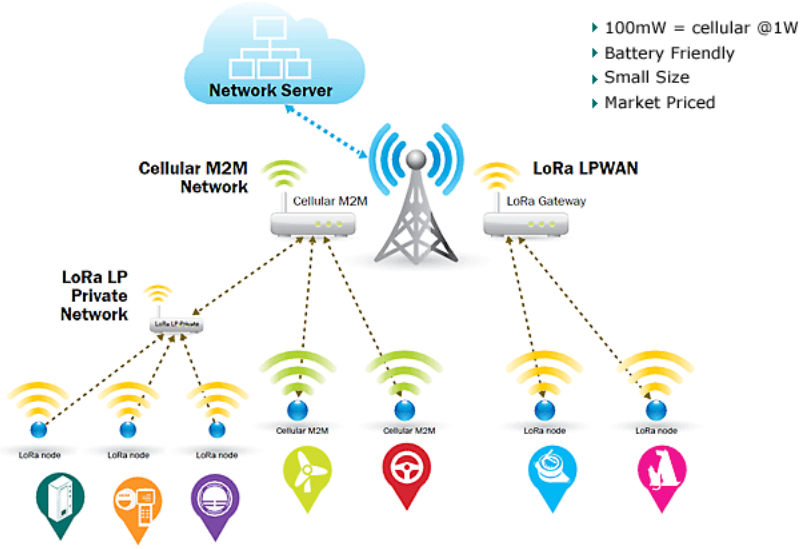
■LoRa Alliance

- ●230社相当の会員企業から構成。
- ●ドイツの電力・ガスエネルギー会社(E.ON)等が、ハンブルク、ベルリン、ニュルンベルクを筆頭に2016年には主要都市をカバーする計画。
- ●フランスのOrangeも採用意向。

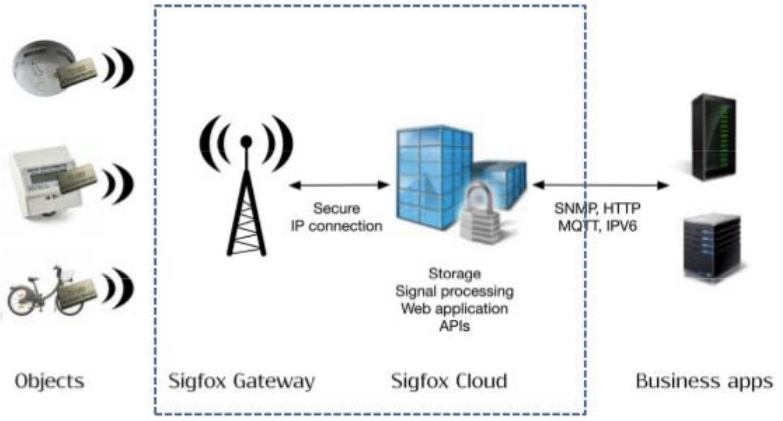
■Sigfox

- ●全米10都市でサービス開始。2016年中に50都市を計画。
  主要顧客としては、Groupe HBF(防犯、ホームオートメーション)
- ●フランス、ドイツ、スペイン等の14カ国でもサービス提供、もしくは2016年内に計画。

LoRa Alliance



Sigfox



IoTのセキュリティ問題の萌芽
・「IoTのアクセルを踏む前に、ブレーキがかかった・・・」

■自動車で改めて大問題へ。

●CANには、ハッキング対策が想定されていなかった?

速度表示
ガソリン残量表示をハッキング

ブレーキ作動、ハンドルロック等
をハッキング

かつてのPC、携帯電話の
ウィルス、不正侵入対策を
自動車にも一気に導入

車につづいて、室内（ホテル）、ペースメーカ等への侵入トライアルが成功。2010年以前の産業系ITは、内部伝送を暗号化しない等の外部侵入を想定していない事例が多数残る模様。

■HEMS

●ホテルの客室機器管理等に利用されているKNX netプロトコルの解析から、機器の遠隔操作の可能性が指摘された。

●エアコン、照明のオンオフ

■ペースメーカー

●不正遠隔操作のトライアル

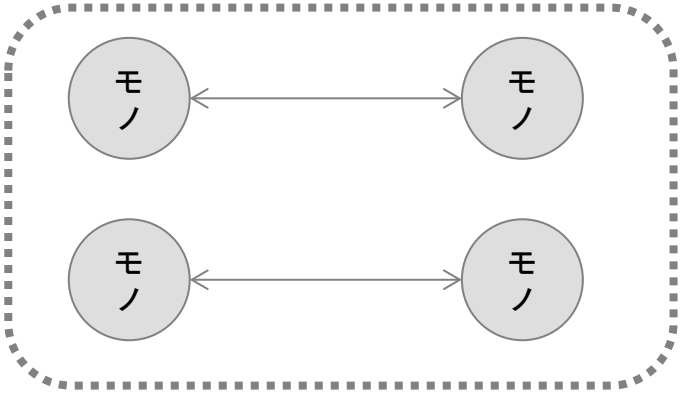
●専用装置と組み込み型ペースメーカ間の通信を解析し、電圧操作を行った。
特殊なコマンドを送ると、ペースメーカーが自身のモデルとシリアル番号を送り返すというプログラミングエラーから、ハッキングし、対象 とするデバイスのタイプを特定すれば、830ボルトの電圧を発生させることが出来た。

●

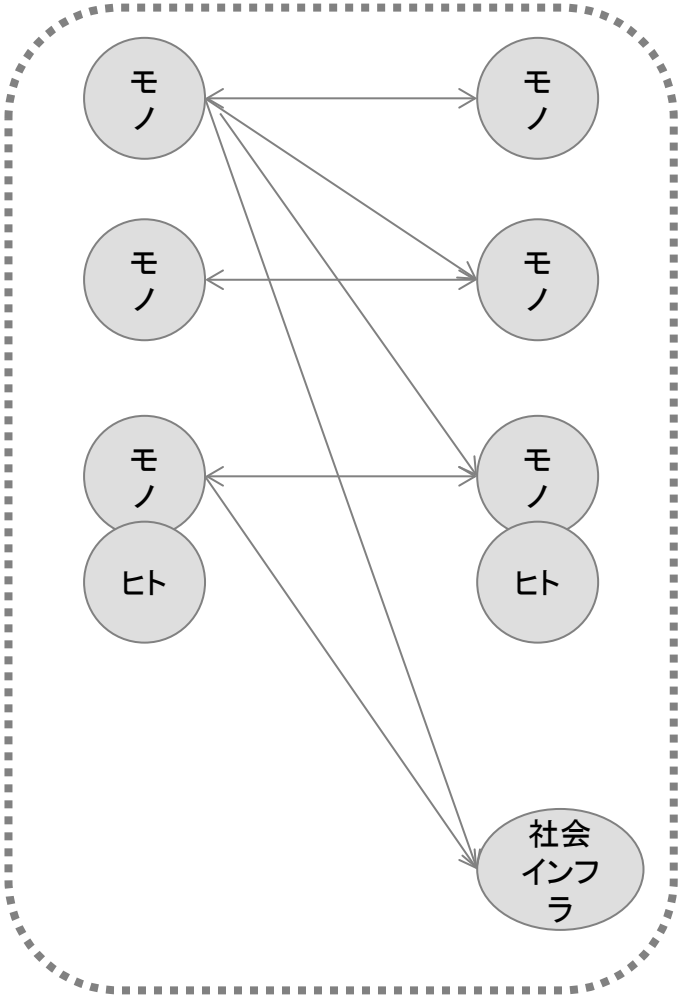
司様

IoTの市場特性とセキュリティ　　どこまで広がるのか？
・ヘルスケアは?ヒトもThings。IoEなのか?社会まるごとか?
・セキュリティの対象も、拡大しつつある。

従来のM2M、当初のIoT



これからのIoT



体重計はIoTなのか?少なくともM2Mじゃないのでは?
→ある意味、ヒトをモノと見なしてデータをとるものは、
IoTと呼んで良いのでは?

映像処理はIoTなのか?
→もう、映像はCCDセンサーということで、IoTに入れ
てしまえ! デジタルなんだから、映像も信号だ!

ヘルスケアのように
人も対象に

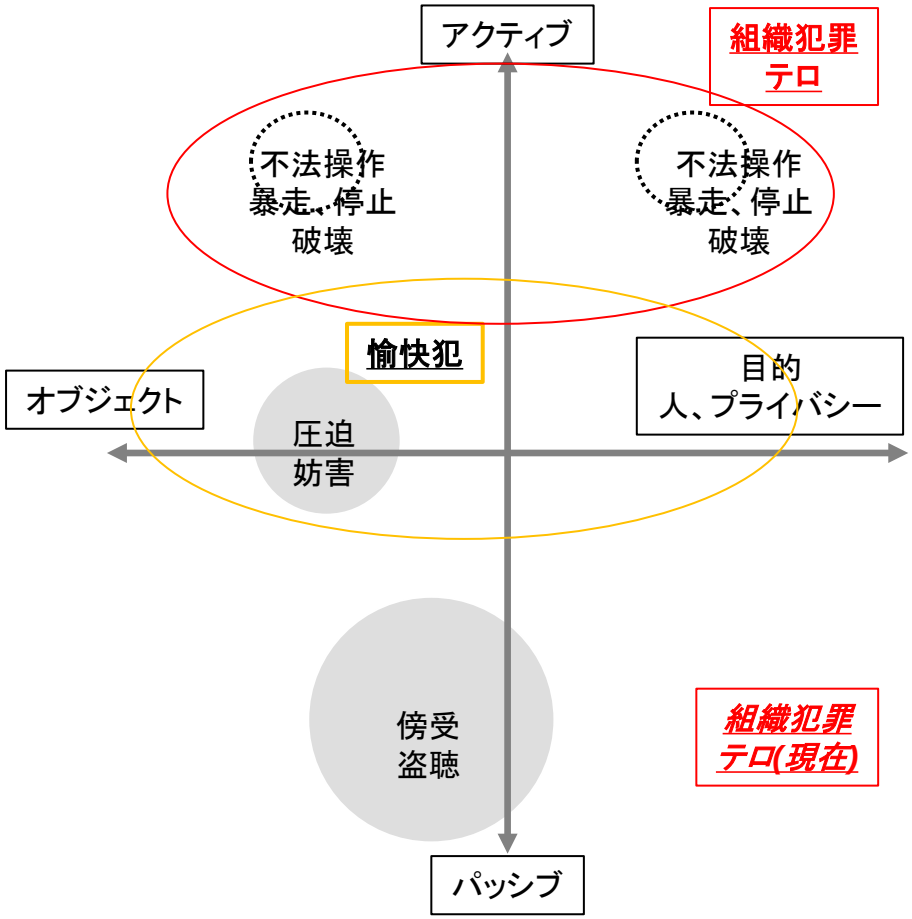
人の動き、流れ
人に関連したコト
(渋滞等)も対象に

出所：NRI

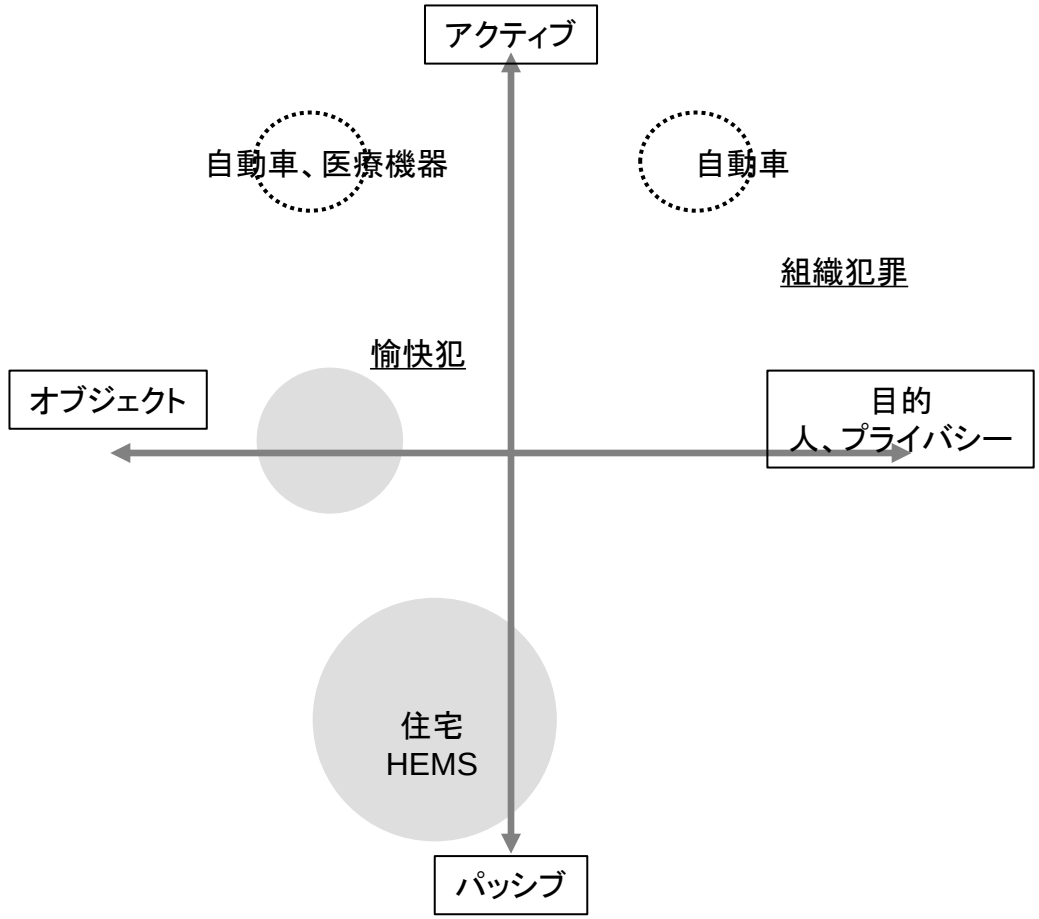
IoTのセキュリティ

・ネットと同様、パッシブから、圧迫・妨害（DDOS相当）、不法操作・破壊へ進展。
・機器そのものが目的となるケースと、人の利用状況・環境等を把握するケースの二種類。
・愉快犯と組織犯罪・テロ等も、想定される。

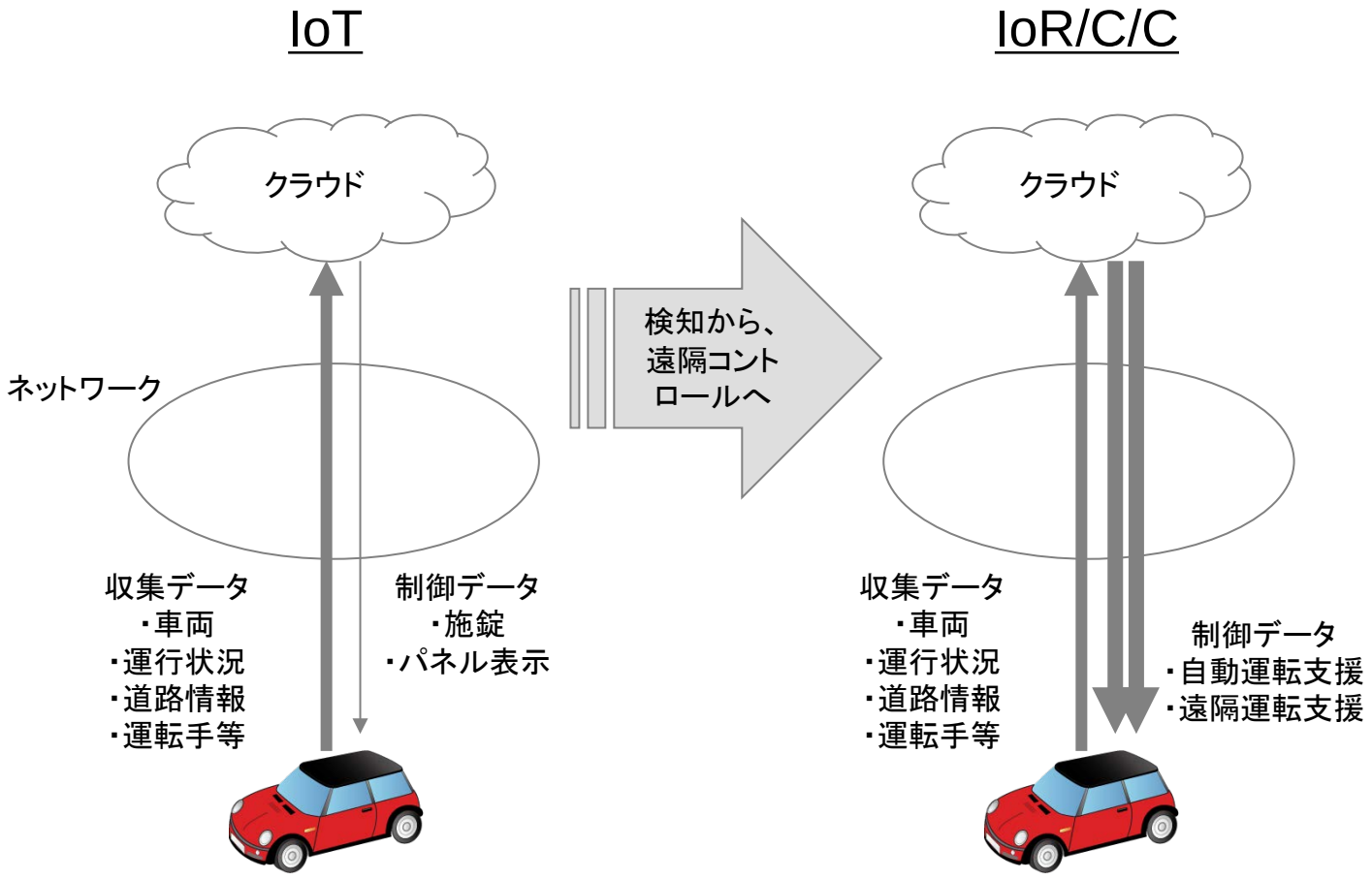
IoTのセキュリティ領域



IoTのセキュリティ領域(産業、機器別)



ポストIoT、Internet of Remote/Connected/Controlの萌芽
・感じるだけではなく、動くになると、リスクが急増することになる。



出所：NRI

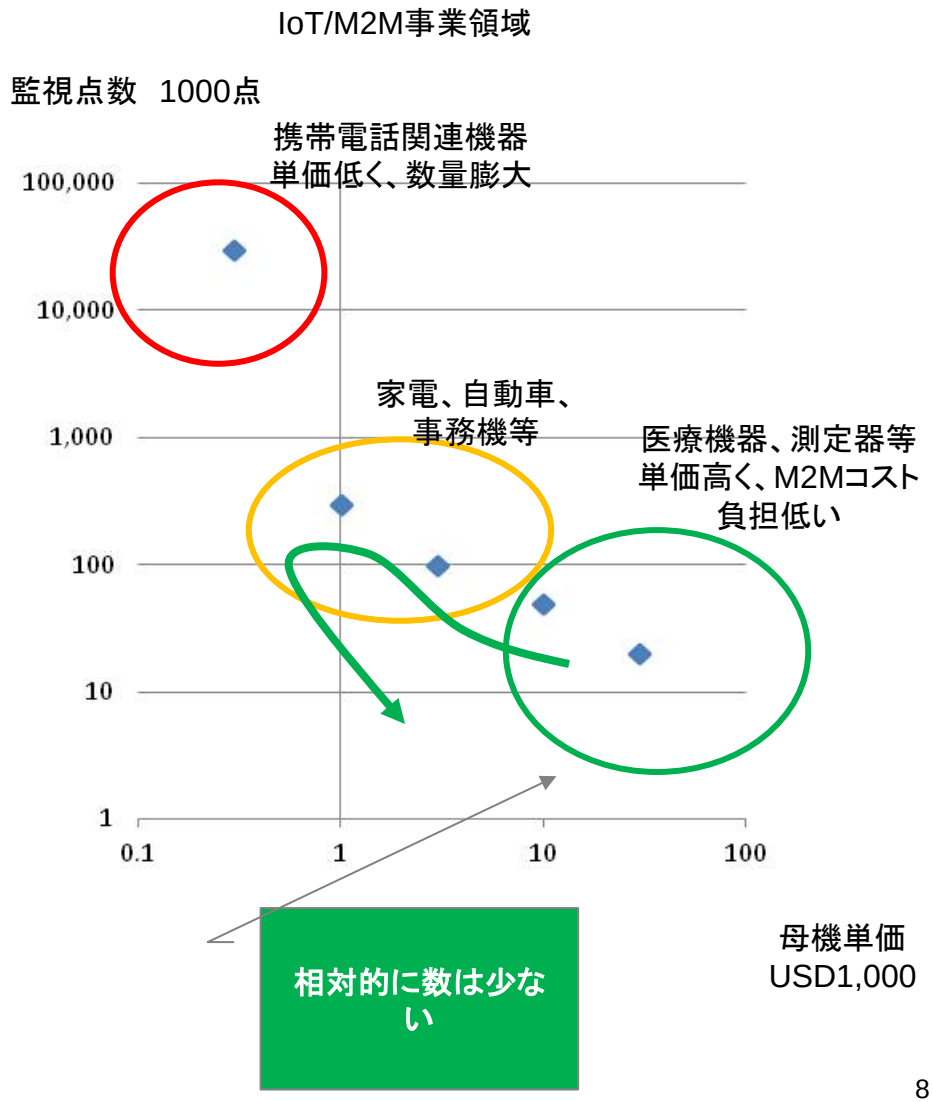
IoTビジネスモデルとセキュリティ　「現在は、重要設備でも数量少ないが・・・」

・今後、自動車、事務機等の100万台級、更にはヘルスケア等の10億級がリスク管理対象の重点となる。

■初期段階
顧客の機器単価が高い場合、監視点数は少ない。
企業運営上、リスクは無視できないが、愉快犯等のリスクは少ない。
(原発等の重要設備は別として)

■端末、USD1k～10k、台数10万～100万
自動車、事務機など、一般市民との接点、リスクが増える。

■端末USD50、台数10億
携帯電話、ヘルスケアなど、人々の生活に密着した装置が対象。



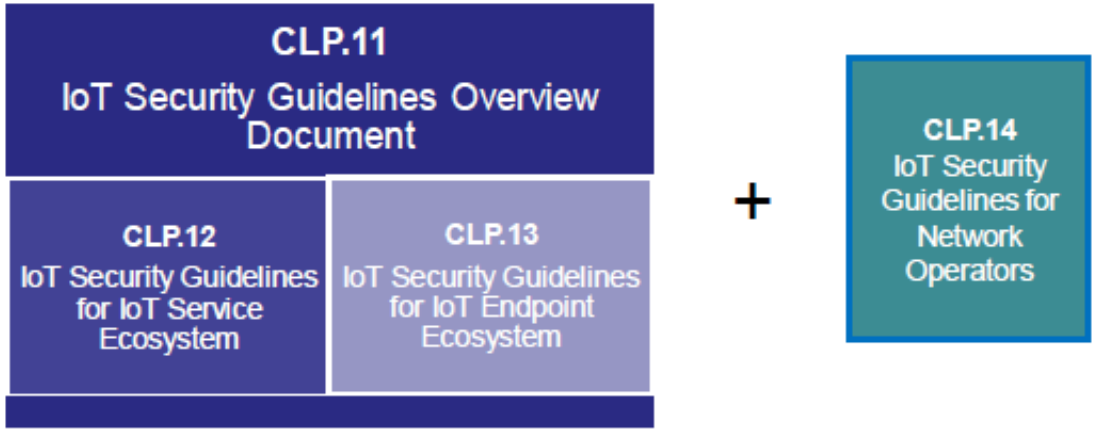
GSMA　IoTセキュリティガイドライン

■モバイル通信事業者等が主となり、IoTサービスプロバイダだけでなく、エコシステム全体に対してサイバーセキュリティ対策およびデータ・プライバシーに関して実践的な提言を盛り込んだ内容を目指している。

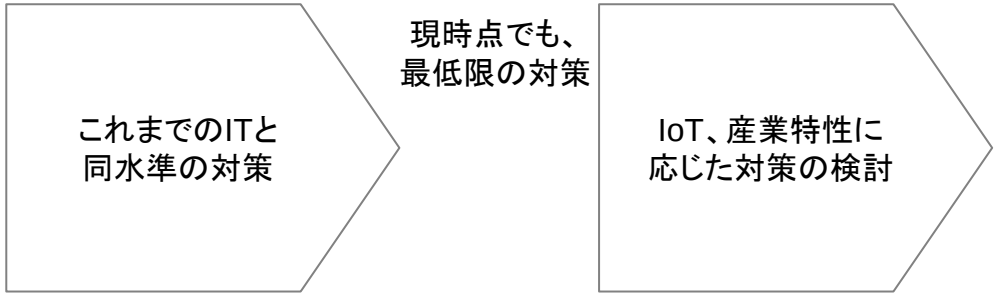
- ●AT&T、チャイナテレコム、Etisalat、KDDI、NTTドコモ、オレンジ、テレノールおよびベライゾン
- ●7レイヤーズ、エリクソン、ジェムアルト

- ●安全なサービス設計について、潜在的脅威を除去するための技術や方策。
  視点としては可用性(LPWA等による広域、低コストな無線インフラ)、ID(盗聴、傍聴、ID窃盗への対策)、プライバシー、セキュリティ等を設定。

- ●IoTサービスのすべての構成要素にについてデータの収集、保存、交換の安全性に関してリスク評価方法を確立することを提案している。
  Service Eco systemsとEnd point Eco systemに分けての検討。



想定される対策



例

■侵入等の悪意を前提とした脆弱性対策
- ●内部処理、コード等の秘匿化
- ●不法アクセス対策

■ウィルス→ワクチン等のPC事例の追随
- ●IoT版ワクチンソフト、FW等
- ●外部事象の監視

■妨害、圧迫等の愉快犯対策
- ●DDOS対策のIoT版

■サーバサイドの対策
- ●侵入検知

例

■ネットワークの仮想分離、スライス化
- ●IoTの社会的な重要性、妨害への脆弱性等に応じた仮想網としての分離
  「膨大なIoT対象からの低速トラフィック向け」
  「少数、もしくはエリア限定だが、リアルタイム性の強いネットワーク」
  「警察、消防や都市管理など、外部アクセスを原則として認めないネットワーク」
  等の異なる仮想ネットワークを、共通の物理的な基盤上で構築。

■ソフトの更新、復旧、デバイス機能の停止など、ネットワーク側での新たな機能要件検討