# ICANN68 Kuala Lumpur

- New gTLD Subsequent Procedures PDP
- A Look at IoT and DNS Opportunities

GMO BrightsConsulting

2020年8月4日

# Index

# 第68回ICANNクアラルンプールミーティング

## Highlights

第68回ICANNクアラルンプールミーティング
- 2020年2回目のバーチャルミーティング
- ポリシーフォーラム

重要なトピック
1. ポリシー策定の進捗
    - 次回の新gTLD申請受付に関するポリシー
    - 権利保護メカニズムに関するポリシー
    - WHOISの将来に関するポリシー
2. DNS悪用に関する進捗
3. 5Gの拡大とIoTの発展、DNSの接続制御への依存増加

# 次回の新gTLD申請募集ポリシーの策定について

## Background & Achievements

- 2012年の新gTLDプログラム・インターネットの拡大
- 2016年から次回申請募集に向けて新gTLDポリシー策定を開始
- ワーキンググループでの議論
- 中間報告書(Initial Report）とWork Track 5の最終報告書(Final Report)

## Current Progress

- 2020年内に最終報告書の公開予定
- 解決済みの課題をまとめている
- 未解決の課題に決着をつけるために議論中（次頁以降）

# ICANN68の議論

## ICANN68 New gTLD Policy Discussion

1つのセッションを開催、2つのトピックを協議

- プライベートオークションのテーマ
- 課題予測の対策フレームワーク

## Background

- 2012年の新gTLD申請結果、232件の文字列対立のセットがあった。
- 文字列対立を解決するため、全対象申請者による合意の下プライベートオークションを実施するケースが多々あった。
- プライベートオークションの結果、負けた申請者はTLD運用者となったレジストリの最終入札金額の一部を得ることができた。その際、複数申請者いれば、入札金額が均等に分布された。

## Identified Issues

- 複数のプライベートオークションに参加する申請者は、負けたオークションで得た資金を他のオークション資金に回すことで、勝ちやすい状況を作り出していた。

- 結果、一つのTLDを申請した申請者は、複数オークションに参加する申請者と比べて、プライベートオークションでの不公平感が発生していた。

- 中には、TLDの運用意図がないにもかかわらずオークションに負けることを前提として申請をしているケースもあったとみられている。つまり、不誠実な申請があったということ。

## Proposal for Resolution

- 不誠実な申請を抑えるメカニズムを採択しながらも、申請者に申請の自由を不当に奪わない方法を探るべきである。

- Hybrid Proposal 2+は、不誠実な申請を抑えるために申請条件として、2つの行為を禁止することを採択。
  - 金銭上の利益を得る目的での申請を禁止
  - 競合文字列を解決する際に負ける側に金銭面の利益を与えない

- 申請者に禁止行為に反しないことを契約事項とする。

- 不誠実な申請を防ぎながら、申請者が競合文字列を解決するためパートナーシップやTLDの共通運用等を許可する。

## Points of Discussion

- 不誠実な申請を抑える必要がある。Hybrid Proposal 2+が上がっている。
- プライベートオークションは、対象申請者の全員の合意の上で行われるので、問題がないという主張がある。
- 申請者が自由に競合文字列に対して解決する権利を持つべきである。
- プライベートオークションのような申請者間の解決方法をなくすことにより、ICANN主催オークションの可能性が高くなる。ICANN主催オークションの結果、ICANNが入札金額を得る。

## Background

- 2012年の新gTLD申請期間終了後に様々予測できなかった課題が現れた結果、申請ガイドブックや申請手続きが変更された。申請者は予定通り、契約締結や委任できなかった。

- ポリシー策定は2012年のプログラムに基づき、ポリシー改善を求めるが、予測できぬ課題がいずれ現れる。

- ポリシー策定後に現われる課題に対して、ある程度予測がつく対処法のロジックを与えるべきである。

## Remit

- 予測されなかった課題が上がった場合、プログラム変更（対処法）を明確にするためのフレームワークを定める。
- フレームワークによって、対象課題の種類、範囲、または背景を分析した上、プログラムへの影響度と課題を対処するための手続きを明確にすることが可能である。
- フレームワークを上手く利用するための役割が必要である。この役割にStanding Predictability Implementation Recommendation Team（常任予測実施勧告チーム・SPIRT） が検討される。

## Framework Aspects

- 課題の影響度によって想定する対処法の手続きを3つのカテゴリに分類する。
  1. ICANN社内手続きに関するわずかな変更：ICANNの指導により、変更を行う。
  2. ICANN社内手続きに関する大きな変更：ICANNがコミュニティ（SPIRT）と連携した上、変更を行う。
  3. ポリシー変更または新たなポリシーの策定：変更を行うために新たなポリシー策定が必要である。

## SPIRT Limitations

- SPIRTはあくまでもアドバイザー的な役割を果たす。
  GNSO委員会へのレコメンデーションのためにフレームワークを利用する。

- SPIRTは直接に課題に対する解決案を作ることができず、
  課題を解決するための手続きを明確にするまでである。

- SPIRTはポリシー策定を行うことができない。

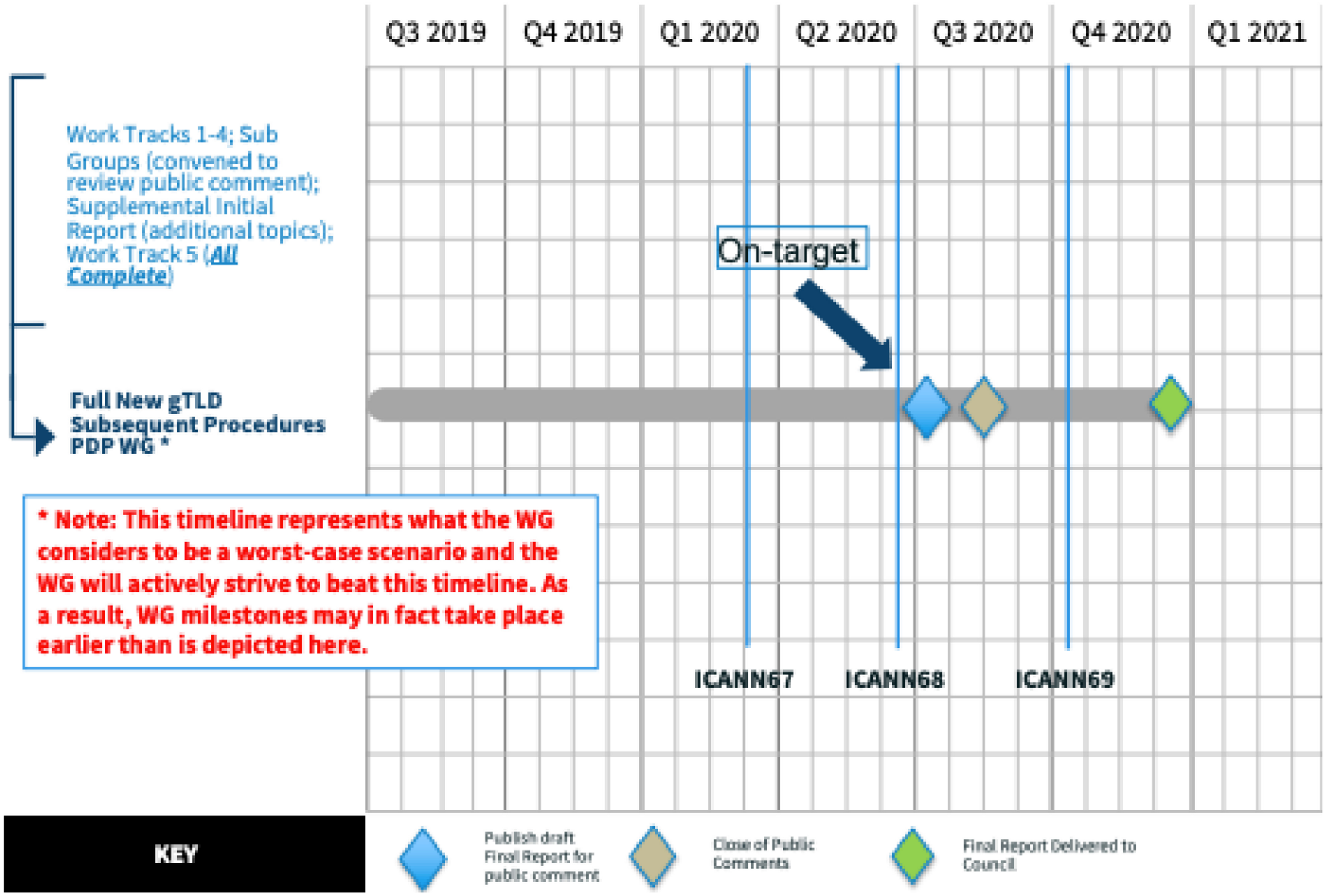
## Identified Issues

- いわゆるフレームワークは、複雑な考え方である。簡素化する必要性がある。
- SPIRTに参加するメンバーは、ロビー活動の対象になるリスクがある。
- ポリシー対象または実施対象の解決案を明確にすることが難しい。
- 課題を対処法の手続に当てはめるのは難しい。

GMO BrightsConsulting

## Working Group Timeline

### SubPro Timeline *



# 5Gの拡大とIoTの発展、それによるDNS接続制御と依存度の増加

## ICANN Discussion

- ICANN68は、5GとIoTの進化により、DNSへの依存度の増加に関する説明をパネルディスカションで行われた。

- このセッションの中から以下のような意見が出た。
  - DNSはIoTのセキュリティリスクを減らす。
  - IoT通信の中、サーバに情報を管理するためにDNSがインフラの一部として機能することが不可欠である。
  - 5GはIPネイティブであるが、IPマネジメントにDNSの利用をしていくことが現実的に考えられる。

ICANNで議論された内容に関して、一部弊社の解釈または考え方も踏まえ、5GとIoTの背景やDNSの重要性を紹介する。

## Background

- 5Gは第４次産業革命の基盤となる。
- IoTは、 Internet of Things、モノのインターネット、またはAIの進化により、Intelligence of Thingsを意味する。
- 5Gは、モバイルネットワークでのデータ送受信容量と速度の進化を意味するモバイル通信環境である。
- IoTと5Gの連携性を見ると、多くのデバイスが接続する中でサービスの安定性を担保できるようになる。Cloud, AI, Big Data, ICTの技術が拡大し、各産業分野が革新的に進化する。

## Security Risks

- IoT進化に伴い、脆弱な機器やシステムも増えている。
  年々攻撃数も増加し、攻撃手段も高度化・巧妙化している。

- 日本の国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology 、NICT）によって、2018年のサイバー攻撃関連通信が2015年に比べて3.9倍増加している中で、IoT機器を狙う攻撃が全体の約半数を占めている。

- IoT機器のマルウェア感染や乗っ取り事件、IoT機器を悪用した大規模のDDoS攻撃などの被害事例も続々報告されている。

## Security Risks

- IoT進化に伴い、セキュリティ脅威が増加する。確実なセキュリティ脅威を分野別に見れる。

| 区分 | 項目 | 発表年/会議 | 概要 |
|---|---|---|---|
| 自動車関連サービス | Connected Car / Sub System | 2015 / Black Hat USA | インターネットから自動車の遠隔操作を可能とする脆弱性を紹介。 |
| 消費者向けサービス | Home Energy Management System（HEMS） | 2014 / Black Hat USA | セキュアでないホームオートメーション開発の危険性を紹介。 |
| 産業別サービス | Health Care | 2012 / Breakpoint Security Conference | ペースメーカー及び植え込み型除細動器へのハッキングのデモを紹介。 |

総務省、「M2M セキュリティ実証事業」成果をもとに作成、2016

## Security Risks

- IoTセキュリティ対策の必要性が高まる中、世界のIoTセキュリティにかかる予算も増加している。

**世界のIoTセキュリティに対する支出（単位：百万ドル）**

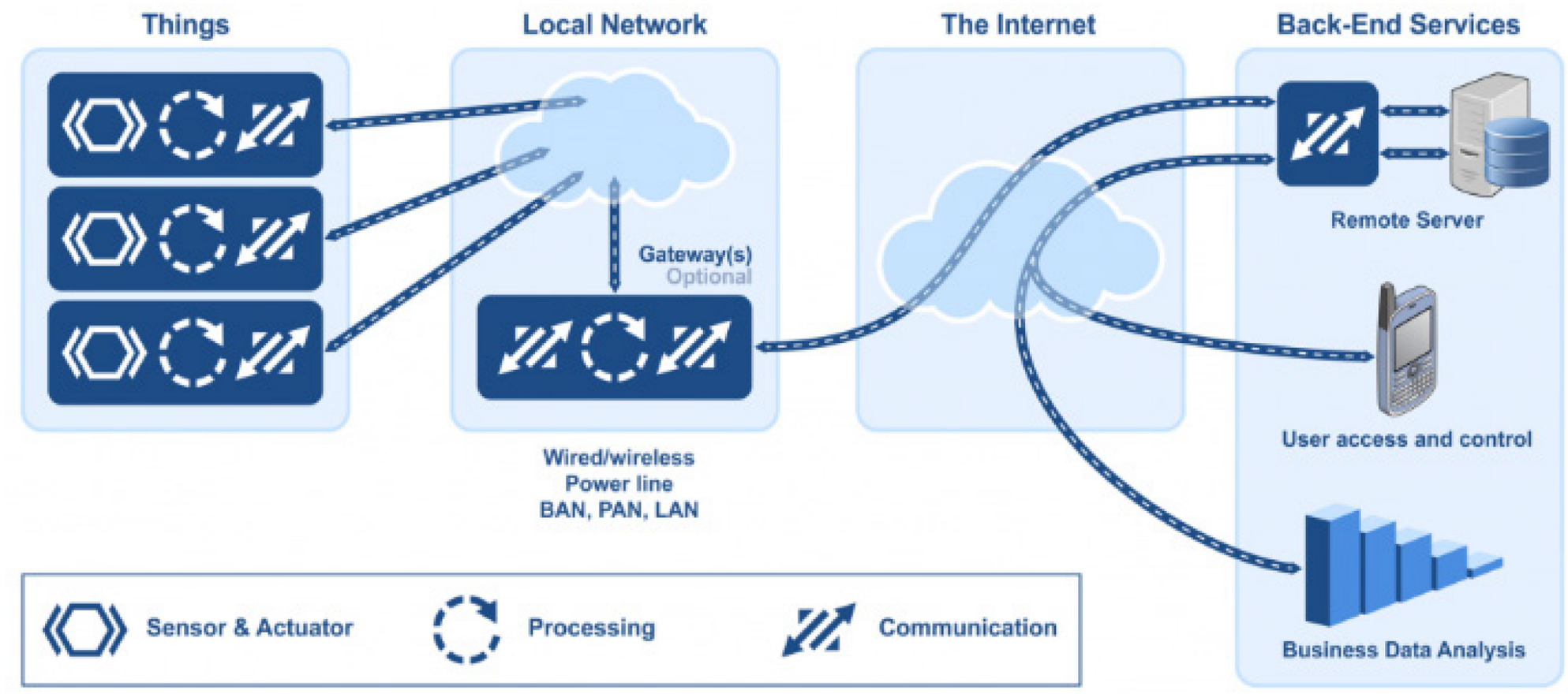
| 項目 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| Endpoint Security | 240 | 302 | 373 | 459 | 541 | 631 |
| Gateway Security | 102 | 138 | 186 | 251 | 327 | 415 |
| Professional Services | 570 | 734 | 946 | 1,221 | 1,589 | 2,071 |
| **Total** | **912** | **1,174** | **1,506** | **1,931** | **2,457** | **3,118** |

Gartner、「Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018」、2018.3

## Understanding How it Works

❑IoTセキュリティを理解するには、システムの構成と動きを実際にイメージするとわかりやすい。

**IoTシステムの主な構成要素**

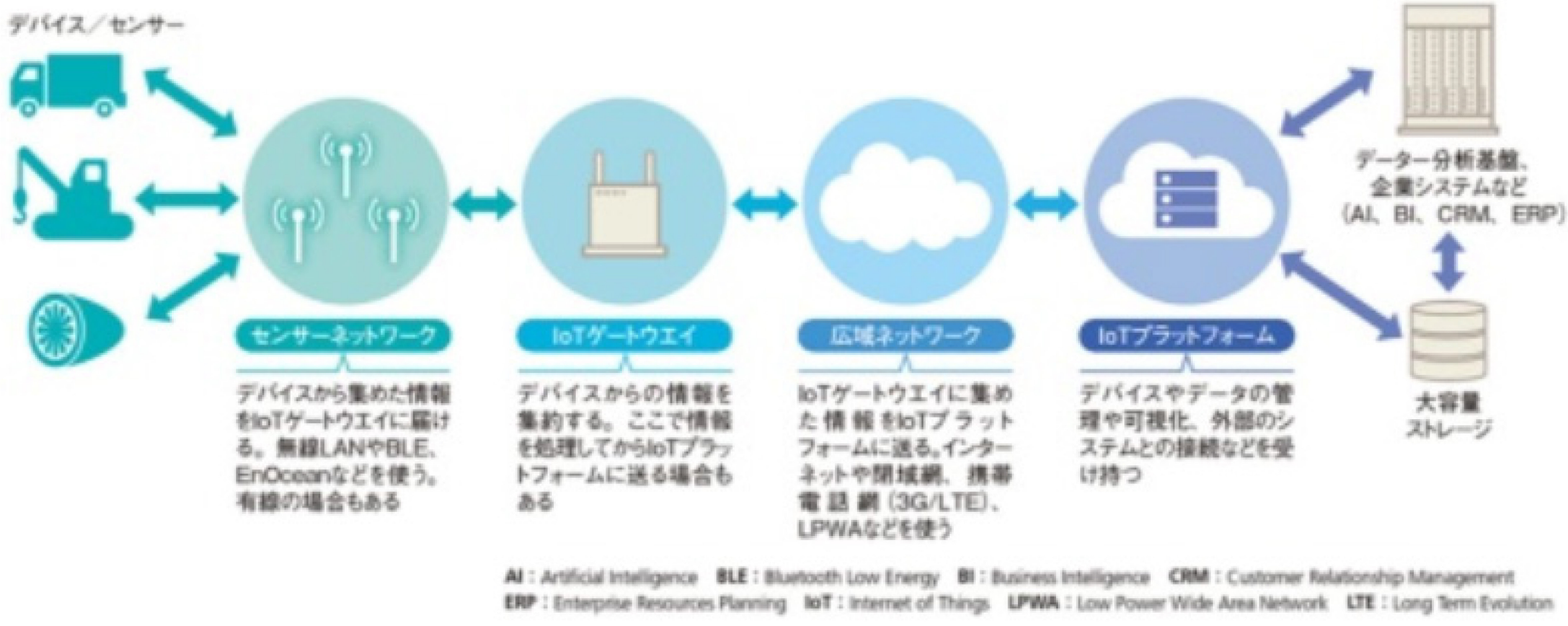



Micrium Website、How to Think about the Internet of Things (IoT)

## Understanding How it Works Pt.2

- IoTゲートウェイやIoTプラットフォームは、インターネット接続にモバイルネットワークを利用し、5Gネットワークの普及がシステム運用にネットワークの基盤となる。

**IoTシステムの要素と運用の流れ**




日経XTECH、IoTシステムに必要なモノ、構成要素を図解、2018.10.3

## IoT Security Approach

- IoT推進コンソーシアムと総務省、経済産業省が提示する「IoTセキュリティガイドライン」の対策方針の要点をバリュー・チェーンで考えると、３つの領域でIoTセキュリティ対策を分類できる。
  1. 機器（デバイス）
  2. ネットワーク
  3. サービス（アプリケーション）

- ネットワークのセキュリティ対策の中でもDNSにセキュリティが注目される。

- サーバーレベルのセキュリティ強化により、DDoS攻撃対象がサーバーではなくDNSサービスを狙うケースが増えている。

## DNS Security

- DNSセキュリティ強化のため、様々な技術やセキュリティサービスの開発・導入が進んでいる。TLS（Transport Layer Security）の認証機能を取り入れ、IoT機器との通信セキュリティを確保する方法や、データの加工を防止するための通信データの暗号化と監視機能の強化、重い通信が難しい小型IoT機器に特化したデータの軽量化なども進んでいる。

- インターネット接続サービスでは、DNSキャッシュサーバーに以下のセキュリティサービスが実装される。
  - DoT (DNS over TLS)
  - DoH (DNS over HTTPS)
  - DNSSEC (DNS Security Extensions)

## Domain Name IoT Security

- DNSセキュリティは、IoTのネットワークレベルでのセキュリティ対策として、効果的な方法の一つとして注目される。

- IoTの発展とともに、ドメインネームのハイジャックリスクも増えている。

- ドメインネームレベルでのセキュリティを考えると、IoT専用のクローズTLDの活用が可能である。ここで、二つの案がある。

## Closed / Restricted TLD IoT Security

- ネットワークのIPアドレス（ドメインネーム）レベルでIoT機器管理・サービス専用のクローズTLDを利用する。
  - GMOインターネットがネットワークサービスやDNSサービスを提供するシステム・サービス側でIoT専用のドメインネーム（.gmo）を登録・付与・管理することで、ドメインネームレベルでセキュリティを担保する 。

- ブランドTLDで自社が利用するIoTサービスや製品において固有のドメインネームを付与し、管理の安全性を確保する。
  - Microsoftが「.azure」のドメインネームで自社提供サービスに固有のドメインネームを付与することにより、メインテナンスがより効率化された。

## New Possibilities

- クローズ型のTLDは、現状のICANNの規制により、取得不可とされている。本件は新gTLDポリシー策定の中の一つのテーマである。

- クローズ型のTLDは、取得許可とされた場合、占領利用になるので、セキュリティ上、ブランドTLDと限定TLD（Restricted TLD）と同様である。このようにIoTが機能されるためのセキュなインフラの魅力性がある。

- ICANNで議論された例としては「.heart」。心臓ペースメーカーをつけた患者が「.heart」のドメインネームにアクセスし、自分の健康情報を確認するために利用することも想定できる。これは、医療分野のIoT機器のデータ管理及び送受信において、より安全なIoTネットワーク利用を担保する方法になる可能性がある。

当資料に関するお問い合わせは、下記までお願い申し上げます。

GMOブライツコンサルティング株式会社

寺地 裕樹／Michael Flemming

e-mail：consul@brights.jp

TEL： 03-5784-1069

Fax： 03-3462-5040



