

## 第1項 アブストラクテッド・ネットワークのコンセプト

過去 20 年間に於いて、TCI/IP プロトコルが普及しコンピューター・ネットワークにおける共通語となりました。そして IPv6 が登場し、従来バージョンでのアドレス制限が排除されたため、世界中のあらゆるデバイスが共通のプロトコルにより簡単に接続できるとされています。

しかし 3 つの新たな要因により、この考え方を見直す必要が出てきました。まず 1 つ目は、モノのインターネット (IOT) を構成しているセンサー、アクチュエータ、デバイスの波です。まだ広く認識されてはいませんが、主導権を握る IPv6 プロトコルを稼働させるには、これらデバイスの多くはあまりに小型、低品質、低能力、多量であると考えられはじめています。このため、企業やインターネットの IP ネットワークになんらかの形で組み込まれるよりシンプルなプロトコル (下記参照) が優位となるでしょう。

これら極小デバイスの反対側に位置するのが、コンピューティングおよび通信リソースのクラウドへの移行が著しい大規模な企業ネットワークです。これら企業の重要な要件のひとつとして、様々な SDN (ソフトウェアによるネットワーク設定) テクノロジーとプロトコルを使用した、自社ネットワークの管理、制御、調整をする能力が挙げられます。このような能力は、ネットワークのエッジにおける相互作用を管理するためのコンピューター・リソースに左右されます。

3 番目はこれまでの 2 つの要因によって発生した難題、つまり企業は、自社ネットワークに多数のシンプルな IOT デバイスを持ち込む必要性に苦しむだろうという問題です。これらのデバイスの多くはコンピューティング能力やプロトコルへの対応能力に欠けますが、それでも全てを SDN を通して管理しなければならないことには変わりません。これと並行して、工場で使用されているような多くの旧式 M2M (マシン同士) ネットワークの多くは、今日企業が SDN 技術で管理や調整することを望む業務サイロにて稼働しているシンプルかつ/または専用のプロトコル、という IOT と同様の問題を提起しています。

そこで、これらの要因に対処する新たなネットワーク・ソリューションには、混乱時においても業務を継続しながら発揮できる途絶耐性、稼働性、変化が必要です。

### アブストラクテッド・ネットワーク

一見矛盾するように見えるこれらの要件に対するソリューションは、概念的にはシンプルでありながら、実行の面では要求の多い、アブストラクテッド・ネットワークという考え方です。MeshDynamics のアブストラクテッド・ネットワークは、位相的に独立したネットワークのグループを、プロパゲータと呼ばれる新たなクラスのデバイスで構成された単一ネットワークに置き換えるというコンセプトです。

図 1a に示されるように、従来型ネットワークは今でも、人の操作によるトラフィック (スマートフォン、タブレット、コンピューター等) であるか、または M2M トラフィック (センサー、アクチュエータ、ロボット等) であるかによって区別されています。工場のような現場環境等では、レガシー・プロトコルおよびレスポンス要件によって、これらのデバイスが「アイランド」や「サイロ」として、その組織の他の要素から切り離されている場合があります。エンド・デバイスのシンプルさや組織特有の通信および管理の要件に対応するため、IP の台頭にかかわらず、このような孤立ネットワークが利用され続けているのです。

ネットワークとして明らかに効率面で劣ることに加え、これら孤立ネットワークは SDN テクノロジーによって管理・調整することができません。さらに重要な点は、潜在的な重要データフローやステータス表示が、組織のその他の業務を管理している主要ビッグデータ・サーバーから隠されてしまうことです。IOT およびレガシー・トラフィックをビジネス情報プロセスに組み込むためのパブリッシュ/ディスカバー/サブスクリプション・モデルの潜在能力は、アブストラクテッド・ネットワークという概念の顕著な利点といえます。(図 1b 参照)

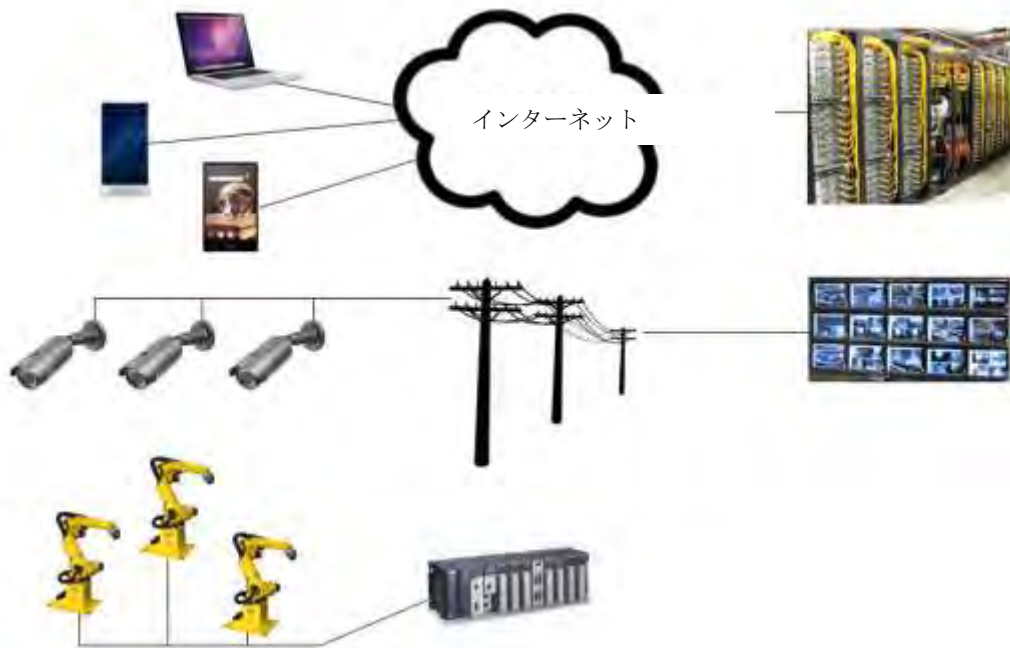


図 1a 手入力および M2M データの典型的な個別ネットワーク

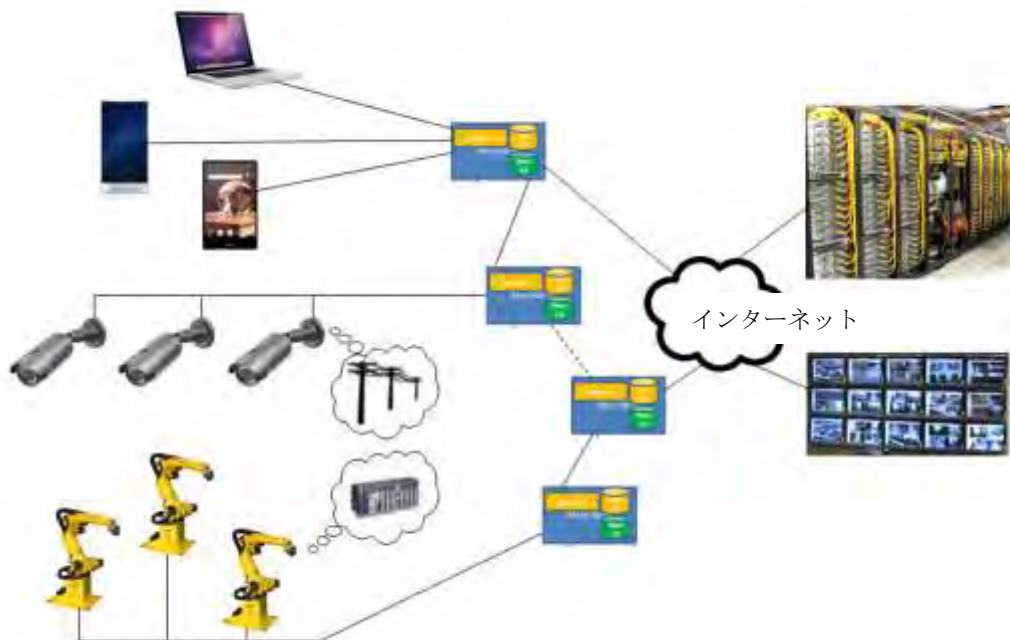


図 1b プロパゲータ・ノードを基本とするアブストラクテッド・ネットワークは、個別ネットワークを模倣しているが、企業による管理およびパブリッシュ/ディスカバー/サブスクライブが可能

アブストラクテッド・ネットワーク・モデルは、MeshDynamics プロパゲータ・ノード通信デバイス（図 1b に青い長方形で表示）を基本とします。このデバイスは、処理能力およびメモリ密度の進歩の恩恵を受けるほか、新たなオープンソース・システムと通信プロトコルを活用しています。プロパゲータ・ノードは、レガシーおよび IOT デバイスが、より高度なプロトコルを必要としないが組織全体の業務体系の一部となるよう、以前に分離されたネットワークの相互作用のプロトコル、タイミングおよび管理を模倣します。

### トポロジーではなくデータベースによるネットワークの構築

MeshDynamics アブストラクテッド・ネットワーク実現の根底となるテクノロジーは、ロジカル・ネットワークの接続と要件のモデルを構築する高度なリアルタイム・データベースです。（図 2 参照）実際

のトポロジーに関係なく効率的なバーチャル・ネットワークを築くため、様々な内部プロセスがネットワーク・トラフィックフローを基にこのモデルを追跡し更新します。これには待ち時間、プロトコル変換、マルチキャスト列込、フォワーディング、さらにはコントロールループ管理の詳細までもが含まれます。



図 2 ネットワーク・デバイス管理のためのデータベースによるアプローチ

重要な点としては、このアブストラクテッド・ネットワーク・モデルは独立して構築されるため、後に企業が SDN 技術とプロトコルを使用して改良、再構築、追跡、調整を行うことが可能です。これには 2 つの方法があります。1 つは、内部プロセスによってプロパゲータ・ノード・ネットワーク自体の中の様々なスケジューリングおよびモデリング・アルゴリズムにより、様々な異なるネットワーク・アプリケーション間の決定論的パフォーマンスを維持することです。

2 つ目は、ネットワークのパフォーマンスを規定その他のパラメータに基づいて最適化するため、各プロパゲータ・ノードに載っているアプリケーション・エージェントは、全社的 SDN メッセージングに参加することが可能なことです。(図 3 参照)

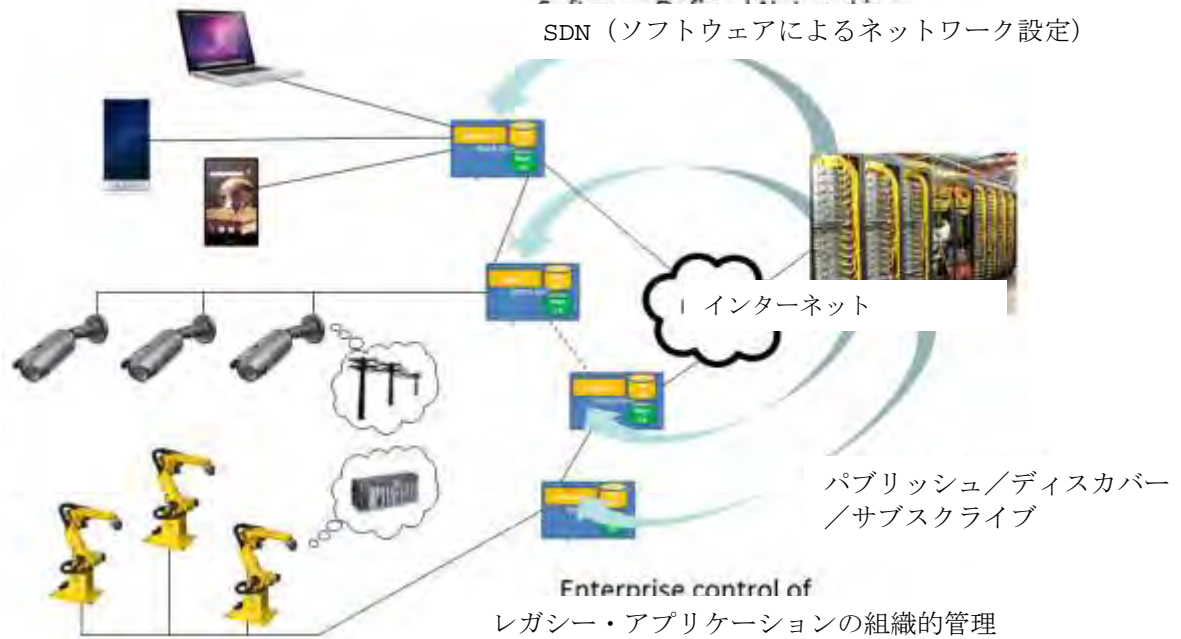


図3 レガシーおよび IOT デバイスまで、あらゆる場所での組織のツールとパブリッシュ/サブスクリプション関係を実現するアブストラクテッド・ネットワーク

プロパゲータ・ノードは、接続を促進するため、広範囲に渡る有線および無線インタフェースを多くのレガシーおよび IOT デバイスに物理的に統合することができます。以下の最も簡単な IOT デバイスに関する説明の通り、プロパゲータ・ノードは、最もシンプルまたは占有デバイスについても、パブリッシュ/サブスクリプション・データフローを許容します。この機能については以下にさらに詳しく説明します。同様にプロパゲータ・ノード自体、典型的インターネット、ビッグデータ・インテグレータ間のリンクとして、様々なネットワーク接続が使用可能です。

### 途絶耐性、移動性、可変性

「たくさんの要素を1つに依存させる」ために、アブストラクテッド・ネットワークの生存性とノンストップ稼働はきわめて重要となりますが、相互接続されたプロパゲーターがそのトポグラフィックと論理ネットワーク構成両方に対するデータベースを維持しますので、本質的な途絶耐性が提供されます。

プロパゲータ・ネットワークは、途絶耐性の第1レベルとして隣接ノードと代替パスの認識を維持し、主な接続として最適なリンクを自動的に利用し、変更または不具合の認識を維持します。これにより、図4に示されている通り、不具合の際の素早いルート変更が可能となります。この詳細は、本文書にて後に説明しています。



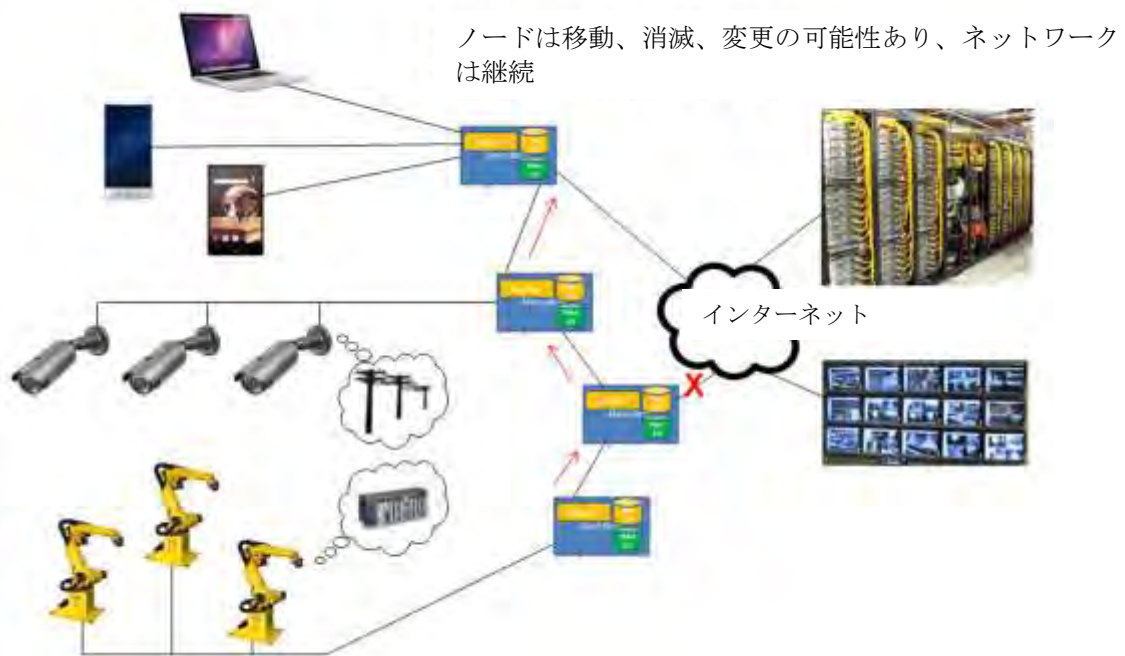


図 4 隣接データベースと経路指定テーブル交換によって自律的に提供されるプロパゲータ・ノード間の途絶耐性

この機能の副産物として、プロパゲータ・ノードが互いに、エンド・デバイスに対して、およびその他のネットワーク要素に対して稼働可能となります。ノードの隣接およびリンク・クオリティの内部データベースは常に更新されるため、個々のノードは古い接続の衰えに伴って新たな接続に移行し、ネットワークの稼働を維持します。

また途絶耐性は、個々のアプリケーションおよび接続されている各グループのデバイスにも及びます。各プロパゲータ・ノード内のアプリケーション・エージェントには、データ収集、警告およびステータス、コントロールループ管理、さらにはネットワークの認識およびリクエストのなりすましまで、接続されているデバイスに代わって様々な機能を実際に実行するソフトウェアを装備することができます。これはアップストリーム接続の完全遮断および往復通信の中断中も維持されます。プロパゲータ・ノードが、アップストリーム接続が回復するまで、ローカル・オペレーションを正常に保つからです。(図 5 参照)

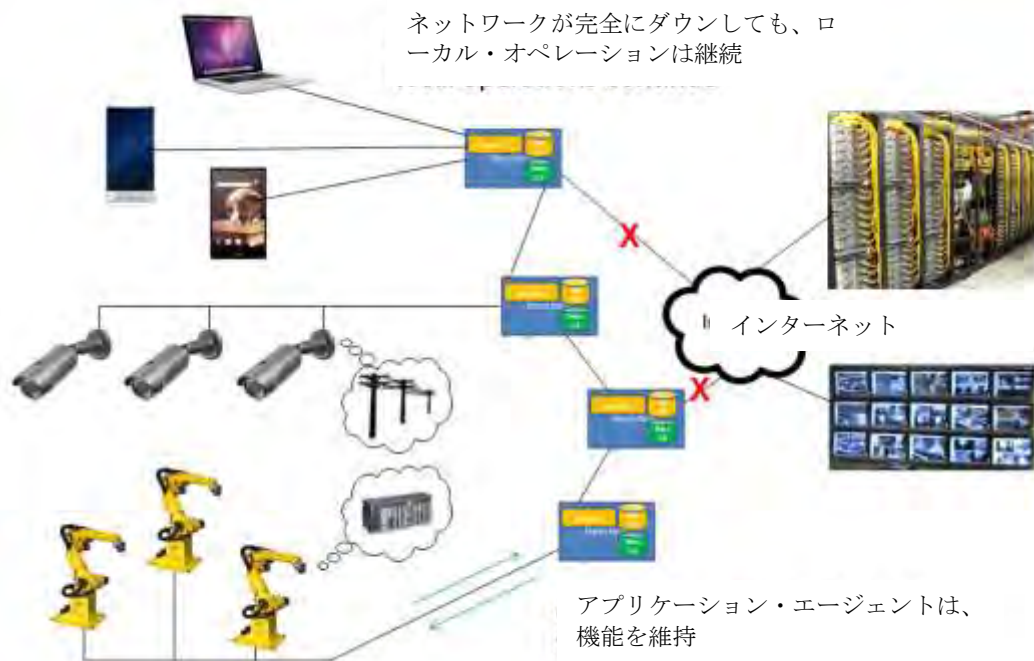


図5 プロパゲータ・ノードのアプリケーション・エージェントは、アップストリーム接続が切断されても、接続されているデバイスのローカル・オペレーションは維持を維持

プロパゲータ・ノードとアブストラクテッド・ネットワーク概念の能力は、今後のモノのインターネット・デバイスの急増と、これらの簡潔は M2M 通信スキームの統合において、特に重要となるでしょう。これらについては、次項で説明します。

## 第2項 モノのインターネットの影響

今後 10 年間に於いて計り知れない数の相互接続されたデバイスが、交通システム、工場、農場、森林、公益事業、土壌状態、天候、海洋、その他資源の監視や対応を行うことでしょう。

これらの多くの多様な IOT デバイスに共通する特質は、IPv6 等の従来型ネットワーク・プロトコルに使用するには小型、低能力、低品質、多量すぎるといった要素です。

同じ理由により、この IOT デバイスの大きな波は、既存の技術やツールでは管理不可能です。その代りに大規模な自然からの教訓が、IOT のための新しいアーキテクチャに導いてくれるでしょう。

自然からの手がかりと OEM ライセンシーとの連携により、MeshDynamics は「[Rethinking the Internet of Things](#)」にその概要が掲載されているコンセプトを、エッジにおける高性能（確実かつ拡張可能）な IOT M2M コミュニティのサポートに関する現実問題にまで拡大しています。

### シンプルなデバイスはシンプルに機能

現時点では、IOT を現行ネットワーク・プロトコルと実践の延長とみなしている企業が多くあります。しかし産業としてのモノのインターネットの最前線に立つ企業は、既に問題を見据えています。

「従来型操作技術の問題に対処するため最新 IT テクノロジーを利用した発展的改善が多く語られている今日だが、真のビジネス・インパクトは、対応可能な問題の範囲を広げることだ。従来型操作技術は、プロセスの正確性と安全性に重点的に取り組んできている。従来型 IT は市場に出すタイミングを焦点とし、さらに最近ではセキュリティ問題を重要視している。どちらの考えも、特定タスクを実行するために多数のデバイスが相互作用している、相対的希少性の世界の中で生まれたものである。しかし未来の方向性は、自律制御の元で瞬時に絶え間なく変化し、分散されすぎているため個人では追跡不可能な無数のデバイスとタスクである。安全や保全および管理を確実にするための既存のプロセスは、このような規模を目の当たりにすれば崩壊する。この新たな世界に対応するテクノロジーの再開発を刺激することが、インダストリアル・インターネット・コンソーシアムの焦点である。」

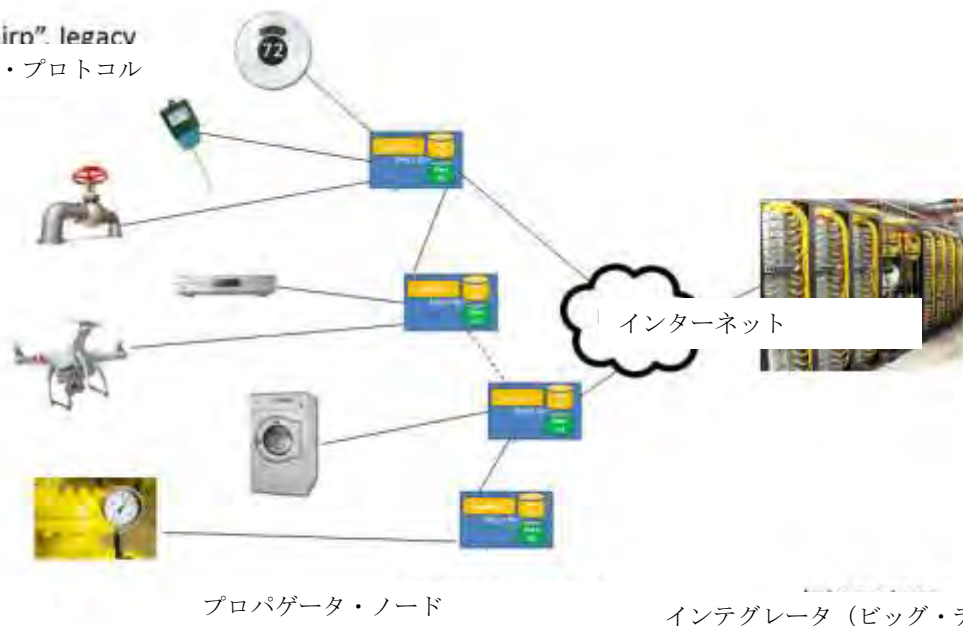
[Industrial Internet Consortium Quarterly Report February 2016](#) (インダストリアル・インターネット・コンソーシアム四半期レポート [2016 年 2 月号])

真に拡張可能な IOT アーキテクチャには、異なる世界観が必要です。マシンが自律的に機能し、例外時のみ人間の介入があるという、シンプルなデバイスがその名の通りシンプルに機能するのです。

このマシン同士の相互作用の世界は、TCP/IP や WiFi よりも、鳥のさえずりやミツバチや蟻といった社会性昆虫の意思疎通のようなものとなるでしょう。

ネットワークの末端は、単純な「デバイス」です。これら末端デバイスは、単にデータを「チャープ」する（さえずる）またはデバイスに対して行われるチャープを聞くだけです。大多数のデバイスは、非常に小さなビット数のデータ（スモール・データ）を発信および受信するだけです。IOT の世界においては、これらの小さく一見して無防備なチャープ（後に解説）は、上流に伝搬され、クラウドによるインテグレーション・ポイント（つまり、ビッグデータ・サブスクライバー）まで連鎖を上ります。（図 6a 参照）

「Chiro」. legacy  
「チャープ」、レガシー・プロトコル



デバイス

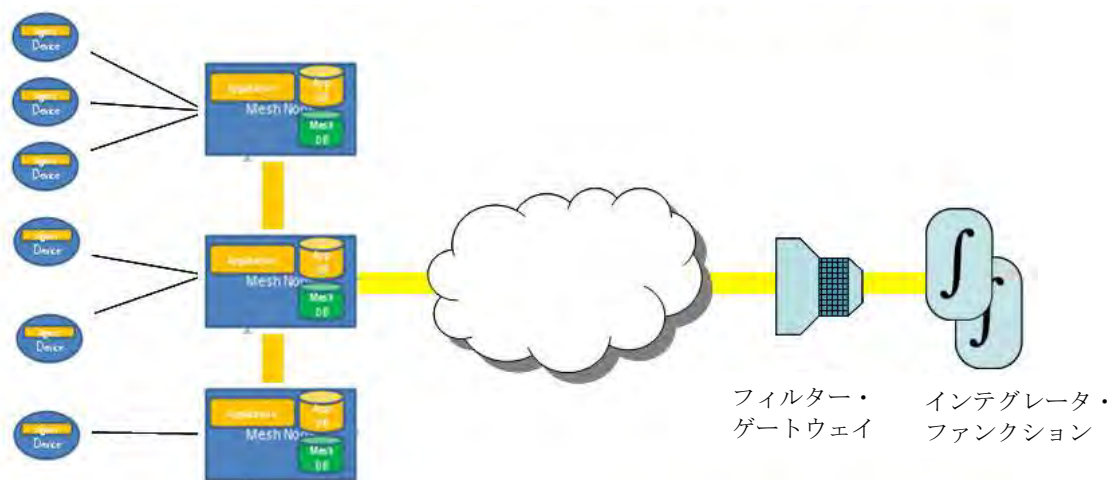
プロパゲータ・ノード

インテグレータ (ビッグ・データ)

図 6a 3層アーキテクチャとアブストラクテッド・ネットワーク・コンセプトが IOT の能力を引き出す

上述の通り、ネットワークのエッジにシンプルなデバイスを統合することの鍵は、ネットワークの複雑性の負担をアブストラクテッド・ネットワークの MeshDynamics プロパゲータ・ノードに移行することです。プロパゲータ・ノードは、シンプルデバイスと上位の組織コンピューターとの間の「ガスケット」となります。(図 6b 参照)

↓ データ・ストリーム ⇒ M2M 「スモール」 データフロー ⇒ 管理ビッグデータ・サブスクリバ



通常モード

インターネット接続不要  
「スモール」データ Pub/Sub で起動

定期監視制御モード

クラウド基盤アプリケーション接続  
「スモール」データ収集/分析

図 6b IOT/M2M の拡張可能安全基本アーキテクチャ

自然が花粉を扱うように、(拡張可能な) IOT は個々のチャープを真の「ベスト・エフォート」として扱うことによって、外部要因による強いブロードキャスト・ストームがいち早く無くなるようにしなければなりません。IOT のチャープはデジタルの花粉と言えるでしょう。軽くて幅広く「拡散」し、「関心のある」受け手/サブスクリバにとってのみ意味を成します。

花粉は受け手主導のもので軽量です。セキュリティはその「パケット」構成に備わっており、意図する花のみがペイロードを解読できます。その他の人にとっては単に花粉アレルギーの季節にすぎま



せん。また、個々のチャープ・メッセージは重要ではありませんので、エラー回復または完全性確認オーバーヘッド（基本チェックサム以外）は必要ありません。

それぞれの IOT チャープ・メッセージには、短いシンプルなマーカー、ショートデータ・フィールド、チェックサムがあります。私の著書で説明した通り、シンプルなチャープとはわずか 5 バイト程度です。（これに対して最も小さなセNDER主導 IPv6 パケットは 40 バイトです。） [スライド]

チャープとは、まさに IP データグラムが意図したものです。帯域幅の節約は明白ですが、多種多様なエンド・デバイスそれぞれにおけるメモリー、プロセス、電力消費の削減に関しては、IP スタックを起動することに比べ見劣りします。IOT において必要のように、エンド・デバイスにかかる費用負担と複雑さは非常に低くなります。

従来のインターネットとは対照的に、エラー確認、ルーティング、上位レベルのアドレス指定その他は必要ありません。末端デバイスは最低限のデータフローのみを要する、ほぼ何も考える必要のない「働き蜂」です。IOT に接続されるデバイスの圧倒的大多数にはこれで十分でしょう。（さらに高レベルなプロトコルが必要であり人の介入によって確認される高度なアプリケーションの場合は、IPv6 が適しています。）

チャープの基本概念は新しいものではありません。 通信を行う専用デバイスやプロダクト（テレビのリモコン、自動車のサブシステム、ネットワークでつながれた工場等）全てには、簡潔な M2M メッセージングが広く行き渡っています。簡潔な M2M メッセージングとは、8 ビットのマイクロコントローラーの時代から行われてきたマシンの通信方法です。課題は、既に機能しているものを安全に拡張することであり、新たに発明することではありません。

### 第3項 技術ストラテジーと実践

アブストラクテッド・ネットワークのコンセプトには、基本的根拠が1つあります。シンプルなデバイスがプロトコルに対応できない場合は、どこかに置かれてエンド・デバイスの代わりに機能しなければなりません。この「どこか」の主な要素は、レベル II プロパゲータ・ノードです (図 6b および図 7 参照)。上記で紹介したように、これらはルーターやアクセスポイントといった良く知られたネットワーク装置のようなものですが、IOT やレガシー・デバイスの場合では異なる機能をします。

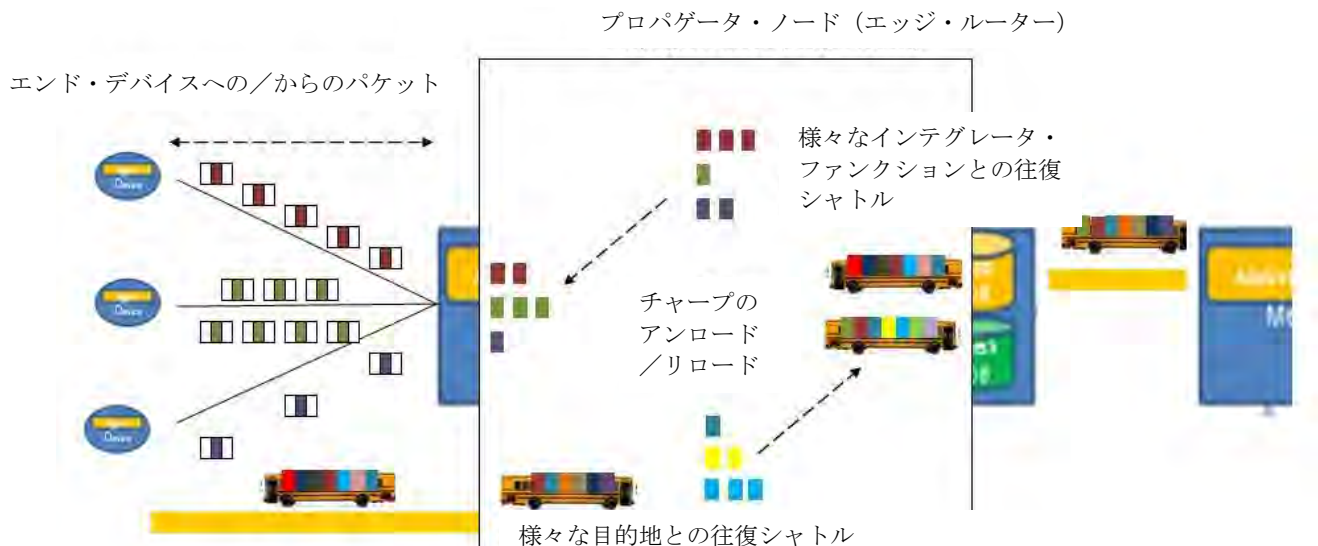
プロパゲータ・ノードの機能をさらに詳しく調査するため、IOT アプリケーションにてこれら機能の試験を行うことが可能ですが、これはレガシーおよび IP ネットワーキングにまでも及ぶと当然考えられます。

#### エッジにおけるパブリッシュ、サブスクライブ、ディスカバリー

プロパゲータは、あらゆるデバイスからのデータ「チャープ」に耳を傾けます。チャープに含まれる「マーカー」のグループ (下記に説明) に基づき、プロパゲータはこれらのチャープを、どのように他のプロパゲータ・ノードに、さらに上位のインテグレータ (ビッグデータ) サブスクライバに配信するかを判断します。

モノのインターネットの非常に大きな規模に合わせて拡大するため、これらのプロパゲータ・ノードには、様々なディスカバリーと自律的管理の能力が備わっていなければなりません。範囲内の他のプロパゲータ・ノードを認識し、隣接要素の経路指定テーブルを設定し、適切なインテグレータへの見込み経路を特定する必要があります。

重要なのは、物理的にメッシュされたプロパゲータから、論理ツリーのようなトポロジーを構築することです。トポロジー・アルゴリズムについては、試験を実施し、(よりオタク的な) MeshDynamics パテントにて説明されています。[詳細]



アプリケーション: アプリケーション/デバイス・データフローのサブスクライバ/アプリケーションへのリアルタイム・パブリッシング

- パブリッシャー/サブスクライバー・アプリケーション間の定期的、定時「シャトル」サービスを定めた Pub/Sub フレームワーク
- 利用可能な専用デバイスのための MAC80211 「無線」 アブストラクション (各インタフェースはポート・ベース)
- 管理レベル監査/管理サブスクライバによって監視されるアプリケーション入出ポート

図7 集合、刈り取り、リアルタイム M2M 「シャトル」のアプリケーション

プロパゲータ・ノード上の Pub/Sub 認識アプリケーションは、集合および刈り取り「ハブ」としての役割を果たします (図 7 参照)。エンド・デバイスから/へのチャープは、転送のため他のトラフィックと組み合わせることができます。アプリケーションは、このネットワーキングを、デバイスおよびイン

テグレータに代わって、これらの上または下のレベルで提供します。いかなる標準ネットワーク・プロトコルでも使用することができ、プロパゲータ・ノードは異なるネットワーク間（パワーラインまたは Bluetooth から ZigBee または WiFi へ等）で重要な翻訳を行い、主にチャープ・データストリームからスモールデータ・フローを作成します。

他の信頼できるアプリケーションおよびエージェントは、多くがプロパゲータの内部に置かれており、エッジのための SDN（ソフトウェアによるネットワーク設定）パラダイムによって、データ処理能力のない、小型、低品質、多量の IOT デバイスの機能調整および管理を行います。

MeshDynamics は、米国海軍および米国エネルギー省向けに途絶耐性のあるネットワークのためのオープンソース・プロパゲータ・プラットフォームを開発してきました。プロパゲータ・ノードは、SDN ベース・ルーティング、ビデオ、IFTTT（「もしこうだったら、ああする」という条件付き規定）等についてのより厳密なパケット検査のため、OpenWRT アーキテクチャ内のユーザ・スペース・アプリケーション・レイヤーをサポートします。これらプロパゲータ・ノードは、内蔵アプリケーション・エージェントによるインターネット接続の確認なしに、自律的で強固な機械制御を提供します。

この結果、応答性あるローカルな自律性のレベルを維持しながら、ビッグデータ・サーバーからネットワーク端末まで拡張できるパブリッシュ/サブスクライブ（Pub/Sub）ネットワークとなりました。基準をベースにした様々な SDN プロトコルが、分配されたアプリケーション・エージェント上で実行可能です。

「末端のデバイス利用をどんなにしても拡大しても、MeshDynamics のスケラブルでオープンな Pub/Sub により、確実なリアルタイム終端間パフォーマンスを提供するための、企業クラスのオブジェクト・マネージメント・グループ (OMG) 承認業界標準である RTI (Real-Time Innovations) のメッセージングシステム、PRISMTECH、OpenDDS、その他との迅速な統合が可能となっている。」  
 (Space and Navy Warfare Center シニア研究システムエンジニア、Curtis Wright)

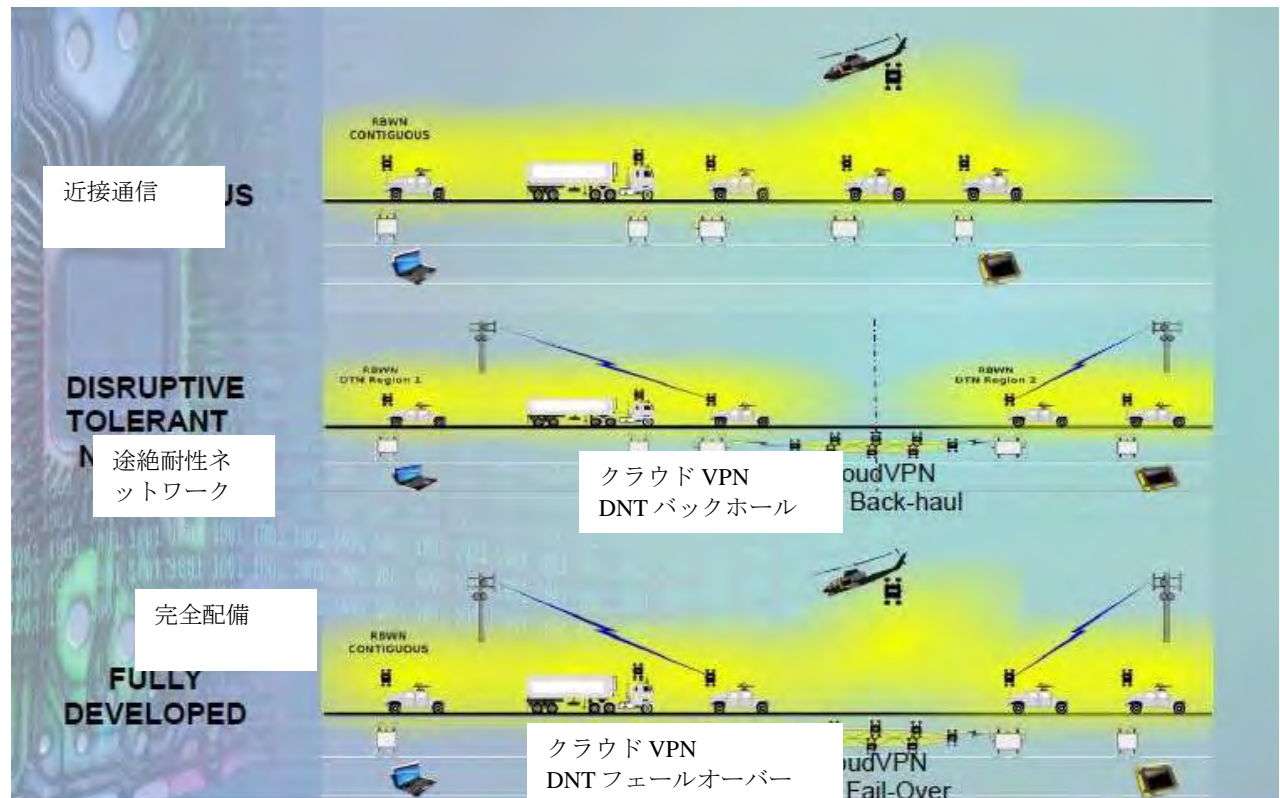


図 8 混乱耐性半自律型ネットワーク (SPAWAR)

上述した要素は、ほぼ全て途絶耐性メッシュ・ネットワーク（図 8）において自律的および自動的に行われます。プロパゲータおよびそのアプリケーションは、リンクまたはノードの機能停止を迂回し、ネットワーク要素のモビリティによる問題に対処します。しかしプロパゲータの最も重要な性能の中には、

ディストリビューテッド・アプリケーション・インテリジェンス・エージェントというものがあります。これは総合的なパブリケーション/ディスクカバー/サブスクリプト基盤の一部としてプロパゲータ・ネットワークを「調整」する高度な機能を可能とし、および・またはノード自体の中にアプリケーション・インスタンス（マシン・コントローラ等）を作成できるようにするものです。これらのエージェントにより、より広範囲のネットワークの接続が切断された際にも、接続されたデバイスは稼働を継続することが可能です。[続きを読む]

### ネットワークの及ぶ範囲を拡大

プロパゲータ・ノードの独自のマルチ無線アーキテクチャは、変化や途絶に対応できる能力の他にも、有線接続を追加せずにネットワークを多数の「ホップ」（ノード間リンク）上で延長できる能力を提供します。この「数珠つなぎ」能力により、大規模な戸外活動が接続できるほか、新たな遠隔地へサービスを拡大することが可能です。

このように拡張されたプロパゲータ・ノードのリンクは、単にアブストラクテッド・ネットワークのもう一つの要素とみなされ、エンタープライズ SDN ツールおよび技術によって管理が可能です。内部データベースは、他のネットワーク接続に比べて最小の追加待ち時間またはジッターで、長く連なるプロパゲータ・ノードを行き来するトラフィックのさらなる遅延を監視し対応します。

### 現行および未来のネットワークの統合

プロパゲータ・ノードは、チャープとレガシー・トラフィックを変換し転送のため IP パケットにパッケージ化する一方、IP トラフィックの典型的スイッチまたはルーターとしても機能します。プロパゲータ・ノードはチャープ・ベースと従来型という両方のプロトコルを取り入れるため、新たに出現した IOT、レガシー、および IP ネットワークの自然な統合ポイントとなります。

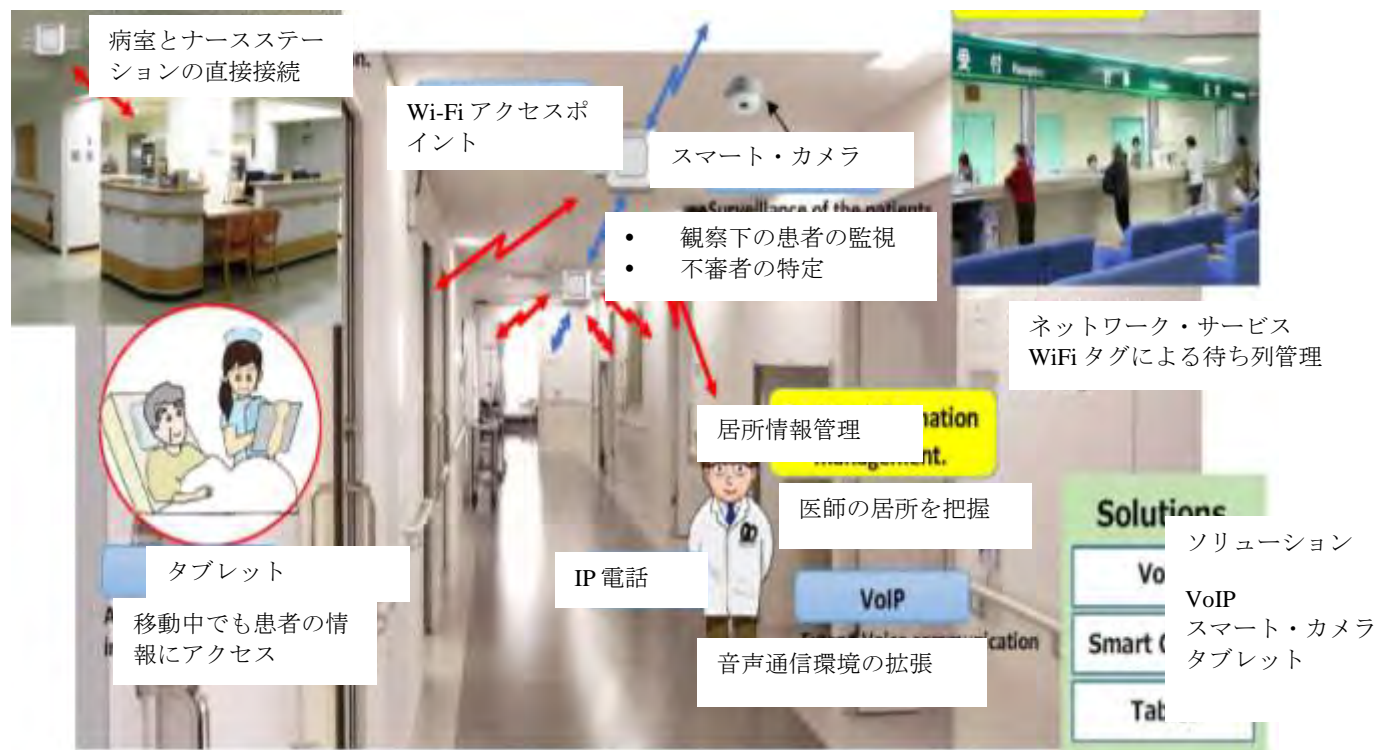


図 9 リアルタイムで状況判断をサポートする「スマート」ネットワーク（SHARP）

シャープは、「スマート・ネットワーク」と称して配備するため、ネットワーク・デバイス QX-C300 シリーズを最近発表しました。従来型の Wi-Fi アクセスポイントとして機能するほか、カメラ等の IOT デバイスの接続を可能とするものです。



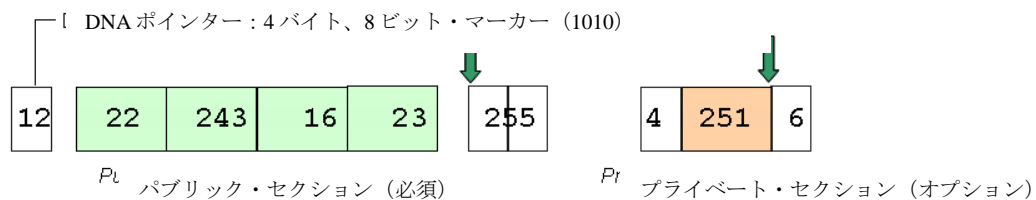
「MeshDynamics のプロパゲータ・ノード・ソフトウェアによって、最低限の配線増設のみでWiFi ネットワークを配備することが可能です。また現時点においても将来的にも、同一インフラ上に新たに台頭してきたモノのインターネットのデバイスを統合することができます。」（シャープ株式会社通信システム事業本部副本部長、新井優司氏）

## シャープがディスカバリーを可能とする

花粉等の自然界における「メッセージ」のように、チャープの構造はデバイスの特定には不足しますが、パブリック・マーカーによるデバイスの種類の区分の特定は可能です。階層的には、デバイスはセンサーまたはアクチュエータで区分され、さらにセンサーの種類、そしてモデル番号等のその他の識別特性で区分することができます。OEM 製造者が利用できるチャープ識別の業界固有のオープンソース・レジストリが用意されることが期待されています。

それぞれの OEM では、エンドツーエンド機能および管理を拡充するため、新たなチャープのジャンルを設定したり、または既存チャープに固有の拡張子を付けることがあります。多数の業界研究部会および SIG（スペシャル・インタレスト・グループ）が協働して、ニーズに適した小区分を作ることが期待されています。重要なのは、従来型の標準プロセスを待つのではなく、このデータ構成が IOT の展開を加速する進化的な手法「素早く初めて、変化に対応する」ことを可能にすることです。自然界では起こらなかったことです。

タイプ ID のつけられたチャープは、IOT において非常に有益な可能性を広げます。企業の IOT ネットワークは「閉鎖型」であることが多く、これらは内部にデータを保護するため、IOT パケット内で独自のマーカーを使っています。（チャープ・データのセキュリティについては、後の「セキュリティについて」で説明します。）しかし、個人や組織がチャープのデータ・ストリームを公開し、その公開されたデータを誰でも使えるようになっているケースも多く見られます。（これはある意味、現在インターネット上で可能となっているウェブ画像のストリーミングに似ています。）



パブリック・エージェント ID は、4.8.255 (4 バイト・パブリック、8 ビット・マーカー、DNA255 [サブスクリプト])、エージェント・ステータス: 分類は 8.8.8.8 (各 1 バイト)、解読チャープ・クラス: 4.8.22.243.16.23

このペイロードには別のエージェントが必要

プライベート・エージェントは、(4.8.22.243.16.23 に対して) 1.4.6、解読値 (251)

パブリック (オープン) ペイロードが短い分類値 (チャープ・クラス 4.8.22 等) のチャープ: 温度 243F、圧力 16psi、湿度 23%

企業はその独自の (社内用) 分類体系を定義する。

検出された「未知」のチャープ・クラスの発見は、SIG にて対処。

配信、チャープ分類法の有機的成長。

図 10 チャープ文法への漸増拡張子が、OEM でのカスタマイズをサポート

これらのチャープ・ストリームはデバイス・タイプのタグ付けがされているため、「関心のある」インテグレート・ファンクションが、地理的な場所、デバイス・タイプ、またはデータ・パターンに基づいて、有用と期待できるチャープ・ストリームを「発見」できる可能性があります。従って、アーキテクチャは、インテグレート・ファンクションが「関心のある」データ・ストリームを探し、サブスクライブする、受信者ベースとなります。

チャープのデータ構成は、従来型ネットワーク・プロトコルとは大きく異なりますが、IOT の過半数のセンサー、アクチュエータ、デバイスに必要なのはこれだけです。またタイプが表示されたチャー

プ・データストリームは、予期されるデータの波を活用するために、非常に大きな可能性を広げるでしょう。

## セキュリティについて

チャープを基本とする IOT の世界では、非常に大きなパケット、パブリッシャーにおけるセキュリティ、個々のメッセージの確実な配信は、過去のものであります。チャープは、「軽い」花粉による大規模なパブリッシュおよびサブスクリプション・ネットワークを持つ自然界を正確に模倣しています。自然界の花粉やフェロモン、鳥のさえずりのように、データが発行されても一定の受け手しかその意味を完全に解き明かすカギを持たないことに、多くの人々が気付いているでしょう。

チャープ IOT は、IP の「男性」（送り手主導）構造に対する「女性」（受け手主導）です。メッセージ展開が受け手主導であれば、ネットワークは容赦ないブロードキャストの嵐を生き延びることができます。IP ベースのネットワークでは、あっという間に崩壊してしまうでしょう。

（従来型 IP ベースの）IOT デバイスが無数に使用される場合のセキュリティ上の脅威は非常に現実的です。IP ベースのメッセージ送受信（サーバーからデバイス）は、拡大縮小ができません。IP は送り手主導のメッセージングですので、暗号化が必須となります。勝ち目の無い戦いです。ムーアの法則が廃れ始め、 $O(n*n)$ 等、メトカーフの法則が飛躍を遂げています。自然がなぜオープンで拡張性のあるサブスクリプション・ベースの（受け手主導の）「メッセージング」を採用しているのかには、それなりの理由があるのです。

プロパゲータ内のアプリケーション・エージェントにより、さらなるセキュリティが実現されます。（図 6b 参照）保護されたデータは、オープンデータと並行してプロパゲータ・ノード・ネットワークを流れるかもしれませんが、アプリケーション・エージェントに提供された暗号化キーがなければ理解はできません。空気が（花粉等の）物質と（鳥のさえずり等の）オープン「シグナル」を運ぶといった、自然界にみられる受け手主導スキームに似たものです。保護されたデータまたはオープンデータを運ぶか、または破棄するか、個々のプロパゲータが偏った動作を行う場合もあります。

チャープ・アーキテクチャのセキュリティに関する隠れた利点として、エンド・デバイスへの終端間直接接続性がなく、プロパゲータは常にデータパスにあることが挙げられます。エンド・デバイスはプロパゲータ内の高度セキュリティ・アプリケーションの可能性があり、コンピュータ・ハッカーからは見えません。このアプローチは、暗号化や何万（または何億）というエンド・デバイスでのセキュリティを管理するより、はるかにシンプルで少ない予算で実現できます。エンド・デバイス自体に、セキュリティ・アプリケーションのための処理能力やメモリーといった負担を強いる必要がありません。小型、低能力、低品質、多量、そして安全です。MeshDynamics の軍用 OEM ライセンスにとって、セキュリティは明らかにカギとなる要素です。

## 基準について

基準の問題は、IOT デバイスのアドレス指定のためにユニーク MAC ID を必要とする、といった誤解を招く論理と同じ論理に悩まされています。私は著書の中でこの誤った考えを示唆しました。世界にはたくさん John Smith さんがいますが、私のアドレス帳に載っている John Smith さんは、（私にとっては）十分な特徴を持っており、個々にアドレス指定することが可能です。ローカルでの独自性があれば十分なのです。自然界も同じことでしょう。受け手主導メッセージングとの組み合わせで、長期に渡る「ブロードキャストの」嵐が花粉をばらまく際にも有効利用されます。花粉を運ぶ風は、広範囲ではありません。有効期限には本質的な制約があります。IP ネットワークでの同様のブロードキャストは機能が損なわれるでしょう。しかし個々のプロパゲータは、そのローカル・エンド・デバイスを、ネットワークから、およびネットワークに効率的かつ自動的に区分します。

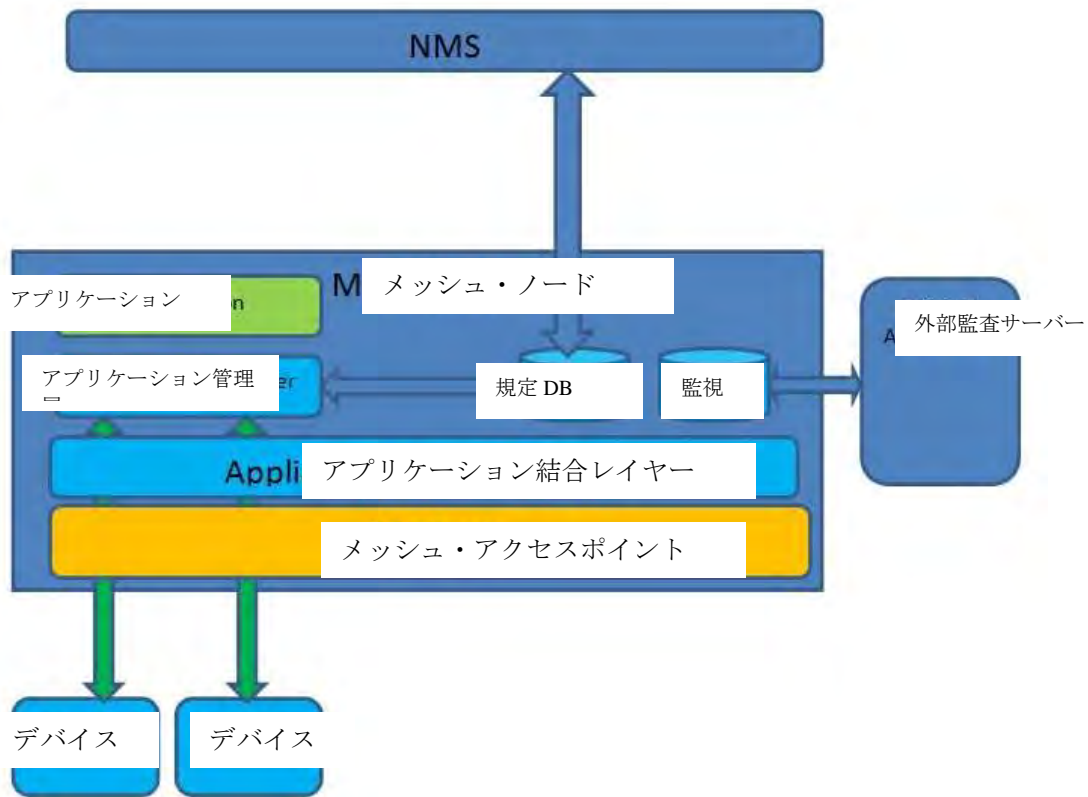


図 11 低レベルデバイス・プロトコル変換サービスのアプリケーション

プロパゲータは、基準の管理および IOT の普及加速にさらなる役割を果たします。個々のプロパゲータにはネットワークの「上位」要素に対して調整または定義されたアプリケーション・エージェントがありますので、様々なエンド・デバイスのためトランスレータとして機能することが可能です。チャープ・ベースまたは IP ベースのみならず、旧 M2M ネットワークにみられるあらゆる特別目的、基準ベースまたは独自のプロトコルなどがあります。プロパゲータ・ノードは、アドレス指定、制御タイミング、その他のデータ・ストリームの特徴を効率的に隔離および「なりすまし」を行います。繰り返しますが、アドレスは大域的に個別で一般的に理解できるものである必要はありません。プロパゲータ内のアプリケーション・エージェントが、あらゆる変換を処理する必要な知能を提供します。

プロパゲータ・ノード上の非常に広範囲な物理的インタフェース（有線、光学、無線等）の可能性に加え、これら変換能力は、基準の問題を緩和し、古いネットワークの IOT への迅速な移行を可能とします。

### 決定論的時間 IOT 試験

モノのインターネットとは、ある目的専用のマシンとその交流です。マシンは決定性有限オートマトン（DFA）における「状態」に基づいて作動します。インターネット「マシン」とはその一例であり、慣れ親しんだ「モノ」に加わるものです。

マシンは「ネットワークング」マシンによってその他のマシンに接続します。プロパゲータはビッグデータ・サーバーから芝生のスプリンクラーまで、マシンを 1 つのエコシステムに接続するものです。マシンのプロトコルやネットワーク・トポロジーについて、いかなる想定もしません。

しかし、マシンは定期的な入力を期待します。多くは、機能するための制御システムに等間隔での入力を必要とします。新たな IOT トレイン（シャトル）は、予定通りに走らなければなりません。

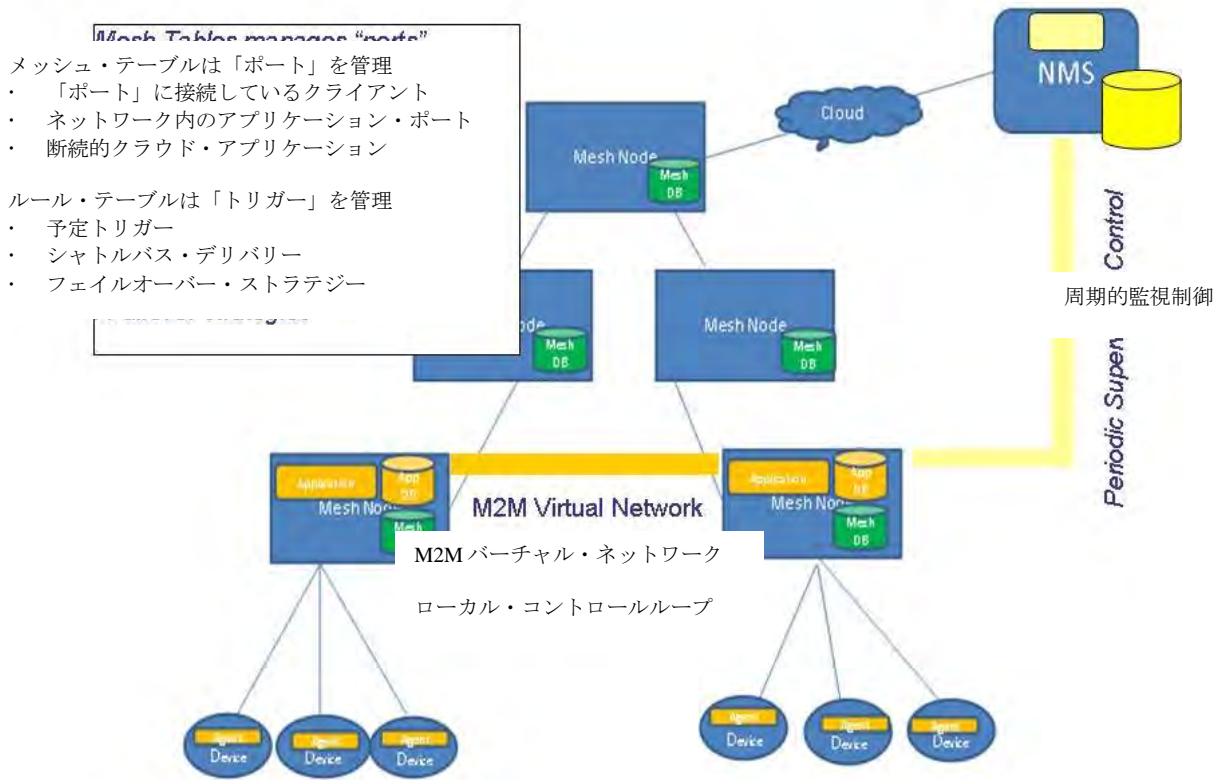


図 12 2つのレベルのコントロールループの同時管理

MeshDynamics は OEM パートナーとともに、上述したコンセプトの試験・調整を行うため、アブストラクテッド・ネットワークの試験台のプロトタイプを作成しています。プロパゲータと（オプションで）デバイスの両方においてアプリケーションを稼働させ、エンタープライズ・メッセージング・システムと通信します。アプリケーションは、公示通りに機能し、これらの「配線図」への変更は不要です。ネットワークのトポロジーに関係なく、タイムリーな配信を確認することが目的のフレームワークです。このフレームワークのアプリケーションのひとつは、遅延途絶耐性ネットワーク（DTN）です。

エッジデバイスの観点から、クラウドの接続が失敗した場合も、サービスの明らかな途絶はありません。フェイルオーバー・ルールが、デバイス管理をシームレスに引き継ぐため、メッシュ・ノード上でアプリケーションを起動します。クラウド接続が復旧すると、フェイルオーバー・サポートを提供しているアプリケーションは、クラウドの更新を行い、新たな処理指示を受けます。

耐故障制御システムの観点から、2つのコントロールループが常に稼働しています（図 12 参照）。1つはモバイル・エンド・デバイス（VOIP 電話等）へのシームレスな接続性を管理します。独自のプロトコルを使い、定期的で時間的制約のある Pub/Sub チャトル・サービスを活用して、メッシュ・プロパゲータ・ノードの情報を共有することによって、この管理が行われます。

クラウド管理の観点から、部分的にプロパゲータに置かれ起動している分散型リアルタイム・データベースがあります。このデータベースは、アプリケーションを「発射」する計画的な IF-THEN 「トリガー」を維持します。この時点で、ネットワークのマシンにはエンド・デバイス、プロパゲータ、アプリケーション、拡張型 Pub/Sub メッセージング・フレームワークのあらゆる部分が含まれることとなります。

ビッグデータのサブスクリバは、修正したトリガー、スケジュール、フェイルオーバー・ストラテジーによって、システム・レベルの挙動を調整することが可能です。これにはネットワークが行う原子タスクまで掘り下げ、提案および自動「調整」を提供する能力が含まれます。

オープンソース・フレームワークの使用は、ネットワーク内の全てのリソースのエンドツーエンド管理をクラウドに送るデバイスのためにこのフレームワークを使用するよう、OEM の関心を喚起します。



IOT デバイス製造者の観点から、ネットワークを管理するための DFA ベース・パラダイムの使用は、どこにアプリケーションをおく「べき」かについて OEM がモデルを作成し試験を行うことを可能にします。

また、よりシンプルなエンド・デバイスを利用可能とすることは、スマート・ネットワークの「スマート」が他のどこかに置かれていることを意味します。どれだけのインテリジェンスが必要か、ネットワークの何処にインテリジェンスを置くべきかは、以下のようにシミュレーションする必要があります。

### ダイナミック・スケジューリングおよびシミュレーション

ダイナミック・ネットワークにより、アプリケーションおよびデバイスのパフォーマンスを確実にするため、アブストラクテッド・ネットワークの「配線図」は、メッシュ・プロパゲータ・ネットワークによって常に見直されています。この見直しは、DFA 論理出力数の様々な段階において、ネットワークの置かれている調整・学習アルゴリズムによって自動的に提供されなければなりません。



図 13 エンドツーエンド・サービス・レベル契約を満たすためのダイナミック・スケジューラ

スケジューラが FIFO 順序を修正しますので、遅れる可能性のあるパケットのために他のパケットが適宜左右に移動します（図 13 参照）。左の図は、FIFO において累積される予想される待ち時間の小さな単位の増加を表しています（スタック参照）。右の図は、アプリケーションのデリバリー規定に基づいて、これをリアルタイムで軽減しています。

シミュレータ・スケジューラは、多種多様なカスタマー「ジョブ」スケジュールに基づいて稼働します。航空管制の基本原則がアプリケーション・スケジューリングに採用されており、「離陸」の前に親アプリが子アプリからの結果を待ちます。アルゴリズムが定期シャトルを運営し、「飛行機」に乗り遅れる「乗客」がないよう、シャトル・サービスのスケジュールを再要求します。アブストラクテッド・ネットワークは、エンド・デバイスとビッグデータ・インテグレータに対して透過的に、この内部スケジューリングおよび最スケジューリング全てを管理します。

## まとめ

歴史的相同コンピューティングおよびネットワーキング環境から大きく離れ、次世代のエンタープライズ通信は、レガシーおよび IOT アプリケーションが最終的にエンタープライズ・ネットワークに組み込まれるのに従い、より広範囲の多様なプロトコルとデバイスの統合が必要となります。これに反して企業は、エッジにおいてこれらの「モノ」を取り込むため、自社の SDN（ソフトウェアによるネットワーク）の機能の拡張を望むでしょう。

特に IOT において、小型、低能力、低品質、多量なセンサー、アクチュエータ、デバイスによる未来は、スケールの両端における再考が求められます。ネットワーク範囲の最も遠くの側においては、簡素なチャープがモノのインターネットの無数のエンドポイントの渉外コストを最小限に抑えるでしょう。

同時に、アブストラクテッド・ネットワークと強力なネットワークのコンセプトおよびプロパゲータ・ノード・デバイスに凝縮されるアプリケーション・ツールは、業界標準 SDN ツールおよび技術を拡張することによる、多様な要素を持つ巨大エンタープライズ・ネットワーク構築において、前例のない制御能力と柔軟性を提供します。

ネットワーク・アーキテクチャを完全に見直すことによって、モノのインターネットの力を余すところなく活用することが可能となります。MeshDynamics はその OEM パートナーと協働し、「モノ」の管理のためのマシン中心アブストラクテッド・ネットワーク・アプローチを研究しています。

## 筆者について

新たに出現したモノのインターネット・アーキテクチャと MeshDynamics のワイヤレス・メッシュ・ネットワーキング・プロパゲータ技術は、創業者 Francis deCosta のロボティックおよびマシン制御における経歴に影響を受けています。（MeshDynamics の初期のノードは、移動ロボットにインストールされました。）

Francis deCosta 氏は、かつて Advanced Cybernetics Group を設立。重要な役割を担うアプリケーションのためのロボット制御システムを提供していました。局所管理リアルタイム M2M 制御等を行うシステムです。その後 MITRE では、米国空軍ロボティックおよびオートメーション研究センター（RACE）のアドバイザーを務めました。

2012 年に Intel の支援により Rethinking the Internet Of Things (2013 年、Apress) を執筆。同書は Dr. Dobbs Journal の 2014 年の Jolt Award 最終候補になりました。