# IOT における精度の重要性

著者: Grainne Murphy、Colm Prendergast
Analog Devices, Inc.

モノのインターネット（IoT）とは、センサーやコントローラを搭載したすべてのデバイスをインターネットに接続したり、デバイスを相互に接続しようという概念に他なりません。これには、携帯電話、家電製品、自動車、機械、機械部品、ウェアラブル・デバイスなど、考え得るあらゆるものが含まれます。 しかし、IoTの原理は、クラウドに接続して広がる計測のシグナル・チェーンにすぎません。

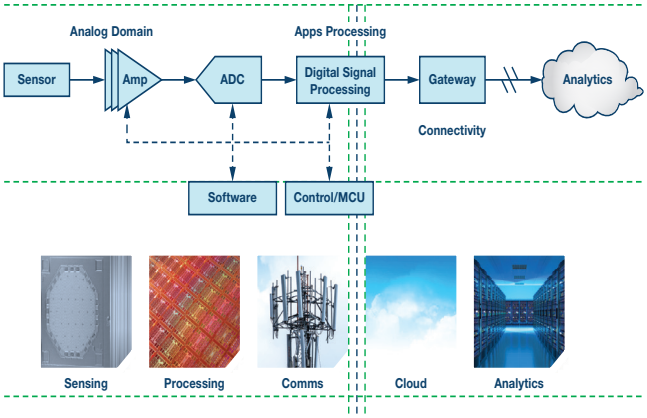


図 1. センサー TO クラウドのシグナル・チェーン

センシング部や計測部はアナログ信号をデジタルのデータ・ストリームに変換します。このデジタル・フォーマットは取得、処理、転送、解析が可能で、その結果に応じた決定をすることができます。このような、光、音、圧力、温度といった物理現象をデジタル・データに変換するという考え方は古くからあるものですが、IoT の発展は、デジタル・データに基づいてなされる決定を、メタパターンと計算モデリングを使用する決定へと一変させました。この手法はクラウドとその大容量ストレージおよび大規模な処理能力によって実現されます。温度計測技術のような昔ながらのセンシング機能の中には、スタンドアロンの計測としても、他の計測のための 1 要素としても十分に理解され、利用されているものがあります。例えば、電気化学センシングにおいて、温度は計測に影響を与えるため、この点を考慮することが必要です。また、最近、画期的なセンサーが開発され、これが IoT の世界に多大な影響を及ぼす可能性がでてきました。

その一例が MEMS 加速度センサーです。これらのセンサーは複数の軸で振動を検出する基礎をなすもので、ドローン、携帯ゲーム機、カメラなどのシステムを安定化させます。振動は、個人の健康を測定する健康測定機器にも利用されています。健康/フィットネス用ウェアラブル・センサーは、常時オンにして、ランニング、サイクリング、ウォーキングなどの際に身体の動きを高い精度で検知する必要があります。検知されたデータは解析され、さまざまな携帯用の健康/フィットネス・アプリケーションにリアルタイムで送信されます。

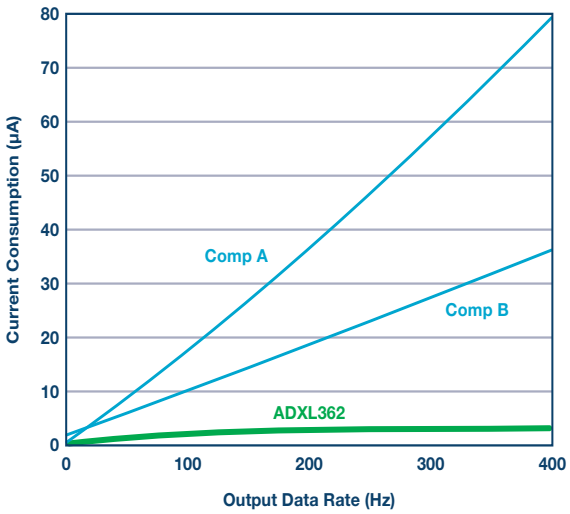


図 2. 業界で最も低消費電力の MEMS 加速度センサー

加速度センサーを例にとると、IoT デバイスに何を期待すればよいでしょうか？また、より正確な測定にどのような価値があるのでしょうか？まず、低消費電力を考慮します。アナログ・デバイセズの ADXL362 は超低消費電力の 3 軸 MEMS 加速度センサーで、その消費電流は、100 Hz の出力データ・レートでは 2 µA 未満、モーション・トリガのウェークアップ・モードでは 270 nA です（MEMS 加速度センサーは加速度の静的な力または動的な力を計測するものです）。これによりバッテリの長寿命化が可能となります。次に、帯域幅と分解能を考慮します。ADXL362 では、アンダーサンプリングによる入力信号の折返しはありません。すべてのデータ・レートでセンサーの全帯域幅をサンプリングし、しかも低ノイズです。これにより、最小の信号でも計測可能となります。

ADXL362 の通常の 550 µg/Hz よりも低いノイズ・レベルが求められるアプリケーションでは、電源電流の増加を最小限に抑えつつ、175 µg/Hz（代表値）までノイズを低減できる 2 つの低ノイズ・モードを選択できます。

## データ品質向上の重要性

しかし、このような高精度計測にどのような価値があるのでしょう？そしてなぜそれが重要なのでしょうか？低ノイズ、低ドリフト成分によってセンサー能力が向上し、ダイナミック・レンジを拡大できます。これにより、さらにさまざまな微小信号をこのハードウェアで計測できるようになります。これにより、エンド・システムは、さらに正確で感度が高く、差別化されたものになります。精度が向上することで、現在および未知の計測ニーズにも対応でき、将来に対するガード・バンディングができるプラットフォーム・ハードウェアの開発が可能となるのです。

このために、同じハードウェアを何世代もの製品に使用することができ、特にハードウェアの交換は困難で費用がかかることから保有コストを低減できるという付随効果も得られます。このことは特に IoT について言えますが、それはセンサーとそれに付随するハードウェアの数が爆発的に増加すると見込まれるからです。アナリスト企業の Gartner によれば、2020 年までに接続されるデバイスは 260 億台を超える見込みです。これは相当な接続数です。さらに、ワイヤレス接続の利点により、IoT のシグナル・チェーンでの使用が進むにつれて、各種ユニットは次第に工場のような人の手の届きにくい過酷な環境に置かれるようになります。最後に、もう 1 つ考慮すべき要素として、排ガス、電力使用量、環境制御を含む複数の市場にわたって政府の規制がますます厳しさを増すことが挙げられます。計測システムの向上によって将来を先取りしようとする考えが生まれ、既存のハードウェアのままでさらに高精度な測定を求めるこうした新たな規制や規制変更に対応できるようになるのです。将来の新たな計測ニーズに応えられるか否かが、熾烈な競争が繰り広げられる IoT 市場で生き残る分かれ道となるでしょう。

したがって、安定した高精度のハードウェア計測プラットフォームの重要性は強調し過ぎることはありません。そのようなプラットフォームを導入すると、ソフトウェアによりシステムの差別化を図ることができます。IoT では、このような能力こそが競争市場において企業が自社をいっそう差別化できる領域であることが判明しつつあります。また、いかなるシステムもアップグレードがさらに容易で単純になり、リアルタイムで可能となります。

## 正当なデータの真の重要性

正当なデータが IoT エコシステムの中で確実に維持されるためには、考慮すべき要因が多数あります。モノのインターネットとは「モノ」からクラウドに至るまでに存在する数多くのレイヤであると説明できます。各レイヤには新しい外部接続とそれに伴うセキュリティ・リスクが存在する可能性があります。また、各レイヤを通って「モノ」まで戻るパスもあり得ます。それはデバイス、ネットワーク、クライアントに関することだけではありません。関連する側面をもつ領域は多数あり、それぞれが相互に接続される可能性があります。例えば、デバイスからクラウドへ、またはデバイスからゲートウェイを経てクラウドへ、といったようにです。正当性を求めるのは、レイヤごとのセキュリティを確保するためです。接続するモノ、クラウド、ゲートウェイが増えるにつれて、セキュリティ上の欠陥になりやすい場所も増加します。

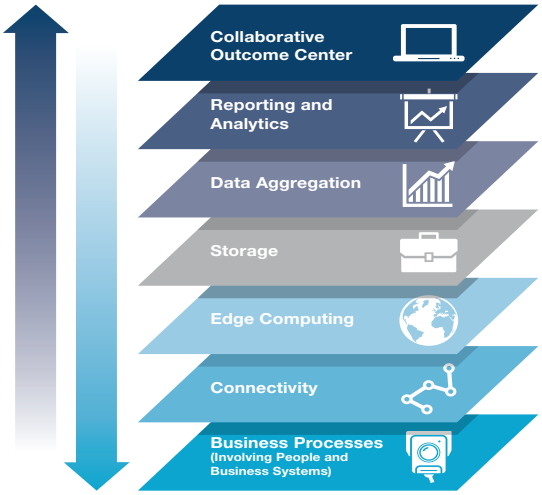


図 3.

OWASP（Open Web Application Security Project）では、IoT のセキュリティ脆弱性の上位 10 項目を次のように分類しています。

- セキュリティが確保されていないwebインターフェース（XSS、インジェクション、フィッシング）
- 不十分な認証と認可
- セキュリティが確保されていないネットワーク・サービス（SSH、SFTP、Telnet）
- 暗号化されていないトランスポート
- プライバシーの問題と懸念
- セキュリティが確保されていないクラウド・インターフェース
- セキュリティが確保されていないモバイル・インターフェース
- 不十分なセキュリティ設定能力
- セキュリティが確保されていないソフトウェア/ファームウェア
- 貧弱な物理的セキュリティ

クラウドでは、セキュリティ脅威はデータ漏洩として現れることもあれば、偶発的データ損失やデータ盗難として現れることもあります。クラウド・サービスが複数顧客にサービスを提供する（マルチテナント）ことは間違いないため、サービスには顧客同士を確実に分離する必要があります。その場合、考慮すべき問題が新たに生じます。オンラインをローカルに維持するときや、データ破壊の可能性がある場合、システムの可用性はどうなるでしょうか？データは複数の場所でどのように共有され、セキュリティが確保されているのでしょうか？また、どのようなセキュリティ基準が設けられているのでしょうか？データは、特に IoT によりデータ量が激増する場合に、バックアップ可能でしょうか？アプリケーション・プログラム・インターフェース（API）は複数の顧客向けに同じクラウド・サービスで開発され保存されることになります。このため、認証と認可の方法が（管理者のような権限のあるユーザを保護する方法とともに）重要です。

クラウド・サービス・プロバイダを検討し評価する方法は多数あります。1 つは、公開されているセキュリティ・ガイドラインを使用する方法です。これらのグローバルなクラウド・ガイドラインは絶えず強化されており、サービス・プロバイダには、これらに適合するとの認定を受けることがますます求められるようになります。

しかし、セキュリティ上の懸念はクラウドに限定されません。スタックのレベルごとに、関連する脅威と対策法があります。物理的な IoT デバイスやゲートウェイが盗まれたり手を加えられたりすることや、データが権限のないユーザによる操作やアクセスを受ける可能性があります。この場合、対策として改ざん検出器、暗号化、デバイス登録などが用いられます。ソフトウェアやファームウェアは、フィッシング、マルウェア攻撃、改ざんの標的となる場合があります。このため、信頼できる OS、開発ライフサイクルへのセキュリティの組込み、脆弱性試験が必須となります。ソフトウェアを実際に組み込んだ後、これを安全に更新する仕組み作りも重要です。データのトランスポート時、チャンネルのセキュリティが確保されていないと、改ざん、盗聴、攻撃を許容する可能性があります。この場合、暗号化したトランスポート・チャンネル、ポートやインターフェースの管理、継続的なプロアクティブ・モニタリングがきわめて重要です。データ・プライバシーについては、顧客から特に高い信頼を得る必要があります。侵害がどんなに些細なものでも、企業ブランドや評判が損なわれてしまうことがあります。そのため、保存データやデータ保持を最小化または難読化するデータ暗号化方式のような優れた手法を用いることが重要です。世界のプライバシー・データ保護政策は絶えず進化し変化しています。世界のさまざまな地域での規制の違いに対応できる柔軟なシステムを保持することが重要です。アプリケーション・レベルでは、権限のないアクセスを阻止するためにユーザの認証と認可を行うだけでなく、脆弱性を発見するためにコードを継続的にテストします。さらに、WAF（web application firewalls）や攻撃を受けたアカウントを隔離しロックアウトする機能のような、アウト・オブ・バンド保護についても検討します。今日の対策はすべて適用可能ですが、セキュリティをエコシステムに組み込み、末端で改造されないようにする必要があります。

## インテリジェント接続の IoT システム

インテリジェンス（データ処理）は、IoT チェーンのどの段階でも追加できます。例えば、バイタル・サイン・モニタリング（VSM）で、体温が危険レベルにあるという警告をセンサーから直接即座に発することができる場合、体温データをクラウドに送信する必要はありません。ただし、同じ温度が他の生体医学データの計算にも使用される場合があるので、ゲートウェイやクラウド内で同様に使用することも可能です。

信号処理がノードで発生する場合は、緊密に統合された帰還制御ループを使用可能なことを含め、いくつか利点があります。センサーやアクチュエーターを緊密に結合させる利点は、即座に決定がなされることです。例えば、振動が設定されたレベルに達したら直ちに機械やモーターの電源を切ったり、温室の温度が上昇したらモーターが起動して窓を開けることが可能です。ノードでは、フットプリントを小さくし、バッテリ寿命を延ばすために消費電力を最小にすることが求められますが、統合化されたアナログ・マイクロコントローラのような部品でこうしたニーズを実現することができます。そのような部品の例として、ARM® M3-MCU と 24 ビット A/D コンバータを組み合わせたアナログ・デバイセズの ADuCM360 があります。将来的には、エナジー・ハーベストを利用可能な、エネルギーに依存しないデバイスがここでの成功の鍵となります。ノード処理の限界は、まさにスペースと電力の限界です。さらに、他のソースからのデータを集約することも困難です。ノードが低消費電力であると、データの送信範囲やペイロードが制限を受けます。ステータスをモニタしてアップグレードを実行するためのノード管理が困難なため、それに伴うネットワーク・エッジでの物理的、ソフトウェア上、データ上のセキュリティ・リスクが生じます。

ゲートウェイ・ベースの信号処理では、短距離のワイヤレス・センサー・ネットワーク（WSN）リンクを一方の側に、LAN リンクまたは WAN リンクを他方の側に置いた IoT ゲートウェイ・デバイスを使用します。これはルーターに類似しており、センサー・ハブにすることもできます。WSN のネットワーク管理とセキュリティ機能に加え、ローカルでの処理と解析（一般にエッジ・コンピューティングとして知られる）用の計算リソースとしてもよく使用されます。ゲートウェイ・ベースの処理の利点は、大規模になる可能性のある処理リソースを使用できることと、他のセンサーやソースからのデータを集約できることす。したがって、ネットワーク・エッジの近くで解析を実行でき、市販の開発ツールを使ってその解析を開発できるので、より IT フレンドリーなソリューションが生まれます。このソリューションはフル・スタック OS に対応する可能性を持ち、（物理的なセキュリティはリスクにもなりますが）セキュリティの優れた標準的なリモート管理ツールで LAN/WAN ネットワーク技術を使用します。一方で、通常は低消費電力でなく、有線電源を必要とし、データ・ストレージにも制限があります。

したがって、クラウド接続の鍵となる利点の 1 つは、履歴データを含む大規模なデータ記録や多数のデバイスからのデータを保存、読出し、検索できることです。クラウドベースの信号処理では、多くの場合、データ・ストレージがビッグ・データの処理と解析に密接に結び付いています。これは、データを保存するだけのものではありません。データを素早く読み書きし処理する必要性がイノベーションを生み出し、オープン・ソース・フレームワークによる簡単なプログラミング・モデルを使って大規模なデータ・セットをコンピュータ・クラスタ間で分散処理する、多くの新しい方法をもたらしました。クラウドベース処理の明らかな利点は、セキュリティが組み込まれた潜在的に非常に大きな計算リソースとストレージ・リソースです。オープン・ソース開発ツールや商用開発ツールの種類は多く、増え続けており、エンド・ソリューションも容易に拡大する可能性があります。

サービスとしてのソフトウェア（SaaS）は、現在、サービスとしてのインフラストラクチャ（IaaS）、サービスとしてのプラットフォーム（PaaS）、サービスとしてのデスクトップ（DaaS）、サービスとしてのモバイル・バック・エンド（BaaS）、サービスとしての IT 管理（ITMaaS）とともに、クラウド・コンピューティングにおいてきわめて重要な商品と考えられています。これらを合わせると、エンド・システムのニーズに応えるさまざまなオプションになります。クラウドベースの処理では、サーバ・ホスティングが必要です（オン・プレミスとリモートがあります）。ストレージとサービスには関連コストがあり、それが通信と大規模データ・ストレージでは高額になる可能性があります。この他の問題として、インターネット通信のチャンネルがあり、このチャンネルでは遅延とスループットの予測がつかないことがあります。

IoT システムの進化に伴い、スマート・システムのパーティショニングも進化し、ノードでのインテリジェンスがいっそう進みます。ノードでは知恵や知識を生まないということは、データはクラウドに到達するまでデータのままであることを意味します。これでは全データを変換し送信するために大量の電力を消費し、帯域幅を集中的に使用することになります。インテリジェント・スマート・センシングでは、ノードにおいてデータを情報に変換することで、全体の消費電力を低減し、遅延を縮小し、帯域幅の無駄を減らします。つまり、後手対応の IoT から予測的で即応的な IoT に変わることができます。

優れたIoT設計のための課題は、十分な測定、セキュリティ、IoTの全パスにおけるインテリジェンスの効果的な使用場所の見極めなど、数多くあります。また、センサー、ゲートウェイ、ソフトウェア、ストレージ・プロバイダのIoTソリューション全体に、複数のベンダーが存在することがあります。アナログ・デバイセズでは、リムリック工場で（温度と湿度を測定する他のセンサーに混じって）当社のADXL362加速度センサーが製造装置の監視に使用されており、当社はIoTのベンダーであり顧客でもあります。機械やモーターからの振動パターンの変化を計測することで、システムがダウンする前に故障を検知できます。これには、予測的なメンテナンス・プログラムを実施できるという利点があるため、工場の効率と生産能力が向上します。当社がIoTを実装したことにより、複雑な製造工程内の複数の機器（多数のサプライヤからの新旧さまざまなもの）にわたって全てをモニタリングし解析するシステムが実現しています。このシステムが、効率をリアルタイムに追跡して報告し、システムがダウンする前に、起こり得る問題を技術者に警告します。これによりウェーハの歩留まりが向上し、顧客が目標とする条件に応じたより定期的な供給が可能となるため、顧客の計画改善に役立っています。この例は、IoTシステムの真の価値を実証しています。IoTシステムの高度さと適用範囲から、多くの信号処理オプションを実行できます。IoTシステム内の処理をクラウドからエッジに移すと、センサーのいっそうのスマート化とソースにより近い情報の抽出が可能となります。ネットワークのエッジ・ノードやゲートウェイ上、またクラウド内に有用な処理リソースがあれば、システム設計者はエッジ・ノードの消費電力、データの帯域幅、計算、ストレージの諸条件を考慮してソリューションを最適化することができます。

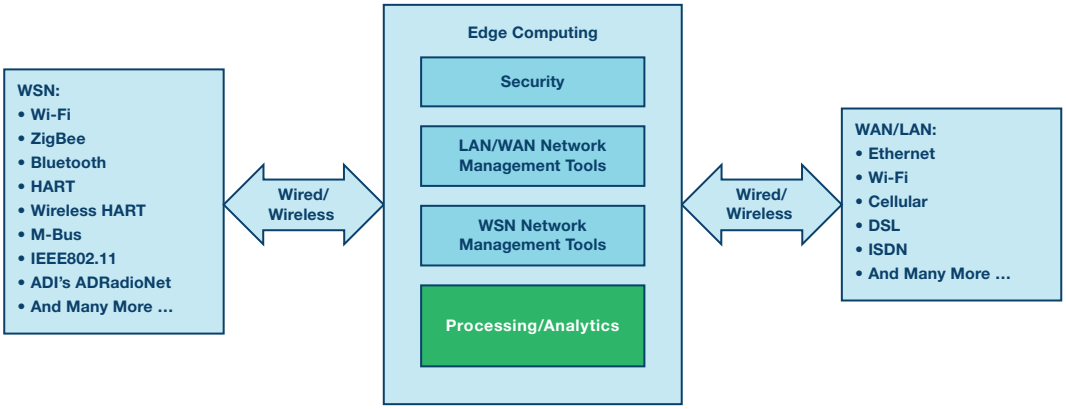


図 4. IoT ゲートウェイの一例

## 著者について

Grainne Murphy は、アナログ・デバイセズのIoT市場担当マネージャです。リムリック大学で工学の学位号を、オックスフォード・ブルックス大学で経営学の修士号（MBA）を取得しています。

Colm Prendergast は、アナログ・デバイセズの IoT クラウド技術担当の主席エンジニア兼ディレクタです。アナログ・デバイセズには、1989 年、アイルランドのリムリックで設計エンジニアとして入社。デジタル・ビデオ、オーディオ、通信、DSP、MEMSなどの幅広い分野に従事し、プロジェクトを率いてきました。11 件の米国特許を保有し、IEEE とSIGGRAPH の会員です。Colm はマサチューセッツ州ブライトンのセント・ジョセフ・プレパラトリー高校の評議委員会のメンバーで、FIRST ロボット・コンテストのアドバイザーです。アイルランドのリムリック大学で電子工学の学士号を、アイルランドのユニバーシティ・カレッジ・コークで修士号を取得。

## オンライン・サポート・コミュニティ

当社のオンライン・サポート・コミュニティで、アナログ・デバイセズの技術専門家と連携することができます。設計上の難問について問い合わせたり、FAQ を参照したり、話し合いに参加することができます。

engineerzone®

*ez.analog.com*

＊英語版技術記事はこちらよりご覧いただけます。

**アナログ・デバイセズ株式会社**

本　　社 〒105-6891　東京都港区海岸1-16-1　ニューピア竹芝サウスタワービル10F
大阪営業所 〒532-0003　大阪府大阪市淀川区宮原3-5-36　新大阪トラストタワー10F
名古屋営業所 〒451-6040　愛知県名古屋市西区牛島町6-1　名古屋ルーセントタワー40F



TA14507-0-08/16

*www.analog.com/jp*

ANALOG DEVICES
想像を超える可能性を
AHEAD OF WHAT'S POSSIBLE™