# SensorCorpus®のコンセプト

## ～The Concept of SensorCorpus®～

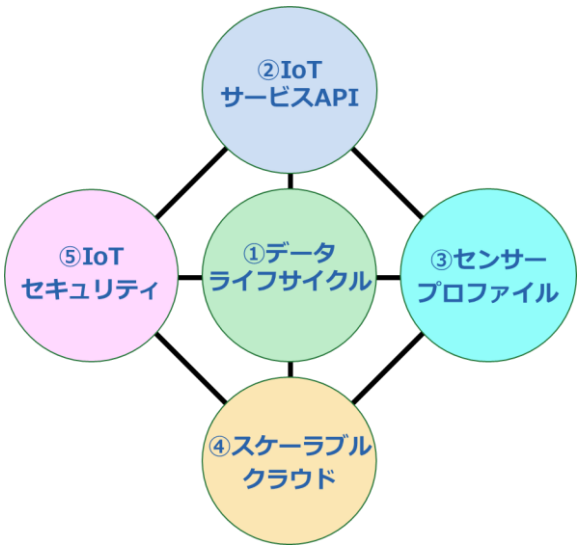
2015 年 9 月 1 日
Rev1.0

## 1. SensorCorpus®とは

SensorCorpus®はセンサーデータの収集、保管、表示、分析、通知を行うクラウド型の IoT サービスプラットフォームです。既に機械（稼動部）の劣化検知、工場の温度・湿度管理、音響計測、屋内・家電の状態監視（ドアの開閉、温度、商品個数、人感）等の場面で利用されています。今後はさらに下記のような業種・分野への展開・適用を進めていきます。

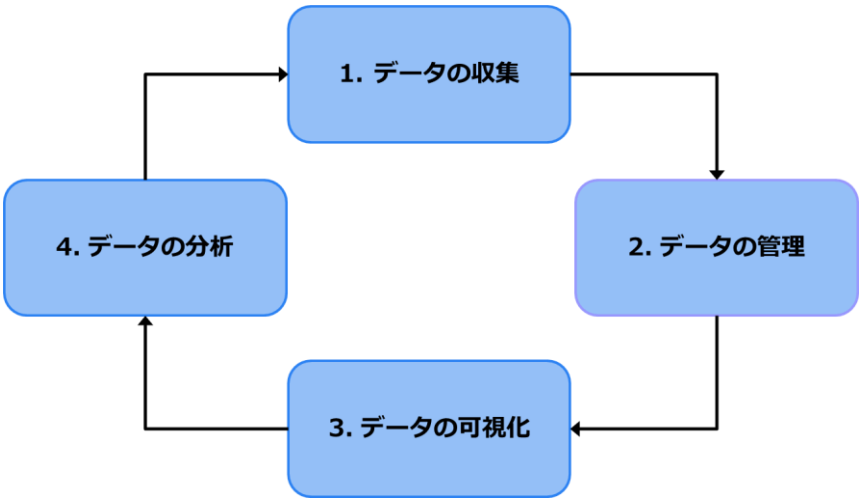

## 2. SensorCorpus®の設計コンセプト

SensorCorpus®は、データライフサイクル、IoT サービス API、センサープロファイル、スケーラブルクラウド、IoT セキュリティの５つの設計コンセプトに基づいて開発されています。データの収集・管理・可視化・分析（評価）の一連のサイクルであるデータライフサイクルを中心に据え、その他４つのコンセプトを軸に IoT サービスプラットフォームを実現しています。



### （1）データライフサイクル

IoT データをはじめとするビッグデータから有用な知見を得るためには、データの収集、管理、可視化、分析（評価）という一連の流れである「データの PDCA サイクル」を回し、仮説と検証を行っていくことが重要です。具体的には、センサーを使用して必要とするデータを適切なタイミングで取得し、その取得データをもれなく、効率的に格納管理し、さらに人が理解できる形で様々な軸から可視化すると同時に、適切なアルゴリズムを用いて分析・評価を行うというサイクルを繰り返す流れになります。SensorCorpus®はこのサイクルを効率的に回すよう設計されています。




### （2）IoT サービス API

ネット時代においてはサービスが相互に API を通じてデータ連携をすることで、それぞれのサービスの付加価値が高まります。また、API の公開はデバイス側のソフトウェア開発者の生産性向上に有効です。SensorCorpus®ではデータ入出力、ダッシュボード、分析、通知、オープンデータ連携、制御等 IoT サービス活用のための様々な API を提供します。将来、API の公開を通じて積極的にオープンイノベーションを推進していきます。


### （3）センサープロファイル

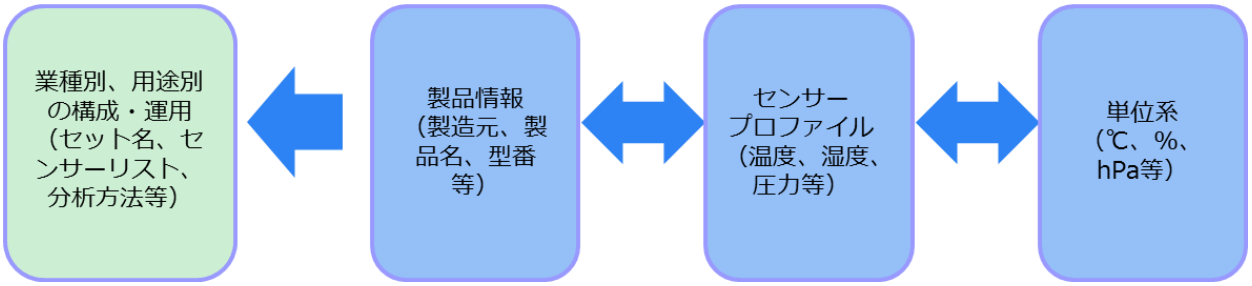
各メーカーで製造されているセンサーの種類は多種多様で、その仕様、属性情報等のメタデータの標準化が細部まで十分になされていません。IoT のシステムを構築するためには、センサーの比較選択は避けて通れず、センサーの仕様、属性情報等のカタログの標準化、一元化は利便性に直結します。

そこで SensorCorpus®ではユーザーの利便性と IoT の普及を促進させるため、「センサープロファイル」として世界中にあるすべてのセンサーのメタデータの管理、カタログ化を行っていきます。

この「センサープロファイル」の仕組みを用いて、環境要件、求められる測定精度、電源の取りやすさなどに応じて適切なセンサーを選択できるようにします。

一方、IoT ソリューションという観点では、センサーの選択で完結することはなく、センサーに合ったゲートウェイの選択、データの容量や測定頻度等に応じたサーバやクラウドの設計、データに合った分析アルゴリズムの選定、システム全体を通してのセキュリティレベルの設計や運用の手順なども合わせて考慮する必要があります。

SensorCorpus®では、センサーのプロファイル技術を起点として、ゲートウェイ、クラウド、分析アルゴリズム、セキュリティ、全体の運用手順などを、業種・用途別にパッケージ化することで、様々な適用領域において最適な IoT ソリューションを提供する仕組みを構築することを最終目標としています。

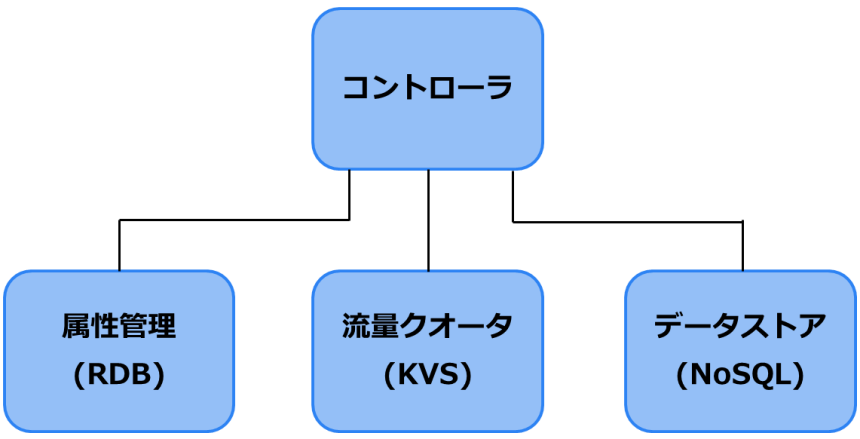



### （4）スケーラブルクラウド

IoT のシステムではセンサーやゲートウェイ等のデバイスの管理とともに、様々なセンサーから日々発生する大量のデータをどのように取り扱うかという問題が生じます。すなわち、測定データ形式が多種多様で、一律的なスキーマで対応できない大量のデータを高速かつ確実に処理する必要があります。

これらの課題を解決する手段として、近年注目されているのが、KVS(Key-Value Store)や NoSQL(Not only SQL)と呼ばれる新しい技術です。

SensorCorpus®では、大量で高頻度、かつ保全性が求められる測定データのストアとして、シャーディングやレプリケーションを駆使した NoSQL である MongoDB や Cassandra を採用しています。また、高速性が求められるゲートウェイ認証や流量クオータ制御には KVS として安定した評価を得ている Redis を、センサーやゲートウェイなどの属性管理には従来型の RDB を採用しています。そして、全体のコントローラとしてイベント駆動型の nodejs を採用し、確実なスケーラビリティと、かつ将来にわたってシステムを持続的に成長させることができる構成になっています。



### （5）IoT セキュリティ

IoT におけるセキュリティは従来の IT セキュリティに加え、IoT 特有のセキュリティを考慮する必要があります。さらに今後、生体情報を始めとして個人のプライバシーに係わる情報を扱う場合も多くなることが予想されます。IoT が直面する課題をまとめると下記になります。

① **セキュリティ**
センサーやゲートウェイの盗難、乗っ取り、詐称、盗聴などへの対応

② **プライバシー**
生体情報や位置・移動履歴など機微な情報の安全性の確保

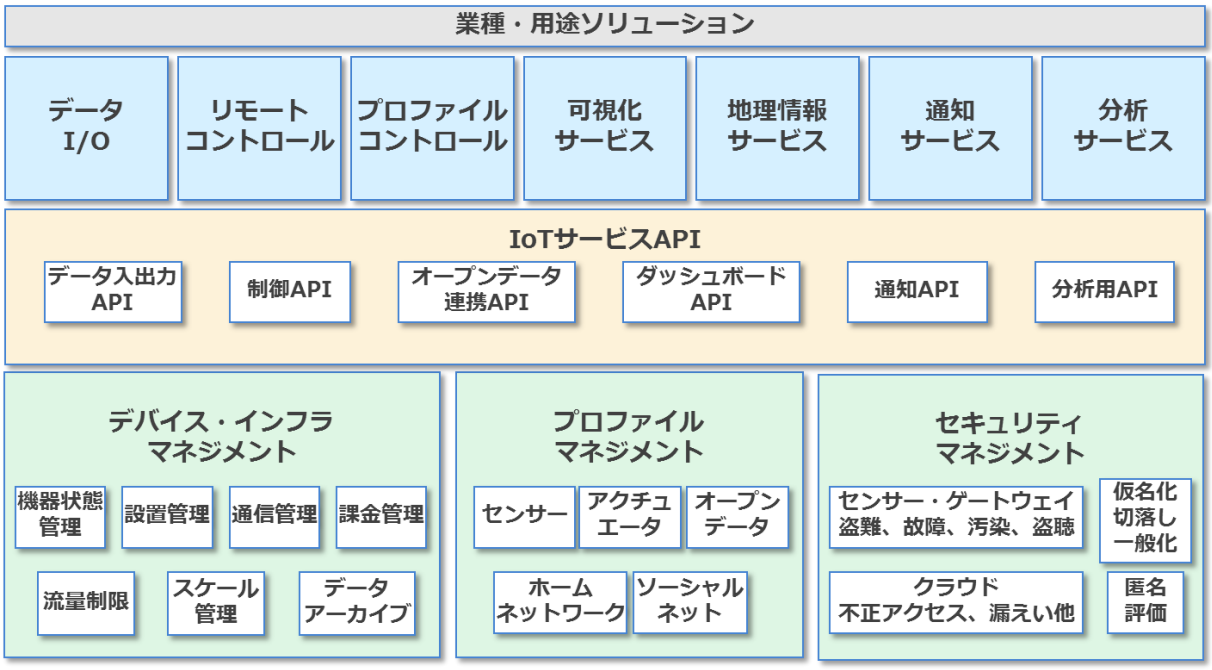
SensorCorpus®では上記の課題を解決するため、センサー、ゲートウェイからクラウドまでを包括的に捉え、IoT データの収集、管理、可視化、分析に至る一貫したセキュリティ技術とプライバシー強化技術(Privacy Enhanced Technology)を用いてセキュリティマネジメントを行います。

セキュリティについては、センサーやゲートウェイの故障や不具合検知、不正な動作をしていないかのマイニング技術等に注力していきます。

プライバシーについては、プライバシーに係わる多種多様なデータの安全な形での二次利用、データそのものを取引するビジネスの出現を念頭に、データを匿名化するためのモジュールを提供することで、二次利用や統計情報としての公開に対応していきます。さらに、今後はこれら加工データの匿名安全性の評価の仕組み作りにも取り組んでいきます。

## 3. SensorCorpus®のテクノロジーフレームワーク

最後に、上記の設計コンセプトに基づき構築された SensorCorpus®のテクノロジーフレームワークを以下に示します。




※実装されている詳細な機能については「SensorCorpus®の特徴」をご参照ください。