報道関係者各位
プレスリリース

平成 27 年 6 月 16 日
株式会社インフォコーパス

# インフォコーパス、プライバシー保護やセンサーのなりすましの防止で安心安全な IoT を目指す「IoT セキュリティフレームワーク」を発表

IoT(*1)事業を手がける株式会社インフォコーパス(本社:東京都渋谷区、代表取締役社長:鈴木潤一、以下インフォコーパス)はプライバシー保護やセンサーのなりすましの防止で安心安全な IoT を目指す「IoT セキュリティフレームワーク」を発表しました。7 月 1 日の SensorCorpus(センサーコーパス)(*2)サービスリリース後、順次実装して参ります。

現在、様々な機器がネットにつながる IoT が普及し始める中、それに対するセキュリティとプライバシーへの不安も高まっています。とりわけ IoT 固有のセキュリティ問題として、センサー、ゲートウェイの盗難、データ汚染、なりすまし、乗っ取りなどの脅威が浮上しています。また、プライバシー面でも、センサーが一般家庭やオフィス、都市空間、ヘルスケア分野等に広がるにつれ、個人の特定や個人属性推定が可能なデータを拾ったり漏洩したりするリスクが高まります。こういったセキュリティとプライバシーの不安を解消・軽減することが、IoT 普及の最大の鍵となります。

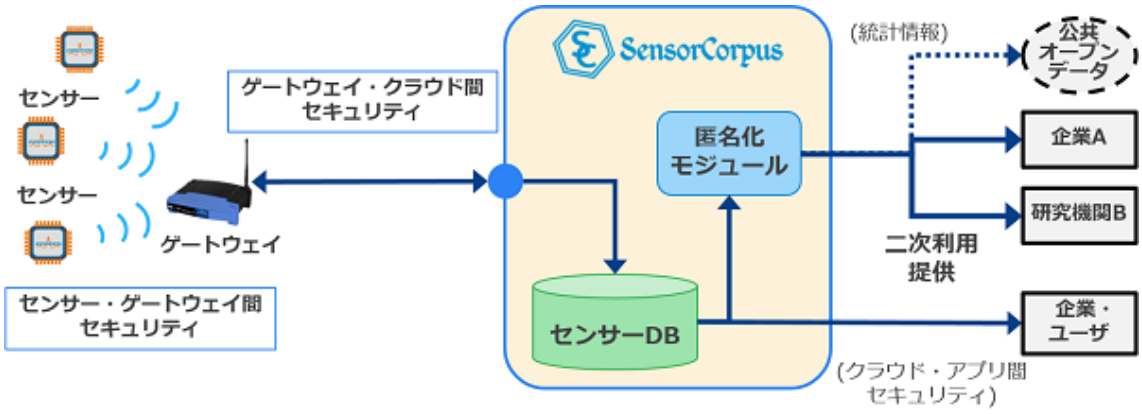
今回インフォコーパスでは、これらの問題を解決するための「IoT セキュリティフレームワーク」を構築いたしました。特徴はセンサー、ゲートウェイ(*3)、クラウドを結び、IoT データの収集、管理、可視化、分析に至るまで、一貫したセキュリティ技術とプライバシー強化技術(*4)を含む以下の三点です。

(1)　センサーの死活監視・データ汚染等の監視技術の導入
センサーとゲートウェイ間のセキュリティ対策として、センサーの死活監視を行うことで、センサー、ゲートウェイの故障・盗難を早期発見します。またセンサーID の識別監視により、センサーデータの汚染も発見します。

(2)　センサー、ゲートウェイの詐称等の発見技術の導入
ゲートウェイとクラウド間のセキュリティ対策として、ゲートウェイ認証を行うとともに、詐称マイニング技術を活用して、センサー、ゲートウェイのなりすまし、乗っ取りを発見します。

(3)　匿名化技術(*5)の活用によるプライバシー保護の強化
クラウドに蓄積された IoT データの活用に際し、匿名化技術を用いることで個人のプライバシーを保護します。個人情報の仮名化、属性の切り落とし、曖昧化等の匿名化処理を実行し、特定個人の識別や個人属性の推定リスクを軽減しつつ、分析や再利用向けのデータを加工、生成できます。

インフォコーパスは今後も IoT 化を推進し、快適で安全な社会の実現に貢献してまいります。



IoTセキュリティフレームワーク

【注】

(*1) IoT：Internet of Things の略。モノのインターネット。コンピュータなどの情報機器だけでなく、全てのモノにセンサーと通信機能が実装され、インターネットを介して情報交換や制御ができる仕組みを指す。類似した概念に M2M(Machine to Machine)等がある。

(*2) SensorCorpus:インフォコーパスが開発した、簡単・安価・セキュアなクラウド型 IoT サービスプラットフォーム。様々なセンサー情報をクラウド上に収集し、管理、可視

化、分析することができる。既にデバイスメーカーや商社等を中心に、冷蔵庫の温度管理、ドアの開閉管理、タッチセンサーによる商品個数管理、消耗材の劣化検知、音響・振動計測、ロボットによる環境情報収集、位置データのマッピング等に利用されている。

(*3) ゲートウェイ:データ通信の中継機器。複数のセンサーから発信されたデータを中継してクラウドまでつなぐ役割を果たしている。

(*4) プライバシー強化技術:Privacy Enhancing Technology(略称 PET)の訳語。個人情報の不正な収集、利用、開示を防止し、個人情報を個人が管理出来るような、プライバシー保護強化のための情報通信技術。

(*5) 匿名化技術:データに含まれる個人特定可能な情報を、匿名化という手法を用いて曖昧化する技術。仮名化、属性の切り落とし、希少データ排除に用いる K-匿名性や l-多様性等、様々な技法がある。

【本件に関するお問い合わせ】

株式会社インフォコーパス
担当：近藤
Tel：03-6416-1365
Email：contact@infocorpus.co.jp
URL：http://infocorpus.co.jp