

OS の最新動向

本田 雄亮, 山下 大輔

Yusuke HONDA, Daisuke YAMASHITA

1 はじめに

OS とは基本ソフトウェアとも呼ばれ、ハードウェアの管理・制御を行う。OS が持つ最も重要な役割は「ハードウェアの抽象化」であり、全てのハードウェア上で同じ基本機能を提供する仕組みである。これにより、ハードウェアとアプリケーションソフトの開発が容易になる。

現在、OS はパソコンやスマートフォン、タブレットなど様々な端末に搭載されている。その中でも近年、特に注目を集めているのが IoT 向け OS である。IoT 向け OS は「スマートウォッチ」や「スマートホーム」など、IoT への関心の向上を背景に注目されている。Google や Apple, Microsoft などの大手 IT 企業も IoT 向け OS の開発を発表している。

2 IoT 向け OS

2.1 IoT 向け OS の概要

IoT 向け OS とは IoT 端末に組み込まれる OS である。既に多くの IoT 端末が存在しているが、それらの機能は各社独自のシステムで開発されており、他社製品との互換性は無い。今後、他社製品も巻き込む大きなネットワークを構築するには、IoT 対応端末開発と他社端末間通信の容易化が必要である。これらの課題を解決するために IoT 向け OS の開発が進んでいる¹⁾。IoT に OS を搭載するメリットは以下の 3 つである。

- 様々なハードウェアの基本機能を一様に実装
- 他社端末間通信の容易化
- アプリケーションソフト開発の簡素化

IoT 向け OS では、ハードウェアに依存せずに、通信や制御などの基本的かつ汎用的な機能を提供する。よって、IoT 端末を開発する際、それら基本機能を実装したプログラムを作成する手間を省き、開発コスト削減に繋がる。

IoT では、複数の端末同士が通信を行い情報共有・制御を行う。OS を搭載することで制御・通信機能の実装が可能であり、規格を統一できる。すなわち、メーカーが異なるハードウェア同士でもスムーズな制御・通信が容易となる。

アプリケーションソフト開発においても、OS の提供する基本機能を利用することで開発工程を簡素化できる。さらに、ハードウェアの差異にとらわれないソフトウェア開発が可能である。家具や電化製品、自動車など多種多様なハードウェアに搭載される IoT 向け OS では、ハードウェアに依存しない性質が重要である。

現在使われている IoT 端末は OS を搭載しておらず、メーカー独自のシステムを開発している。よって、端末ごとに一から専用のソフトウェアを開発する必要がある、開発

コストが高くなる。さらに、端末によってシステムの仕様に差異があるため、他社端末間での通信が容易ではなく、専用のアプリケーションソフト開発が必要である。したがって、これら既存問題の解決が可能な IoT 向け OS の開発が進んでいる。OS と IoT 端末の関係性を Fig. 1 に示す。

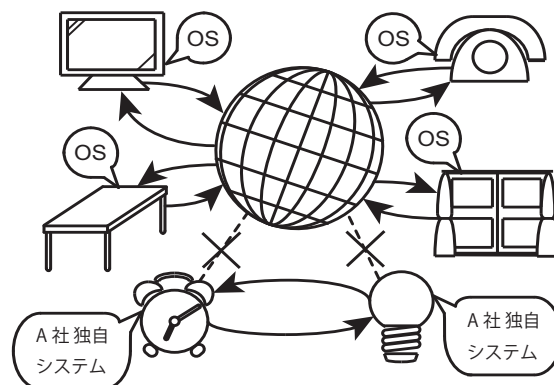


Fig.1 OS と IoT 端末の関係性

2.2 IoT 向け OS の課題と動向

Intel や Microsoft など大手企業は、今後 IoT 端末の数は増加し続け、2020 年には 500 億台を突破すると予想する。しかし、IoT 端末の中には、電池駆動の製品のように、消費電力を抑えるために高機能な処理機能を搭載していない端末も多い。よって、低機能な端末でも正常に動作する軽量の IoT 向け OS が必要である。

低性能端末向けの軽量の OS の実現に向けて、OS に搭載する機能を限定する方法がある。例えば、Google の IoT 向け OS 「Brillo」は、Android OS の端末管理や通信接続の機能を抜き出したような構成である。カーネルや端末抽象化機能、コネクティビティ機能など必要最小限の機能を提供する。通信規格には、同社が開発している「Weave」を採用している。「Weave」は Brillo 端末だけでなく、スマートフォンやパソコン、クラウドなどとの通信もサポートしている。このように、Google は OS に搭載する機能を限定することで軽量の IoT 向け OS の開発を目指している²⁾。

機能限定以外にも OS に搭載された各機能の軽量化というアプローチもある。

3 ID ベース暗号方式

東京大学では、IoT 向けの軽量の HTTPS 通信の開発に取り組み、実証に成功した。東京大学の発表では、現在よく使われている RSA 暗号方式を用いた HTTPS と比べて、通信データ量は 16 %、通信時間は 22 % の削減に成功

している。この軽量版 HTTPS は、ID ベース暗号方式で実現した。

HTTPS はやり取りするメッセージを暗号化することで、第三者による盗聴を防ぐ通信方法である。この暗号化に ID ベース暗号方式を用いる。この方式は公開鍵暗号方式の一種で、公開鍵を受信者の個人識別子で作成できるという特徴がある。公開鍵は送信メッセージの暗号化に用いる。現在主流の RSA 暗号方式では、多く存在する公開鍵の内、この鍵が自分のものであることを示す証明書が必要である。しかし、ID ベース暗号方式では送信者が受信者の ID から公開鍵を作成するため、証明書を必要としない。例として、ID に受信者のメールアドレスを使用する場合を考える。送信者は受信者のメールアドレスと鍵生成センタが公開しているパラメータで公開鍵を作成し、暗号化を行う。公開鍵は受信者のメールアドレスから作成しているので証明書は不要である。このように、ID ベース暗号方式の採用は、鍵の証明書を不要として情報量の削減を実現する³⁾。ID ベース暗号方式のイメージを Fig. 2 に示す。

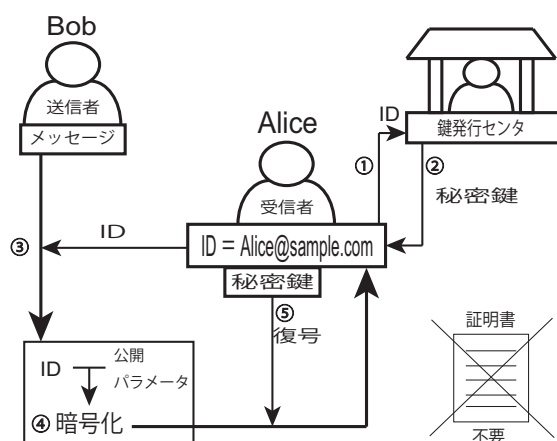


Fig.2 ID ベース暗号方式のイメージ

軽量版 HTTPS 通信は、低性能な端末で動作するだけでなく、安全性の向上にも繋がる。IoT では全端末が通信を行うため、通信機能の性能向上と共に、セキュリティ性能の向上も必要である。したがって、軽量版 HTTPS 通信の採用は、IoT 向け OS の軽量化だけでなく、IoT 端末間の安全な通信を実現するためにも重要となる。

4 IoT 向け OS の活用例

IoT サービス提供会社 OPTiM は IoT 向けクラウド OS 「OPTiM CLOUD IoT OS」を開発した。このクラウド OS に対応したアプリケーションソフトは、ハードウェア上の仕様にとらわれずに各 IoT 端末を利用したサービスを実装できる。さらに、それらサービスはスマートフォンやパソコンなど様々な端末から使用可能である。アプリケーションソフトには、IoT 端末の管理・制御や集められたデータの分析、地理情報に結びつけてのデータ閲覧・分析などがある。クラウド上のシステムのため、サーバやストレージなどは拡張が自由であり、ハードウェア上の物理的制約が無い。よって、IoT システムが容易に実装・管理

でき、導入のきっかけになる OS 提供サービスである。

今後、さらなる進展が期待される IoT 向け OS として IoT 向けの車載 OS がある。トヨタや日産、Google なども開発に取り組んでおり、自動運転の実現に向けて大きく期待されている。自動車に IoT 向け OS が搭載されると、ハードウェアの仕様にとらわれないスムーズな通信が可能となる。つまり、街中の防犯カメラや歩行者の持つスマートフォン、自動車など他の IoT 端末と情報を共有できる。運転者による確認や車載センサでは、これまで確認できなかった情報を発見可能であり、死角情報の取得に役立つ。したがって、IoT 向け OS を搭載することで、より安全な自動運転が可能となる。IoT 向け OS 搭載車の通信イメージを Fig. 3 に示す。

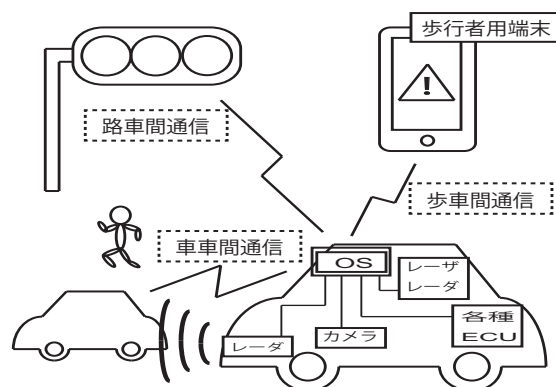


Fig.3 IoT 向け OS 搭載車の通信イメージ

5 今後の展望

IoT 向け OS の開発は企業だけでなく、国家規模で進められる。日本国内では 2016 年度内に「スマート工場」の実証試験が始まる。IoT により、製造現場の情報をデジタル化し、製造ラインの自動化や工場間での連携など行える日本独自の OS 開発を国のサポートのもとに進める。

このように、国家主導で IoT 向け OS の開発が進められることで、企業の関心もさらに高まり、より一層 IoT 向け OS の開発は加速する。OS に低性能端末でも動作する軽量化が備われば、OS を搭載できる端末が増える。そのうえ、「Brillo」や「OPTiM CLOUD IoT OS」では、既に対応アプリケーションソフトの開発環境を提供している。したがって、アプリケーションソフトの開発は容易かつ活発になると予想される。今後、IoT 端末・サービスの数は増加し、新たなサービスの登場も期待できる。

参考文献

- 1) 野田勝: IoT 時代を制するのは誰だ? IoT プラットフォームを開発する巨大グローバル企業にせまる, <http://o2o.abeka.asia/product/post-9890/>
- 2) Google: Brillo と Weave についてのアップデート, <http://googledevjp.blogspot.jp/2015/12/brillo-weave.html>
- 3) レスアンヒウ, 井手口哲夫, 奥田隆史, 田学軍: 高速道路における車々間通信システムへの ID ベース暗号の適用とその評価.