

WebサービスとIoT機器を融合したサイバーフィジカルサービスの実現

メタデータ	言語: ja 出版者: 静岡大学 公開日: 2019-06-12 キーワード (Ja): キーワード (En): 作成者: 二村, 和明 メールアドレス: 所属:
URL	https://doi.org/10.14945/00026682

(課程博士・様式7) (Doctoral qualification by coursework, Form 7)

学位論文要旨

Abstract of Doctoral Thesis

専攻： 情報科学

氏名： 二村 和明

Course :

Name :

論文題目： Web サービスと IoT 機器を融合したサイバーフィジカルサービスの実現

Title of Thesis :

論文要旨：

Abstract :

現在のサイバーサービスでは、利用者がスマートフォンなどを使って検索を行い、オンライン店舗などのポータルサイトを選択することでサービスを受けている。一方、2020年には、数百億個の物理的な IoT(Internet of Things)機器がクラウドに接続され、生活や産業を大きく変革するといわれている。このような中で、従来のサイバー空間に閉じていたサービスに、ネットワークと接続された様々な IoT 機器を組み合わせることで、サイバーサービスと物理サービスを融合させた、サイバー空間と物理空間の垣根を超えたリッチなサイバーフィジカルサービスの実現やその拡大が期待される。

IoT 機器は2つの種類に分類される。それ自体ではインターネットとの接続あるいはサイバーサービスとの連携ができない非完結型 IoT 機器と、それ自体で利用者に対してサイバーフィジカルサービスを提供できる完結型 IoT 機器である。

非完結型 IoT 機器は、サイバーサービスと連携することによって、サイバーフィジカルサービスを提供する。しかし、システムリソースが限定された能力の低い非完結型 IoT 機器をどう收容し、サービスプロバイダがサービスを構築できるようにするかという点が課題となる。これには、Web ページのようなサイバーサービスポータルが既に広く安全なサービスを提供・運用していることから、このサイバーサービスポータルに対してゲートウェイを介して、非完結型 IoT 機器によるフィジカルサービスポイントをアドオンするアプローチが適していると考えられる (アドオン型サイバーフィジカルサービス)。

完結型 IoT 機器は、IoT 機器自体が既に独自でサイバーフィジカルサービスポータルとフィジカルサービスポイントを提供している (クラウドと IoT 機器が予め固定されているボルトオン型サイバーフィジカルサービス)。完結型 IoT 機器の場合は、個々の IoT 機器の中

で自由にサービスを構築することができるため、その設計や開発においては、種々存在する既存の手法やツールの中から適切なものを選んで利用すれば足りる。従って、研究課題としては、サービスをどう実装するかという観点よりも、サービスをどう利用するかという観点が重要となる。中でも、サービス利用時における利用者認証の機構を共通化する意義は大きい。

Web サービスと IoT 機器を融合したサイバーフィジカルサービスの実現にあたり、ヒューマンセントリックの視点に基づいた検討・設計を行う点が本研究の特徴である。

前者のアドオン型サイバーフィジカルサービス（非完結型 IoT 機器）に関しては、主として開発者の観点からのヒューマンセントリックコンピューティングの達成に焦点を当て、既存のサイバーサービスに非完結型 IoT 機器をアドオンするために、Web 技術の活用するアプローチをとる。具体的には、サイバーサービスと IoT 機器(非完結型 IoT 機器)の接続を自由に組み合わせられる Web 型デバイスドライバ技術を提案する。これにより、非完結型 IoT 機器もゲートウェイを介して自在にサイバーサービスに接続可能となり、人の移動が伴う場合であっても自由度の高いサイバーフィジカルサービス提供が可能となる。Web 開発者はこれまで Web サーバや Web ブラウザ上で動作するアプリケーションを開発することが多かったが、Web アプリケーションから直接非完結型 IoT 機器の制御を可能にすることで、Web 開発者がサイバーフィジカルサービス開発にも簡単に取り組めるようにする。

後者のボルトオン型サイバーフィジカルサービス（完結型 IoT 機器）に関しては、主として利用者の観点からのヒューマンセントリックコンピューティングの達成に焦点を当て、サイバーフィジカルサービスにおける利用者認証の実用性を高めるために、利便性・安全性・実在性・可用性の観点を兼ね備えた認証手法を提案する。様々なサービスが多数展開される中で、それぞれが異なるユーザインタフェースを提供してしまうと、利用者の利便性が著しく損なわれることになるため、認証機構を統一可能にし、これを共通フレームワークとして提供することで利便性を確保する。また、利用者が普段携帯する生体認証機能を具備するスマートフォンを使った本人確認により安全性を確保、さらに、利用者が物理的に完結型 IoT 機器にタッチするという動作を活用することで、利用者が完結型 IoT 機器の前に所在すること(実在性)の確認手段とする。その際、サービスサーバと IoT 機器の間で予め形成されているローカルな通信路に認証プロトコルを安全に収容し、データオフロードに配慮したサービスインフラを提供することで可用性を確保する。