山本レポート：システム安全性向上―世界の最前線（2）

IoTにおける説明責任

国立大学法人 名古屋大学
大学院 情報学研究科
教授　山本 修一郎
博士（工学）

IEEE COMPUTER 誌の 7 月号に、IoT における説明責任について解説記事 [1] があったので紹介したい。

IoTの本質

我々は、物理的世界とデジタル世界が高度に結合された環境が実現される IoT 革命の最初の段階にいる。この段階では、個別的な IoT システムが登場し始めているので、特定の場面ごとに IoT が導入されており「Internet of Silos」になっている [1]。今後は、より全体的に IoT システムが統合されるだろう。そのためには、人々が IoT 技術を快く受入れることが前提になる。

特に、多様なシステムが結合されることから、このような広い意味での IoT では SoS（System of Systems、システムのシステム）であることがもたらす新たな課題を明らかにしておく必要がある。文献 [1] では SoS の特性として、ガバナンスの多様性、動的相互作用、データアナリティクス、自動化を挙げている。

■ガバナンスの多様性

IoT では管理・運用する組織が異なるので、それぞれの IoT に対する関心事・義務・責任の考え方も異なる。異なる組織が提供する IoT ではガバナンスが異なるので、それらの IoT が結合すると、ガバナンス方針が対立する可能性がある。例えば、周辺機器と相互作用する携帯機器のガバナンス方針の対立である。

■動的相互作用

IoT が社会に普及すると、複数の異なる IoT が動的に連係する場面が増加する。例えば、携帯端末を持って新たな街に到着すると、ウェアラブル端末が自動的に周囲に組み込まれたサービスと連動することになる。

■データアナリティクス

多数のセンサが環境に配備されることで生じる膨大なデータが分野横断的に結合され、機械学習される。例えば、顧客が小売業者から購入した商品の利用方法を、顧客の家庭内の多様なセンサから得たデータによって小売業者が推論するかもしれない。

■自動化

IoT が自動的に反応・適応・応答する。例えば、問題が発生すると IoT がこの問題を自動的に検知して救急サービスに通知して自動的に警告することができる。また、家と車など異なる環境間で個人の嗜好を IoT が記録して、周辺の環境に組み込まれた IoT 機器に継承することができる。

表 1　SoS の特性

特性	説明	例
ガバナンスの多様性	IoTを管理・運用する組織が異なるので、関心事・義務・責任の考え方が個別化する。	ウェアラブル端末の運用者と相互作用する周辺機器の運用者とが義務・責任について異なる方針を持つ。
動的相互作用	複数のIoTが動的に連係する。	新たな街に到着するとウェアラブル端末が自動的に周囲に組み込まれたサービスと連動する。
データアナリティクス	多数のセンサが環境に配備されることで生じる膨大なデータが分野横断的に結合・機械学習される。	顧客の家庭内の多様なセンサから得たデータによって、小売業者が商品の利用方法を推論する。
自動化	IoTが自動的に、反応・適応・応答する。	問題が発生すると、救急サービスが警告する。 家と車など異なる環境間で、個人の嗜好を継承する。

以上をまとめると、表 1 のようになる。

説明責任

Cambridge Dictionary によると、説明責任の意味は「行為について責任があること、および、それについて満足のいく説明を提供できること」とある。したがって、行為と責任が何であるかが明確になっていないと説明責任を果たすことができない。また、説明責任を遂行するためには、行為の事実と根拠となる証拠が必要になる。

IoTの説明責任

IoTの説明責任について文献[1]では、ガバナンスと責任、プライバシーと監視、安全性とセキュリティという3つの側面があるとしている。

■ガバナンスと責任

異なる組織が管理する構成要素が結合して相互作用する場合、だれが全体の責任を負うべきかが問題になる。IoTを提供する組織が異なれば、前述したように、ガバナンス方針が対立する可能性がある。そもそもガバナンス方針が明確になっていないIoTもあるだろう。多数のIoTが構成要素となって接続する世界では、ガバナンスのガバナンスGoG（Governance of Governance）が課題になる。また、ガバナンスの条件として利用条件を明確に規定していても、利用条件を無視して利用される可能性も否定できない。

このように、ガバナンスと責任の留意点には、結合する構成要素の不透明性と利用状況や目的外使用の不可視性がある。このため、相互に結合されるIoTを提供する場合、構成要素のガバナンスと責任範囲を明確にするとともに、説明責任を遂行するための証拠を利用時に記録する必要がある。

■プライバシーと監視

IoTによって高度にデジタル化された環境は、同時に高い監視能力を持つことになる。物理環境に埋め込まれた多数のセンサと携帯機器によって、個人の状況が詳細に記録できるので、個人行動がデジタル化され、自動的に追跡できてしまう可能性がある。したがって、プライバシーと監視の留意点には、個人データの監視権限、IoT提供者によるデータ利用・管理の透明性、データ処理権限の管理などが適切であることを根拠に基づいて説明することが求められる。

表2　説明責任の側面

側面	説明	留意点
ガバナンスと責任	異なる組織が管理する構成要素が結合して相互作用する場合、だれが全体の責任を負うべきかが問題になる。	結合する構成要素の不透明性 利用状況や目的外使用の不可視性。
プライバシーと監視	高度にデジタル化された環境は同時に高い監視能力を持つ。	個人データの監視権限の管理、データ利用・管理の透明性、データ処理権限の管理。
安全性とセキュリティ	包括的なIoTでは構成要素、相互接続、個人および組織が膨大な数になるので、構成要素の障害が物理的な危害に波及する。	障害の抑止とリスクの緩和 障害からの学習を容易化するための監視。

このため、個人のプライバシーを保護できていることと権限を越えた監視をしていないことについて、説明責任を果たせるような仕組みが構成要素としてのIoTに求められる。また、構成要素としてのIoTがプライバシーを保護できていたとしても、複数のIoTを結合することでプライバシーが保護できなくなる可能性があるかもしれない。この点についても今後留意していく必要がある。

■安全性とセキュリティ

包括的なIoTでは構成要素、相互接続、個人および組織が膨大な数になるので、構成要素の障害が物理的な危害に波及する可能性がある。

留意点には、包括的なIoTにおける障害の抑止とリスクの緩和がある。複数のIoTからなるSoSシステムの安全性とセキュリティを保証するためには、構成要素としてのIoTについて安全性とセキュリティを保証することと、複数のIoTの相互関係の安全性とセキュリティを保証する必要がある。この場合、問題となるのは複数のIoTの相互関係についての安全性とセキュリティを、どのように定義して記録・保証するかということである。この留意点は、異なるIoTのガバナンスと責任の問題とも関連する重要な留意点である。

また、障害からの学習を容易化するための監視についても、構成要素としてのIoTであれば個別的に障害について学習できる。しかし構成要素間の関係についてどのように学習するかについては今後検討していく必要がある。

上述した内容を整理すると表2のようになる。

まとめ

本稿で紹介したIoTにおける説明責任について、まとめると以下の3点になる。

- IoTの本質は、SoSである。
- SoSの特性には、ガバナンスの多様性、動的相互作用、データアナリティクス、自動化がある。
- IoTにおける説明責任では、ガバナンスと責任、プライバシーと監視、安全性とセキュリティという3つの側面が重要になる。

＜参考文献＞
[1] Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, Jon Crowcroft, Accountability in the IoT: Systems, Law, and Ways Forward, IEEE COMPUTER, July 2018, pp.54-65

＜システム安全性のことなら下記へ＞
yamamotosui@icts.nagoya-u.ac.jp