2016年5月

新たなITリスクに立ち向かう 連載シリーズ 第20回

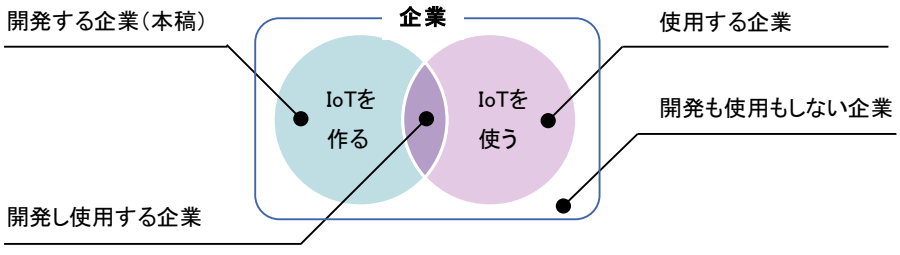
IoTを開発する企業に まず必要なセキュリティとは

IoT（Internet of Things：モノのインターネット）は、多数のデバイスがインターネットと接続したり、または相互に接続したりすることにより、今まで人間が行っていた認識や判断等の自動化をもたらすものである。世界中でIoTが生み出され、ヘルスケア、モビリティ、エネルギー等のさまざまな分野でも普及が見込まれている。しかし、既に世界に広く普及したスマートフォンの現状に鑑みると、「未来は明るい」とは言い難い。スマートフォンでは日々新しい脆弱性が発見され、その脆弱性が改修されないまま放置されるデバイスも散見される。また、そんなデバイスを狙ったマルウェアが作成されるなど負の連鎖が続いており、問題が発生してから行う、後付けのセキュリティ対策では限界がある。同様にIoTが普及すると、その用途から察するに、スマートフォンより甚大な被害が生じるであろうことは想像に難くない。負の連鎖を断ち切るために、IoTについてはデバイスを「作る」と「使う」の両方の面から、セキュリティを考える必要がある。

IoTを「作る」と「使う」では、考慮すべきセキュリティが異なる。よって、その2つの観点から企業の分類を考え、「開発する企業」、「使用する企業」、「開発し使用する企業」、「開発も使用もしない企業」の4つに分けた（図表1参照）。本稿では、このうち「開発する企業」について解説する。

なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りする。

【図表1】IoTにおける企業の分類



1. IoTのセキュリティ高度化に必要な設計

IoTにはインターネットや、相互に接続するといった機能があるため、想定外の問題が発生した場合にはその影響が他のIoTに波及し、人命や企業の存続にかかわる事態に発展する可能性がある。よって、IoTを開発する際には組織として、人の身体や財産等のハザードに対するセーフティ設計と、重要データの漏えいや攻撃によるシステム停止等の脅威に対するセキュリティ設計が必要である。

では、どのように組織としてセーフティ設計とセキュリティ設計を行うのか。IPA（Information-technology Promotion Agency, Japan：独立行政法人情報処理推進機構）が公開した「つながる世界の開発指針」[1]では、製品開発を「方針」、「分析」、「設計」、「保守」、「運用」という5つの大項目に分割し、それぞれについて最低限考慮すべき事項について指針を示している（図表2参照）。

【図表2】開発指針一覧

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1　安全安心の基本方針を策定する
		指針2　安全安心のための体制・人材を見直す
		指針3　内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4　守るべきものを特定する
		指針5　つながることによるリスクを想定する
		指針6　つながりで波及するリスクを想定する
		指針7　物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8　個々でも全体でも守れる設計をする
		指針9　つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 つながることによるリスクを一般利用者に知ってもらう

出典：独立行政法人情報処理推進機構「つながる世界の開発指針」

2. 経営者がすべきこと

組織としてセーフティ設計とセキュリティ設計を行うには、組織を横断した基本方針の策定や、コストに影響する体制・人材の見直し、他社との連携等が求められるが、それらは開発の現場だけで対応することが難しい。よって、経営者がリーダーシップを示し、体制を整える必要がある。IPAでは、「つながる世界の開発指針」の5つの大項目のなかで、「方針」については経営者が率先して参画することを促している。

1 「『つながる世界の開発指針』を公開」（独立行政法人情報処理推進機構 2016年3月24日）
https://www.ipa.go.jp/sec/reports/20160324.html

では、実際の開発において、セーフティ設計とセキュリティ設計がどのように実施されているのか。それを知る手がかりとしては、IPAが公開した「セーフティ設計・セキュリティ設計に関する実態調査結果」[2]がある（図表3参照）。

【図表3】アンケートから判明した事項（抜粋）

すべての回答者が、セーフティ設計またはセキュリティ設計のいずれか、もしくは両方が必要と回答した。
セーフティ設計またはセキュリティ設計の基本方針を明文化している組織は半数以下である。
基本方針に基づいたセーフティ設計、セキュリティ設計のルールについても明文化率は低く、その実施は開発リーダーなどの判断に任されている。
セーフティ・セキュリティの重要な設計上の判断への経営層や品質保証部門等の責任者の関与が少ない。

出典：独立行政法人情報処理推進機構「セーフティ設計・セキュリティ設計に関する実態調査結果IPAアンケート」を基にKPMGが作成

このアンケート結果から、実際の開発では、属人的なIoTのセーフティ設計／セキュリティ設計が行われている様子が伺える。そのような設計が行われている原因は多々考えられるが、たとえば、IoT自体が高度な技術の集合であり複雑性が高いため、開発以外の部門や場合によっては開発者の間でも、製品に対する理解に差がある事が原因となっているのではないだろうか。また、IoTはインターネットや他の機器と繋がるため、それらに対する深い知見がある個人に依存している事が原因とも考えられる。

その様な事も考慮すると、経営者は自社のIoTについて、「指針1 安全安心の基本方針を策定する」、「指針2 安全安心のための体制・人材を見直す」、「指針3 内部不正やミスに備える」を実施する前に、今まで以上に開発者等からフィードバックを受ける必要があるといえる。

3. 開発者がすべきこと

IPAは、「つながる世界の開発指針」のなかで、開発者には大項目の「分析」、「設計」、「保守」、「運用」の指針について対応が必要だとしている。考慮すべき指針とその対策の内容は多岐にわたるが、それは最低限の事項であり、開発するIoTによってはさらなる対策が求められる。

たとえば、IoTを安価で汎用的なSoC（System on a chip）を用いて開発する場合、SoC等のメーカーは販売活動の一環としてインターネット上で製品の仕様や技術情報を公開している。このような情報は攻撃の足がかりとなり、ハッカーから狙われる恐れがあるため、基盤のシルク印刷やICチップに印刷された型番を隠す・除去する等といった対策も必要になるかもしれない。また、人命にかかわるようなIoTにおいては、内部に完全に独立したWatchdog Timerを実装することにより定期的に自己診断を実行し、問題があれば自己復旧したり、ネットワークを通じて外部に自動的に通報したりするような対策も必要となるだろう。

このように、新しい技術や製品を開発する現場においてセーフティ設計／セキュリティ設計を行う際に、すべての事象を予測し対策を考慮することは容易ではない。そのため、開発者は経営者や品質管理者等の他部門に、IoTに関する技術的な内容をわかりやすく説明して協力を得るべきである。

2 「『セーフティ設計・セキュリティ設計に関する実態調査結果』を公開」（独立行政法人情報処理推進機構 2015年9月10日）
https://www.ipa.go.jp/sec/reports/20150910.html

4. まとめ

最後に、IoTを「開発する企業」に必要なセキュリティについて、ポイントをまとめる。

- 開発する企業の経営者は、まず自社の IoT を理解し、組織としてセーフティ設計／セキュリティ設計を行えるように体制を整備する。
- 開発者は体制を構築するため、また協力を得るために IoT に関する知見を可能な限り平易な言葉で経営者や他部門に周知する。
- IoT の開発には今まで以上に、経営者や品質管理者と開発者間での情報の連携が必要である。

KPMGコンサルティング株式会社
マネジャー　小寺　孝一郎

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号　銀泉備後町ビル
TEL ： 06-7731-2200

名古屋事務所
〒450-6426
名古屋市中村区名駅3丁目28番12号　大名古屋ビルヂング
TEL ： 052-571-5485

kpmg.com/jp/kc