

実験法律学

第1回 IoT デバイス篇

(渡邊 明彦 2020/10/08)

I はじめに

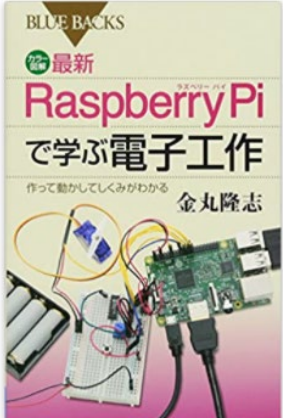
IT 関連の契約書を読んでいるとき、書かれている内容が、もしまったく理解できなかったとしたら、きっと面白くないでしょう。そのようなことのないように、技術的内容に突進して行こうというのが、このシリーズ『実験法律学』です。

第1回目は、「IoT デバイス」を取り上げます。IoT は、「モノのインターネット」、Internet of Things で、この「モノのインターネット」に繋がっているのが IoT デバイスです。モノではありません。IoT デバイスとして想定されるものの範囲は、極めて幅が広く、ただ羅列するだけは面白みがないので、今回は「気温（室温）計測器」を対象を絞って検討します。

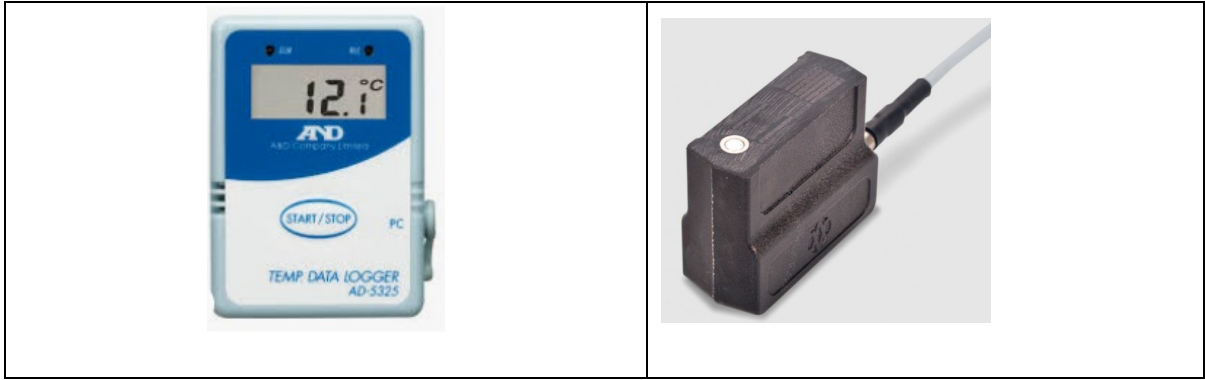
II Raspberry Pi による回路の組立て

分析の道具として、Raspberry Pi を用います。

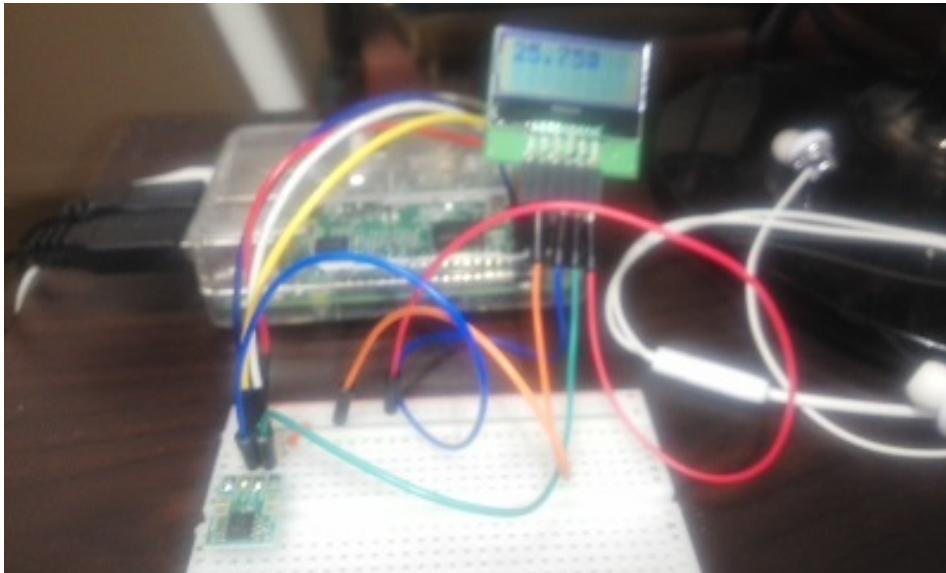
超小型コンピュータ Raspberry Pi 3 Model B+（以下「Raspberry Pi」）については、次の書籍を参考にしました。

	<p>Raspberry Pi 4 対応 カラー図解 『最新 Raspberry Pi で学ぶ電子工作 作る、動かす、しくみがわかる! (ブルーバックス) (日本語) 新書 - 2020/6/18</p> <p>金丸 隆志 (著)</p> <p>に極めて懇切丁寧な解説があり、この本を手にしなから Raspberry Pi 本体を設定し、パーツを揃えていけば、誰でも以下の実験ができます。</p> <p>以下この本を「金丸、164 ページ」のように引用します。</p>
---	---

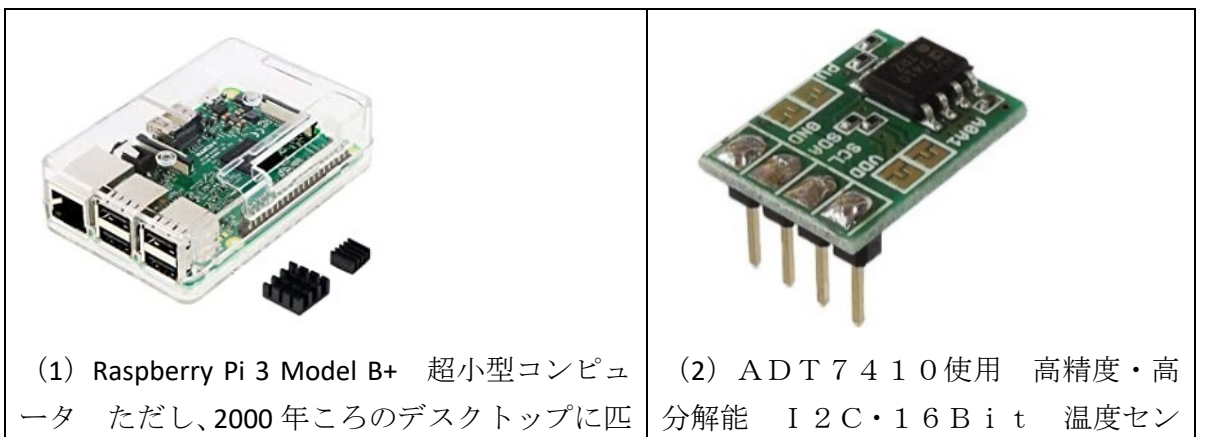
さて、一般的に気温計測器としてイメージされるのは、どのようなものでしょうか。左側は、AND 温度データロガーで、右側は、Vaisala というメーカーの道路/滑走路表面センサです。



ただし、これらの計測器を分解しても、圧倒されるだけでさしたる成果は得られないと思われますので、Raspberry Pi により「温度の計測器であって、計測結果をインターネット経由で送信することのできる」デバイスの回路を組みます。一種のシミュレーションで、組み立てると、次の写真のようになります。



構成内容は、次のようです。



<p>敵するとのこと。 ディスプレイにつないで、キーボードとマウスで、通常のパソコンとほぼ同じ操作ができる。</p>	<p>サモジュール</p>
--	---------------

あと、ブレッドボード、ジャンパーワイヤーがいるのは、写真のとおりです。

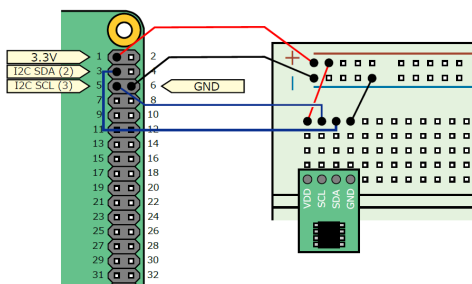
温度センサモジュールでは、センサと AD コンバータ AD T 7 4 1 0 がチップに内蔵されている（金丸、165 ページ） こととなります。

なお、Raspberry Pi 3 Model B+ の設定、パーツの購入方法等については、前述の『Raspberry Pi で学ぶ電子工作』をご覧ください。書かれているとおり、忠実にたどっていくと失敗はありませんでした。

III 計測された温度の表示

III A 計測された温度のパソコン・ディスプレイへの表示

金丸、164 ページにあるように、ブレッドボード上に AD コンバータ AD T 7 4 1 0 を差し込み、下のような回路を組みます。



Raspberry Pi の OS である Raspberry Pi OS をインストールすると、デフォルトで使用できる Thonny Python IDE という統合開発環境に、以下のスクリプトを入力・あるいは添付のスクリプトをコピー&ペーストして実行すると（金丸、166 ページ以下）、

```
# -*- coding: utf-8 -*-
import smbus
from time import sleep

def read_adt7410():
    word_data = bus.read_word_data(address_adt7410, register_adt7410)
    data = (word_data & 0xff00)>>8 | (word_data & 0xff)<<8
```

```

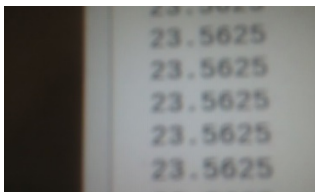
data = data>>3 # 13ビットデータ
if data & 0x1000 == 0: # 温度が正または0の場合
    temperature = data*0.0625
else: # 温度が負の場合、絶対値を取ってからマイナスをかける
    temperature = (~data&0x1fff) + 1)*-0.0625
return temperature

bus = smbus.SMBus(1)
address_adt7410 = 0x48
register_adt7410 = 0x00

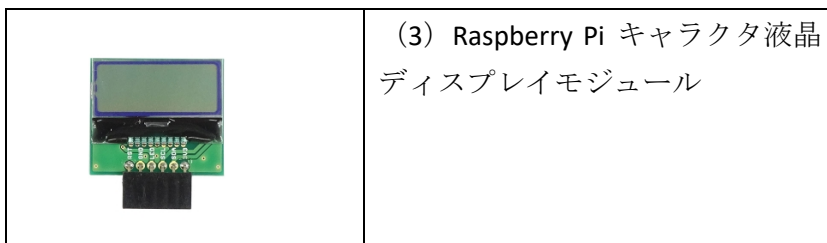
try:
    while True:
        inputValue = read_adt7410()
        print(inputValue)
        sleep(0.5)
except KeyboardInterrupt:
    pass

```

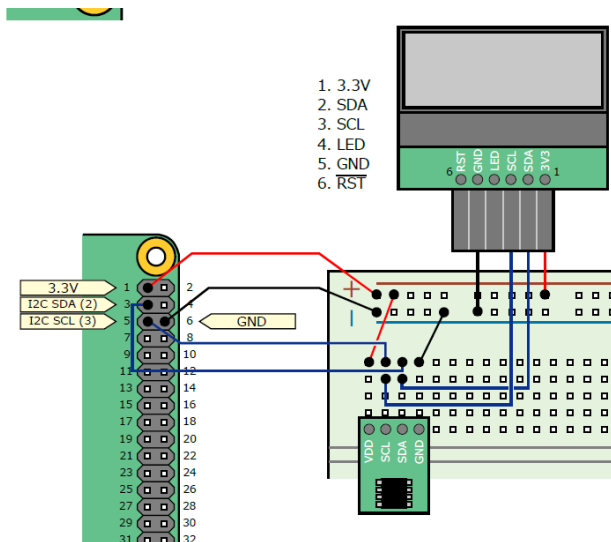
Raspberry Pi に接続しているディスプレイ上に、0.5 秒間隔で、次のような数値が流れるように表示されます。



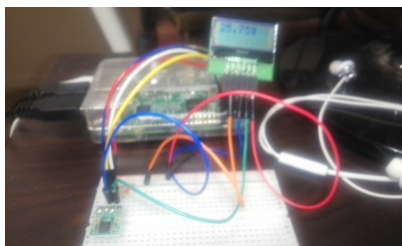
III B 計測された温度の小型ディスプレイへの表示



回路の配線は次のようになります。



実物は、第 1 ページ目のイメージと同じです。小型液晶モジュールに 25.750 度と表示されているのがわかります。



この段階で、最初の AND 温度データロガーと同等のものが実現できました。

IV Raspberry Pi で表示されている計測値に、別のパソコンからアクセスする

さて、次に、この計測値を、Raspberry Pi 以外のパソコンから（外から）見ることができないか、という作業に進みます。使用する回路は、III で用いたものと同じです。具体的には、Raspberry Pi に、ブラウザからの HTTP 要求に応答できるウェブサーバー機能を持たせることとなります。そのために、金丸、227 ページにしたがい WebIOPI というソフトウェアをインストールします。

```
$ sudo service webiopi start
```

で webiopi を起動させ、

Raspberry Pi に割り当てられているプライベートアドレス、例えば金丸、254 ページにある

192.168.1.3 をもとに

別のパソコンのブラウザ、私の場合は Chrome に

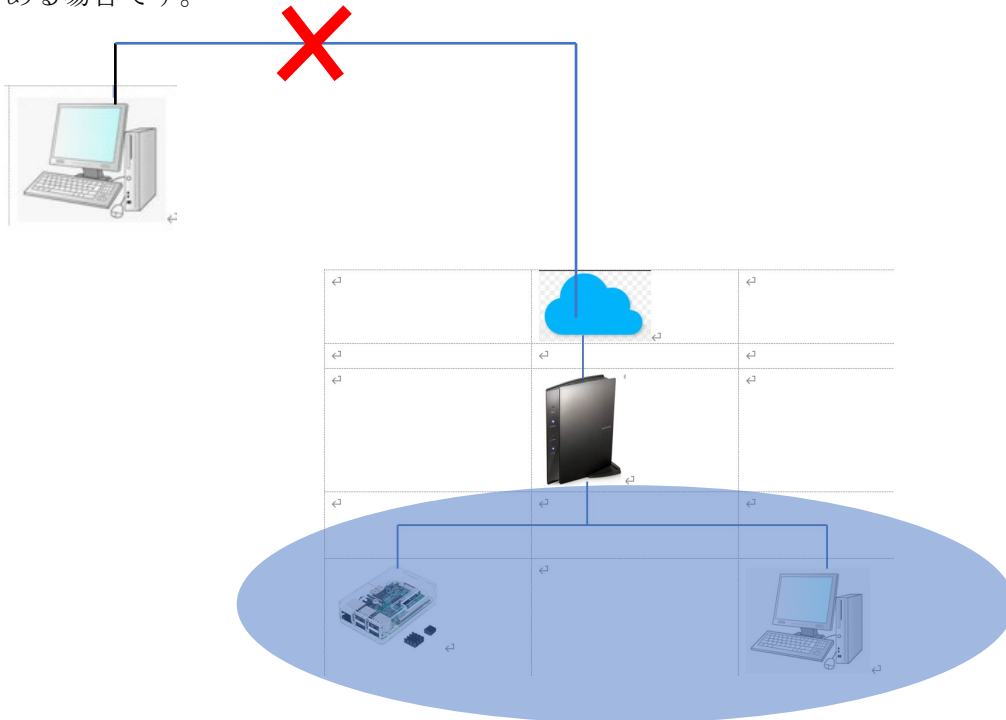
`http://192.168.13:8000/bb/02/`

と打ち込み、ユーザー名とパスワードを打ち込むと、パソコンのディスプレイに

温度:

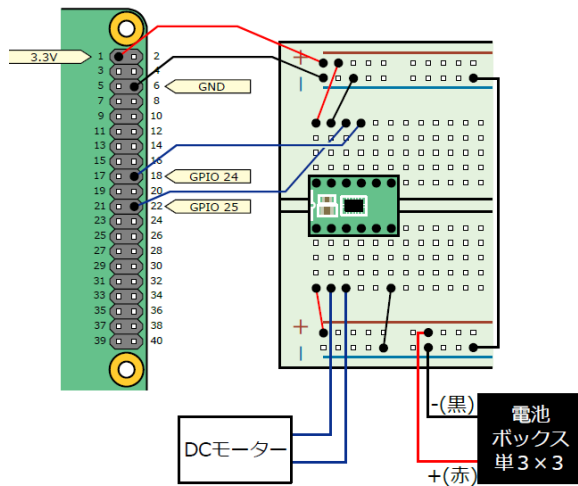
のように表示され、温度が 2 秒毎に更新されます。

【問題点】ここで行った実験は、Raspberry Pi と使用したパソコンが、同一のルーターの下にある場合です。



今回、試しているのは 1 台のルーターの下にある Raspberry Pi とパソコン間の通信です。金丸、227 ページは、理論的にはルーターをまたぐ場合も可能であるが、「ネットワークの高度の知識」が必要であり「セキュリティの問題」も関係すると指摘しています。ネット上には、SSH 通信により、インターネット経由で Raspberry Pi を操作する方法も紹介されていますが、それはセキュリティ関係の実験後に、再度、取り上げます。

【補足】金丸、264 ページ以下には、ほぼ同じ操作で、パソコンから Raspberry Pi に接続された DC モーターを制御する例が紹介されています。したがって、理論的には、データを受信するだけでなく、モーター等を制御するという働きかけも可能です。



V 法律学

以上のように「手を動かして」作業をしてくると、いろいろなことが分かってくる。議論が散漫にならないように、米国でも初の IoT 立法（以下「IoT 法」と言われている、TITLE 1.81.26. Security of Connected Devices, §§ 1798.91.04., 1798.91.05.（以下「CA 法」として引用）を参照基準にして検討して見ましょう。

1. プライバシー保護法か？

IoT 法に関しては、とくに欧州の文献に見られるように、プライバシー、個人データ、個人情報保護法として位置づけ（CA 法は、「An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, **relating to information privacy**」とされており、「(e) “Unauthorized access, destruction, use, modification, or disclosure” means access, destruction, use, modification, or disclosure that is not authorized **by the consumer**」としているように見える。ただし、米国の法律事務所のメモでは「そのような制限はない」との記述もあり、注意）これら個人情報を「protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure」することを目的としていることが多い（CA 法 1798.91.04.(a)(3)）。IoT デバイスは、産業用の用途が（圧倒的に）多くなることが予想されるので、IoT システムへの侵入を想定する立法が望まれる（いわゆる「ハッキング防止法」）ではないか。

2. IoT 法の対象（その 1）

CA 法が、「connected device」を対象としており、この connected device を「(b) “Connected device” means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.」と定義しているとおおり、device であって（other physical object は、intangible なソフトウェア等を除く趣旨で

あろう)、「モノ」ではない。つまり、Internet of things に繋がっているのは、thing(s) ではなく device である。日本の文献でも、数は少ないが海外の文献でも、「モノ」、thing が繋がっていることを前提にしているものがあるが、適切ではないのではないかな。



つまり、左のイメージにある「乗用車」「航空機」「クレーン」も、また「テレビ受像機」も device ではないであろう。IoT デバイスを組み込んだ appliance ではあると思われるが。

したがって、IoT の対象が定まらないという指摘は、根拠がないように思われる。

3. IoT 法の対象 (その 1)

IoT を、(1) IoT デバイスの形成するエコシステム (ecosystem) であって、(2) 自律性のあるもの (autonomous) とする定義が、技術的な文献では多いように思われる。だとすれば、孤立した a Connected Device をベースに法規制を行うのは (個人的な用途の、例えば体温を測定してそのログを保存したり送信するデバイスを除けば)、実情に合わないように思われる。

【セキュリティに関連する自律性の一例】

ソフトウェアファイアウォールで保護されたロボットがウイルスに感染し、それを他のマシンに伝播させました。安全なハードウェアを備えたソースでデータを保護し、製造中にフラッシュメモリにキーが組み込まれたセキュアなエレメントの機能を使用しているロボットが異常を検知しました。システム全体がシャットダウンされ、OS、ファームウェアが再度インストールし直され、システム全体が元の安全なプロトコルを使用して再起動されました。

4. connecting to について

CA 法では、上記のとおり、「(b) “Connected device” means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.」という定義がある。

今回の実験では、Raspberry Pi には 192.168.1.3 というアドレスが割り当てられていた。このアドレスは、いわゆるクラス C プライベート IP アドレス (192.168.00 ~ 192.168.255.0) で、グローバルアドレスではなく、LAN 内で使用されるもの。LAN 内で使用されるものと言っても、現在は NAPT によって、アドレスもポート番号も変換されてインターネットに接続されることから (今回の Raspberry Pi は、現状でも自由にインターネットに接続でき、例えば Chrome の Linux 版 Chromium で YouTube を閲覧できる)、IP アドレスを割り振られているデバイスは directly or indirectly に接続されているものとして取り扱われるのではないかな。潜在的には、「MAC アドレスを割り振られた NIC を装着しているデバイス」が、connected devices になるように思われる。

つまり、CA 法の「outside a local area network」基準は、ミスリーディングであろう。

1798.91.04.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication **outside a local area network**, it shall be deemed a reasonable security feature under subdivision

5. reasonable security feature について

CA 法には、

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

- (1) Appropriate to the nature and function of the device.
- (2) Appropriate to the information it may collect, contain, or transmit.
- (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

と、

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision(a) if either of the following requirements are met:

- (1) The preprogrammed password is unique to each device manufactured.
- (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

という規定がある。

(a)では、デバイスと情報に関して適切であること、およびデバイスと情報を不正アクセス等から保護するように設計されているデバイスを装着していることを求めている。セキュリティについては、デバイスにインストールされるアンチウィルスソフトのような個別的な対応でなく、個人使用レベルでもルーターでのフィルタリングのように、孤立したデバイス単位ではない対策が重要であり、デバイスに限定するのは難であろう（エコシステムとしてのアプローチが必要）。

IV の【問題点】で引用した金丸先生の警告にあるとおり、個人が Raspberry Pi をサーバーとしてインターネット上で公開するのは、リスクがあるようです。これなども、IoT デバイスの問題というより、接続されているルーターの設定を、個人で変更することが原因であり当該デバイスに security feature を求めることでは対処できないのではないかと。

ネット上では、Raspberry Pi にウェブカメラを接続して、SSH 通信で外出先から自宅のペットを監視（？）する用途が報告されていますが、「用心」が必要なようです。

【参考】

もみじあめ・著『TCP/IP ネットワーク入門』、149 ページ、7.2 Destination Nat、にも

ご用心： インターネットから到来するパケットにはサーバー攻撃が含まれるため「ポートを空ける」ときは慎重になりましょう。

【ハードウェアレベルでの対応】

「ハッカーによるソフトウェアの変更またはバイパスを妨げるものは何もありません。つまり、ソフトウェアだけではセキュリティ攻撃を阻止できません。

メモリにセキュアなエレメントの機能を追加すれば、このような種類の水平方向の不正アクセスを遮断できる可能性があります。」として、「フラッシュコンポーネント内に強力な独立した保護層を追加します。...フラッシュにある重要な資産またはデータへのアクセスを許可または拒否するフラッシュ内の論理機能...という標準的なハードウェアプラットフォームとしてセキュアなエレメントの機能を統合する」

というアプローチを提唱するチップメーカーもあり、産業用の IoT では、このようなアプローチが優勢になってくるのではないかと。

(b) は認証 (authentication) で、(1) 製造される各デバイスについてユニークなパスワードの付与と（最近では「一意」という用語は使われなくなっているが、「ユニーク」は、要は「一意」の意味）、または「最初にデバイスにアクセスする前に、ユーザーに認証方法を与える新しい手段を与える」という要求事項を定めているとともに、認証の定義を設けている。

1798.91.05. For the purposes of this title, the following terms have the following meanings:

(a) “Authentication” means a method of verifying the authority of a user, process, or device to access resources in an information system.

「認証」は、「ユーザー認証」（本人確認）と「メッセージ認証」（内容確認）のうちの、ユーザー認証だけが取り上げられているように思われる。パスワード等を冒用されてデバイスに侵入するのを防止するのを主眼としている。実用的には、パスワード、メッセージの暗号化が HTTP over SSL が利用されていることから、より強度な方法が reasonable security feature として求められるのではないかと。

6. リスクベースのアプローチ

前項の reasonable feature に関連して、「合理性」はリスクベースで判断されるべきであるというのが一般である。これは、医療機器ですで見られるように、リスクに応じて、また想定される業種に応じて、ことなったレベルのセキュリティ上の要求事項が定められるのでは

ないか。

【IoT を巡る脅威】

- 工場ロボットがハッキングされ、作業ルーチンが破壊される
 - 医療業界で目立つハッキング例として、ランサムウェアによって病院を人質にする攻撃
 - インターネットに接続された脆弱なプリンターがひとりで印刷を始める
 - 構内の監視カメラ（閉鎖回路テレビジョン）の映像が外部に公開される
- 個人情報情報の漏洩といった脅威とは異なる脅威が存在する。

7. 規制対象は manufacturer か？

CA 法では、規制となる対象（主体）を manufacturer（製造業者）と規定しているが、IoT を「自律性を備えたエコシステム」ととらえると、企業向けの業務システムの納入とおなじく、システム構築の委任契約が主体となり、委任契約の納入物の 1 つとして IoT デバイスが位置づけられるのではないかと。つまり、売買契約中の保証として問題が生じるのではなく、（請負契約であることを否認する）委任契約中の個々の条項の問題として、IoT システム、IoT デバイスの法律問題が登場してくるのではないかと。

8. 免責条項の有効性

一般的、汎用の IoT システム、IoT デバイスには、市販のソフトウェア製品のライセンス条項にある、①ミッションクリティカルな作業で用いない、②人の生命、身体に傷害をもたらす状況では使用しない、③核施設では使用しない、という禁止条項が設けられることになる。

他方で、「組み込みシステム」で長らく問題となっている、ソフトウェア製品のライセンス契約にある「免責条項」が、そのまま有効でありうるのかという問題は残るであろう。カーネギー・メロン大学の教授が、「自動車の自動運転システムで使用される組み込みソフトウェアに瑕疵があった場合にも、一般のソフトウェア製品のライセンス契約にある完全免責規定が、そのまま使われるのか？」という疑問提起に代表される問題である。自動車のパーツに欠陥があれば、製造物責任が問われるのに、ソフトウェア製品では契約書の規定どおり免責されるのかという問題である。

産業用の IoT デバイスは、より大きな何らかの機器類の保証の問題として対処できる（つまり、外のパーツ・コンポーネンツと同じ）と思われるが、一般消費者がかかわる自動運転システム等では困難な問題になるのではないかと。ソフトウェア製品のライセンス契約に含まれているような広範な免責規定が認められない場合、ソフトウェア製品のライセンス契約自体に backlash が起きるといふかたちである。

（完）