Joho System linkai
情報通
2017.August　8月号
発　行：東京税理士会 情報システム委員会
題　字：神津　信一（四谷）
（税理士会員章の日輪と八重桜をイメージしています。）

速報
「法人電子申告義務化等の今後の行方」公表される

平成29年６月30日　行政手続きコスト削減の為の財務省基本計画が策定され、財務省HPに公表されました。

①大法人の法人税・消費税の電子申告義務化100%、中小法人85%の方向で検討
②ダイレクト納付の利便性拡大　③マイナポータル利用活用促進
④イメージデータ送信容量拡大　⑤e-TaxとeLTAX連携の推進、他

財務省HP：http://www.mof.go.jp/about_mof/other/e-j/kihonkeikaku.html
※本会HP「お知らせ」欄にも掲載いたしました。

【予 告】ミニセミナー復活！

・日　時：平成29年９月21日（木）　※時間未定
・テーマ：「事務所の効率化　はじめの一歩」
・講　師：安田　信彦　会員（日本橋支部）

身近になってきたIoTの仕組みと注意点

荒川支部　齋藤　潤一

1．はじめに

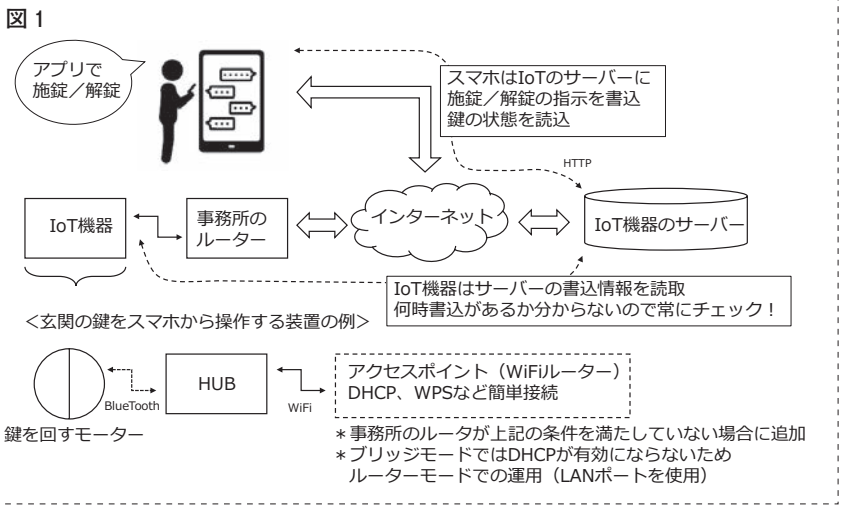
最近何かと耳にするIoT（Internet of Things：モノのインターネット）とは、パソコンやスマートフォンなどの情報機器以外の家電、住宅機器、産業機器、製造設備などをインターネットに接続し、様々な情報のやり取りや機器の制御を行うことをいいます。産業用機器は既に相当な割合でインターネットや専用ネットワークに接続されており、身近なところでは、コインパーキング、自動販売機、監視カメラ、デジタルタコグラフなどもネットワーク化によって合理化が進んでいます。今後、自動車の自動運転制御や走行中の車両相互の情報交換、製造装置、稼働中の機械の様々な情報の入手によって産業構造を変革する可能性のある技術として注目されています。本稿では事務所内の機器をインターネットに接続する際の方法と注意点についての概要を説明します。

2．事務所内IoTとその仕組み

事務所で使用するインターネットに接続する機器としては、ホームセキュリティ機器、監視カメラ、DVD等のオーディオ機器、出入口のシリンダー錠、エアコン、音声で制御するスピーカー、食材が届く冷蔵庫（ボタン１つで食品が宅配されます）、などがあります。これらの共通する特徴は「簡単に使えます」という点で、マニュアルもWi-Fiに接続するという簡単な説明のものがほとんどです。

外部から事務所内の機器を制御するということは、セキュリティ的には大きな危険を含んでいるため、安全を確保する為にはVPN（Virtual Private Network）※1と言われる外部から遮断された安全な通信経路を確保した上で情報のやり取りをするのですが、家庭用の場合は難しいため、**図１**にあるように外部サーバーを中継する方法をとっています。

図１



我々は、スマートフォンからエアコンをオンにしたり、事務所の鍵を施錠したり、機器を制御しますが、その情報は直接に事務所内の機器に届くのではなく、機器のメーカーが用意したインターネット上のサーバーに情報を送っています。事務所内の機器は、ホームページを閲覧する手順やメールの送信手順を用いて、機器それぞれのサーバーにアクセスして自身に対する指示を確認し、現在の状況と違いがあれば機器を操作します。何時、指示がくるかわからないので一定間隔でサーバーにアクセスしています。

3．セキュリティホールの出現にご注意を

事務所でパソコンをインターネットに接続する為には、光ファイバ業者と回線契約し終端装置をリースし、インターネット・プロバイダ契約の上で開通します。マイナンバー制度のセキュリティ対策として、高価なUTM（Unified Threat Management）※2装置を会計ベンダーに勧められて導入している事務所も多いと思います。そういった環境では一般的にIoT機器を接続するためのWi-Fiルーターは設置されておらず、家電量販店で購入して追加設置することになります。家庭用IoT機器の殆どは、Wi-Fiルーターの簡易接続機能（WPS）やDHCP（Dynamic Host Configuration Protocol）※3を利用して簡単に接続するという運用となっており、細かなIP設定などはできません。結果的にIoT機器を接続するためのアクセスポイントを追加する事となります。確かにIoT機器は簡単に接続できるのですが、アクセスポイントとして追加したWi-Fiルーターについて適切な設定を行わないと大きなセキュリティ・ホールを作ってしまうことになります。Wi-Fiルーターのセキュリティは基本的に自身の管理画面のIDとパスワードの管理、Wi-Fiの暗号化設定の選択です。ルーター機器の初期設定はIPアドレス、管理者IDとパスワード、などがすべて公開されており、初期設定のまま運用するのは非常に危険です。得意先などの外部の方の為のゲスト用IDなどを入力し易い文字列で作成している場合なども、不用意にセキュリティ・ホールを作ってしまうことになります。

図２

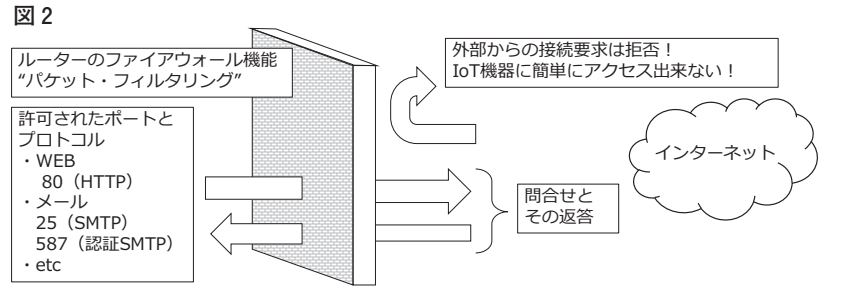


図２にあるように、インターネット接続に関するセキュリティの要はルーターです。しかし、ルーターやUTMでインターネットとの接続をセキュアにしたとしても、追加したアクセスポイントから部外者がネットワークに侵入しWi-Fiルーターの管理機能にアクセスしてしまえば、事務所内のデータにアクセス出来てしまいます。IoT機器は所長の知らないところでスタッフなどによって追加されてしまう可能性もありますので、思わぬところでセキュリティ・ホールを作ってしまわないよう注意が必要です。

4．おわりに

セキュリティの危険性について説明してきましたが、IoT機器自身は事務所の内部から自社のサーバーにアクセスしているだけで、外部から接続できるように設定されている訳ではありません。適切にアクセスポイントを追加すれば便利な機能を利用できますので、導入の際の参考にしていただければ幸いです。

※1 **VPN**：通信事業者の公衆回線を経由して構築された仮想的な組織内ネットワーク。また、そのようなネットワークを構築できる通信サービス。企業内ネットワークの拠点間接続などに使われ、あたかも自社ネットワーク内部の通信のように遠隔地の拠点との通信が行える。
※2 **UTM**：複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行うこと。
※3 **DHCP**：インターネットなどのネットワークに一時的に接続するコンピュータに、IPアドレスなど必要な情報を自動的に割り当てるプロトコル。ネットワーク設定を手動で行わなくてもすぐに適切な設定で接続することができ、ネットワークの設定に詳しくないユーザーでも簡単に接続できる。また、ネットワーク管理者は多くのクライアントを容易に一元管理することができる。