中小企業に於けるIoT
～ＩＴコーディネータが考えておくべきこと～

２０１８年3月３１日

企業内ITC・IT ガバナンス研究会

序

「あらゆるモノがインターネットを通してつながる」IoT 時代、IoT とは「Internet of Things」の略で、「モノのインターネット」時代がやって来ている。

IoT では、従来の企業での情報処理システムやWEB システムとは大きく異なる点、新たに考慮しなければならない点などが多々ある。

その違いを正確に捉え、中小企業を含む事業者が安心・安全に、IoT を活用出来ることが肝要となる。

IoT は、様々な分野での用途が期待されており、これまでになかった産業やサービスの創造の可能性を秘めているが、一方でセキュリティリスクもこれまでの常識だけでは対応しきれなくなっている。

中小企業の IT 経営を支援する立場の IT コーディネータは、中小企業経営者が適切な知識、ルールを踏まえて、この有効なツールを活用する支援を行わねばならない。

平成 27 年 9 月に閣議決定されたサイバーセキュリティ戦略をもとに、平成 28 年７月には「IoT セキュリティガイドライン ver 1.0」が発行された。

そこで我々は、「IoT を利用し企業の付加価値を高める」ことに関する深い理解と、その実現を支援するための新たな知見を、上記ガイドラインを踏まえ獲得するために、今年度は、

- IoT を語る上で必要な知識を習得し、新発想の価値創造事例を学び、
- 「IoT セキュリティガイドライン」を十分に読み解き、
- ＩＴコーディネータとしての「IoT セキュリティ」に関する知見をまとめ、
- 経営者に対して、「IT コーディネータのなすべきことは何か？新しい中小企業のビジネスモデルを創出できるのか？」を論述させて頂いた。

尚、本稿では大雑把に IoT を表現して、「IoT = M2M + AI」と定義させて頂く。

２０１８年３月

執筆者　一同

執筆メンバー　ITガバナンス研究会
久住　昭之(元 IT ｺｰﾃﾞｨﾈｰﾀ)
坂本　徳明(0064952006C)
瀬戸　昭彦(0065252006C)
滝沢　　康 (0012552001C)
千枝　和行(0029302004C)
古川　正紀(0005462001C)
牧田　一雄(元 IT ｺｰﾃﾞｨﾈｰﾀ)
山﨑　直和(0035252003C)

1. はじめに

IoT は「Internet of Things」の略で「モノのインターネット」と訳される。身の回りにある様々なものをインターネットに接続することで、新しい価値を生み出そうという取り組みである。

IoT で期待されているものの１つが、「ものづくりの現場」の安全対策である。

例えば工場設備への応用が期待されており、工場などにはパイプやケーブルなどが多く使用されているが、傷んでくると交換が必要となる。そこで振動や温度を検出するセンサーを大量に取り付け、そのデータをインターネットを経由して人工知能によって分析することで、それぞれの部品がいつ劣化するかが予測出来るという試みである。

IoT に関して先進のドイツやアメリカは、いずれも次の産業革命と位置づけるほどの勢いで注力している。国内では 2015 年の秋に、産学官の利用推進団体が設立されたほか、IoT を導入する企業に補助金を出す制度が始まってから、徐々に活動が活発になって来て居る。

しかし IoT 導入には大きな課題がある。それが「情報セキュリティ」である。

例えば、商店や工場の中に設置した防犯カメラが、勝手に覗き見られるというリスクがある。こうしたカメラはインターネットを通じて、パソコンやスマートフォンで映像を確認できる機能があり、無論勝手に他人に映像を見られないようにパスワードを設定する製品が主流ではあるが、実際には初期設定ではパスワードを設定しないようになっている製品も、国内では多く出荷されて仕舞って居る実態が在る。そのため、およそ 5000 ヶ所ものハッキングが行われている状態だと言われている。

また、世界中の多くの IoT 機器が、すでにコンピューターウイルスに感染している恐れがあるとも言われている。

サイバー攻撃の観測をしている国の研究所に依ると、観測機器に届く攻撃は 2014 年から急増していると云われている。その原因を分析したところ、多くの攻撃を仕掛けているのは、パソコンではなく、IoT 機器だということがわかったということである。機種としてはインターネットに接続されたハードディスクレコーダー、防犯カメラなどが多く、中には火災報知システム、駐車場の管理システム、ビルなどの入退室管理をする指紋スキャナなど 360 種類以上あるということである。

更に通信内容を分析したところ、そうした機器の中にはすでにコンピューターウイルスが入り込み、他の IoT 機器に感染を広げようとしている通信であることが確認できたということである。IoT 機器の中身は実際はコンピュータで、何者かがウ

イルスを使って遠隔操作したり、情報を盗み取ったりしようとしていると見られる。発信元は中国、トルコ、ロシアなどで国内の感染機器は少ないと見られるが、近年1か月平均世界の 10 万ヶ所以上から 50 万回以上の攻撃が確認できたということである。

IoT のセキュリティを高めていくためには、何よりも、メーカー側がセキュリティ対策を充分に行った IoT 機器を作ることが不可欠であるが、ウイルス感染してしまった IoT 機器を調べたところ、パソコンの世界では 15 年前に指摘された古典的な脆弱性がまだ残っているものが多いということである。

もしも、家庭の IoT 機器にウイルスが侵入すると、家庭内の情報が盗まれたり、遠隔操作によってサイバー攻撃に加担してしまうおそれもある。さらに健康状態を調べる機器に入り込むと、最悪の場合命にかかわるトラブルを引き起こすかも知れない。工場の中にはいってしまうと、事故や火災につながる可能性もある。

もうひとつの対策は、利用する我々もセキュリティ対策の確認をして導入することである。のぞき見られた防犯カメラの場合、パスワードを設定していなかったり、パスワードが簡単なものだったので、入り込まれたというケースがほとんどである。

IoT は世界中でブームになっているが、セキュリティ対策が不十分だと、パソコンとは比べ物にならない危険性があることは間違いない。利便性を重視するあまり、対策をおろそかにしないようにすることが不可欠である。

内閣府のサイバーセキュリティ戦略のなかに次のような記載がある。

「到来しつつある連接融合情報社会においては、パソコンのみならず、家電、自動車、ロボット、スマートメーターなどのあらゆるモノがインターネットなどのネットワークに接続され、そこから得られるビッグデータの利活用などにより新たなサービスの実現が可能となるシステム(以下「IoT システム」という)が普及してくる。この IoT システムの普及により、サイバー空間と実空間の融合が高度化する。今後、企業は、こうした IoT システムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる。」

本稿は企業経営を支援する ITC を対象読者とすることから、IoT を単なるモノではなくシステムと捉えるべきかと考える。

2. IoT とは何か

繰り返しになるが、IoT とは Internet of Things の略語であり、直訳すれば「モノのインターネット」になる。これだけシンプルな用語ゆえに、人によって解釈も微妙に異なり、広義の意味で使われるケースや狭義の意味で使われるケース等、様々なケースで使われているのが実状ではないだろうか。

本章では、ある程度 IoT という用語の持つ意味のイメージあわせを行いたいと考えているため、国内および海外の事例確認を含めて改めて IoT とは何かについて考察してみたい。

まず、従来の用語として良く耳にしていたと思われる「M2M」との違いについて考えてみることとしたい。IoT という用語が持つ意味は、簡単に言えば色々なモノがインターネット等のネットワークにつながることであり、この解釈の範囲では M2M との違いはそれほどない。では何が違うのか。M2M は Machine-to-Machine の略で、人が介在することなくモノ同士が相互の情報連携を行うことであるが、大きな違いは、あくまでもその情報はその対象システム内に閉じており、インターネット等を通じた外部の世界にはその情報が出回らないという点だと言える。つまり、逆の言い方をすれば、IoT とは、ネットワークでつないでモノの情報を連携するという手段こそ M2M と同じであるものの、インターネットを使って外部の様々な情報まで収集できる、さらには、収集した大量のデータを使って新たなビジネス価値を見い出すことを可能にする、という点で M2M とは決定的に違う概念だと言える。

では IoT によりどれだけの情報を収集することができるのだろう。2020 年頃には、世界中で 500 億台以上のモノがインターネットに繋がるのでは、と予想されている。この数字はとてつもない数であり、それだけのモノが相互につながり、それぞれが多くの情報を出したり受けたりすることが可能になるとすれば、インターネット上を流れる情報量はとんでもない数字になることは容易に予想できるだろう。さらにはそれらの情報を収集し、ビックデータとして管理され、最近流行りの AI 技術によって情報分析等が行われるようになれば、現時点では想像できないような新たな価値の創出も可能になるだろう。まさに IoT の真の狙いはそこにあり、そのような世界を目指して IoT は進化していくものと考えておくべきではないだろうか。

そのような前提を踏まえ、引き続き国内および海外の IoT 事例について見ていくこととしたい。

2-1. 国内事例（コマツ社の事例）

国内事例を考えるにあたり、やはり外せないのは建設機械製造大手会社「コマツ」社の事例だろう。コマツ社の IoT への取り組みは、日本が世界に誇れる最先端 IoT 事例の一つとも言えるものであり、多くの経営者が参考にしていると思われる。

それでは具体的に何がすごいのか。概要は次のとおりである。

１．KOMTRAX（コムトラックス）というシステムを構築。

２．KOMTRAX を活用して、全世界に展開する建設機械（建機）約 40 万台をネットワークで接続。

３．約 40 万台の建機を常時監視、遠隔制御。

４．GPS 技術と組み合わせて建機 1 台 1 台の所在を個体認識。

５．万が一、盗難や暴走等、トラブルが発生すれば遠隔操作で即時にエンジンカットが可能。

６．最新鋭建機にいたっては、サポートセンターから遠隔ガイドおよびコントロール等が可能。

７．その結果、新人オペレータでも難しい建機の操作が容易に可能。

上記でお分かりだと思うが、この事例のミソは、IoT を駆使することによって余計な運用コストや管理コスト、さらには人件費まで削減することができる、という点である。つまりは IoT を有効活用することで、非常に大きなメリットを得ることができることを証明した事例と言える。

ただし、このような便利な世界を誰でも簡単に作れると思ってはならない。実際、コマツ社もこの世界を築くまでに多くの歳月と投資を要したとも言われているし、おそらくこの成功に至るまで多くの失敗やチャレンジを繰り返したものと容易に想像できる。やはり、IoT を有効活用し相応の結果を出すためには、後述する情報セキュリティ問題等を含めた IoT の特性を十分に理解し、明確な企業戦略を持って取り組んでいくことが重要と考える。

【参考】

コマツのKOMTRAX （コマツのホームページから類推）

◇KOMTRAXとは

・建設機械の情報を遠隔で確認・制御するためのシステム

・全世界の約40万台の建機をインターネット上で接続、位置確認、制御。

・KOMTRAXから送信される車両情報を無償で顧客に提供。

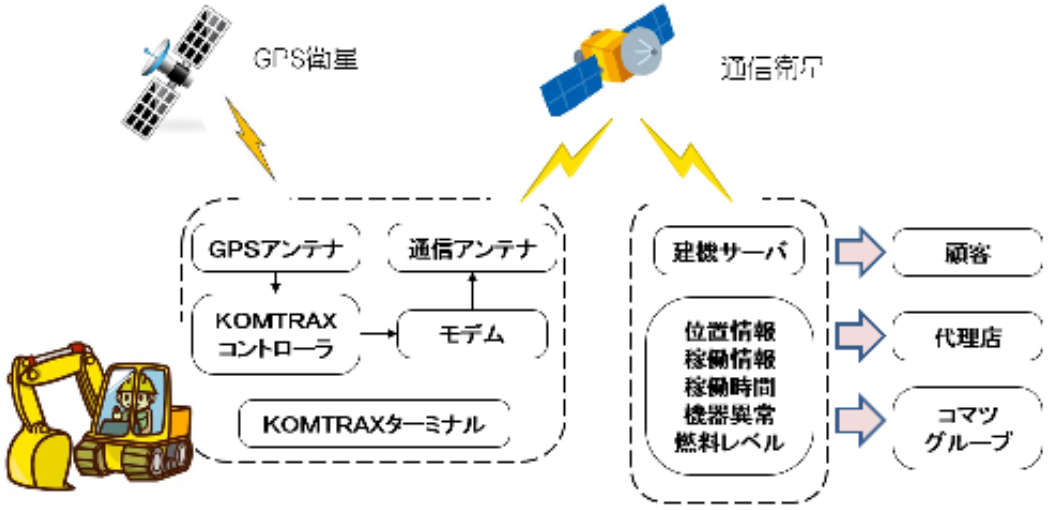

図　2−1

出典：http://www.komatsu-kenki.co.jp/service/product/komtrax/

2-2. 海外事例（GM社の事例）

次に海外事例も見てみよう。海外では IoT を活用した様々な取り組みが既に行われているが、ここでは分かり易い事例として、IoT の活用により異業種企業間連携が最も進んでいる自動車分野に焦点を当ててみたい。

近年、自動車メーカと先進 IT 企業（Apple 社や Google 社等）が手を組み、車体にインターネット機能を備えたコネクテッドカーの開発が盛んに行われている。具体的には、リアルタイムで収集された情報を活用したサービスや機能の提供や自動運転等を実現する取り組みである。

例えば、General Motors（GM）社は IBM 社と協業し、人口知能（AI）を活用した車載情報システム「OnStar Go」の開発を進めている。今現在においては、数百万台以上の GM 車に標準搭載されていると思われる。

「OnStar Go」 で実現できる機能の概要は次のとおりである。

１．利用者の同意を得て、利用者に関する様々な情報を収集＆分析。

２．AI（OnStar Go においては IBM 社の Watson）技術によって利用者の行動履歴等から嗜好や癖等を学習。

３．運転時、学習した内容と地理情報等を組み合わせて利用者が便利に思えるような情報／サービスを適宜提供。

（例１）ガソリンの消費量により給油の必要性を警告し、渋滞を避けて最寄りのガソリンスタンドまで誘導するサービス。

（例２）利用者が喜ぶようなメディアコンテンツを適宜提供するサービス。

（例３）利用者の好みに合った最寄りのレストランやショップを適宜お知らせするサービス。

（例４）車の中から欲しい商品を注文し、最寄りのショップやデパートで商品を受け取ることができるサービス。

：

いかがであろうか。前述のコマツ社の事例でも言えることであるが、IoT の世界が広まっていくことで、一昔前には思いもつかなかったような便利な世界が実現しつつある。まさに、今後の豊かな社会生活基盤を実現するためには IoT×AI は必要不可欠な技術要素なのである。

ここまでの前置きを踏まえ、次章以降では、IoT を活用するメリット／デメリット、我々IT コーディネータが支援すべき中小企業における IoT への取り組み意義、その上での IoT リスク（特にセキュリティ関連）等について深堀していくこととしたい。

3. IoT を利用するﾒﾘｯﾄ/ﾃﾞﾒﾘｯﾄ（使う事は MUST,使わないと取り残される）

3-1 第四次産業革命とIoT

今世の中で騒がれている「第四次産業革命」は

① データ収集の自動化　→IoTの活用

② データ同士の連携(データとデータをつなぐ)　→EDI：企業間情報連携

③ データ活用（分析、見える化）　→AI:データで稼ぐ

を行うことにより新たな産業構造の変革の契機として、日本経済へ大きな影響を与えると考えられている。

すなわち、あらゆるモノや情報がインターネットを通じてつながり、それらが互いにリアルタイムで情報をやりとりしつつ、人の指示を逐一受けずに判断・機能し、システム全体の効率を高めるとともに新たな製品・サービスが創出されると考えられる。

ちなみに、今までの産業革命は

第一次産業革命：動力(蒸気機関)の獲得による大量生産・高速輸送

第二次産業革命：動力の革新(モーター)による微細な制御

第三次産業革命：自動化(ICとプログラム)による省人化

であり、今後は

第四次産業革命：自立化、相互強調（IoT、人工知能、ビッグデータ、クラウド）による高度化

が始まりつつあると思われる。

出典：中小企業庁スマートSME(中小企業)研究会(第一回)　配布資料
(http://www.chusho.meti.go.jp/koukai/kenkyukai/smartsme/170329smartsme.htm)

3-2. 何故IoTを使うのか？

IoTを使うことにより、センサを用いてデータを収集し、ネットワークにより統合して処理することで、作業や状況の分析を行い、付加価値の高いサービスや効率的な業務運営に活用できる。またIoTによって集められたビッグデータをAIにより分析し、以下の様な新しいサービスにつなげることも可能になる。

【製造業】

・製造装置にセンサを搭載し、使用回数を測定し、正確な交換次期を測定。

・仕掛品の管理を一品一品のレベルで求められるばあいに、格行程に係るデータを収集し、生産の状況を顧客にフィードバック。

【ヘルスケア】

・従業員のｽﾄﾚｽチェックや運動の状況をモニタリングし、健康経営を促進。

・患者や介護者の健康状態を、モニタリングすることにより、異常発生時に性格にフィードバックする。

・要介護者の排尿のタイミングを予測しQOL(**quality of life**)の改善につなげる。

【宿泊】

・自動車のナンバーから顧客を特定し、おもてなしを行う。

・顧客の室内環境をモニタリングし、次回以降の予約の際に再現。

・温泉施設の利用状況をモニタリングし、適切な清掃のタイミングを判定。

【モビリティ】

・センサにより車外環境を測定し、運転手に伝えたり、事故の回避に活用。

【エネルギー】

・スマートメーターにより、エネルギー使用量を測定することで、効率的な利用につなげる

近年は改善傾向にあるものの、従業員一人当たりの付加価値額で見た場合、この２０年平均で見れば、中小企業は製造業、非製造業とも、労働生産性が低下してきている。

中小企業の中にも労働生産性の高い稼げる企業は存在しており、こうした企業は、成長投資に積極的に取り組んでおり、その結果　IT投資、設備投資、賃金水準がいずれも高くなっている。利益率では二極化が進んでおり、設備投資やIT投資をせっきょくてきに行う中小企業の方が、売上高・売上高経常利益率の水準が高くなっている。

また一方で今後１０年間の間に、７０歳(平均引退年齢)を超える中小企業の経営者は約２４５万人となり、うち半分の１２７万(日本企業の約３割)が後継者未定。

事業継承問題も重要な課題の１つになってきている。

going concern の観点からもIoTを始めとする技術革新に対応することは必須と思

われる。できないガラパゴス中小企業については今後の淘汰がさらに加速されると思われる。

　またITコーディネータについても従来得意としていた　IT投資が一定度存在する中堅以外の中小企業への対応を深化させて行く必要があるのではないかと思われる。

企業規模：大（積極的なIT投資、設備投資）
ITを事業部門でも十分に利活用し、収益につながっているトップ層
第四次産業革命への対応が課題であり。IoT、人工知能のツール化が必要

企業規模：中（IT投資が一定度存在）
企業組織が大きめであり、オンプレミス型を中心にITシステムを整備し、クラウド型への対応も関心がある（始めている）。
　BPRを詳細に実施するとともに、IT人材の確保やCIOの育成が課題になっている。
　　→ITコーディネータが得意とする分野

企業規模：小（IT導入が進んでいない）
企業組織が大きくなく、PCを使っていない場合もある。
「IT導入が進んでいない」というより「合うサービスが無かった」と言う状態。
　簡便なクラウドシステムに合わせて、業務を見直す形で　簡易なBPRを実施し、IoTを活用した見える化システムだけでなく、効果的なシステム導入の見える化や、ITコーディネータ（IT事業者）との連携構築に課題。

出典：経済産業省「中小企業・小規模事業者の生産性向上について」平成29年10月
出典：中小企業庁「中小企業・小規模事業者のIT利用の状況及び課題について」
　　平成29年3月

3-3. IoTに関する調査（ARM社とIBM社の共同調査結果）

ARM社（マイクロCPU）とIBM社（AIクラウド）は2016年に共同で、企業の上級幹部825名を対象として、アンケート及びヒヤリングの調査を行った。その結果、以下の様な結果が得られた（一部抜粋）。

（https://www.eiuperspectives.economist.com/sites/default/files/EIU-ARM-IBM%20IoT%20Business%20Index%202017%20copy.pdf）

IoTのビジネスへの影響について

- ・すでに大きな影響を及ぼしている　２１％
- ・現在は限定的だが将来は大きな影響を及ぼす　３２％
- ・これまでも将来も限定的なインパクト　２０％
- ・これまでは無かったが将来は大きなインパクト　１２％

IoTの導入速度について（当初の予想を下回っているか）

- ・そう思う　２４％
- ・ややそう思う　３３％

IoT導入の阻害要因について

- ・導入に必要な投資コスト　２９％
- ・セキュリティとプライバシーに関する懸念　２６％
- ・シニア経営層の知識不足／コミットメント不足　２３％
- ・組織における技術インフラが弱い　１６％

上記の調査結果を大まかに表現すると、導入のインパクトは騒がれているほどではなく、それに従ってIoTの企業への普及は半数以上の上級幹部が想定より遅れ気味であると認識している。導入に関しては、投資コストの確保・セキュリティ対策・経営者の認識不足・自社のインフラレベルの問題などが足かせとなっていると読み取れる。

4. 中小企業に於けるIoTの意義と取り組み方（ITCが考慮と指導すべき事柄）

「IoTはIT（Information Technology）とOT（Operational Technology）の融合したもの」とも言われ、その包含する範囲は「技術の情報化・データ蓄積・データ解析・新しい知見の創出・現場での判断の支援・最適化・自律化・現場への適用」と内容が広範囲で、しかもそれらを統合して考察する必要がある。

前章までで述べられた通り、IoTを導入し活用すると新しいサービスが生まれ、従来の様な「技術を売る商売」から「サービスを売る商売」へとビジネスモデルを変貌させ、新たな利益を生むことができることは、既に多くの事例を生んでいる。しかし、IoTは機器やソフトウェアパッケージの様に導入すればそれで良いという性質のものではない。そもそも、IoTを導入する理由は自社の抱えている問題を解決することであって、導入することが目的ではない。IoTの本流は、機器に対してナレッジマネジメントを適用して新しいビジネスモデルを創出する事であるから、サービスを提供する側だけではなく、サービスを受ける顧客側、サプライチェーンを形成する関係会社、技術を提供する会社、ネットワークやクラウドサービスを提供する会社などを含んだ広範囲なものになる。これらの全体を考慮に入れステークホルダーを巻き込んだ「サービスデザイン」の実施がキイポイントである。

以上のことを実施する前提で中小企業のビジネスへの適用を考えたときに、一部の経営状況が良い企業を除き、経営体力の弱い中小企業が果たして実施できるのかどうかである。IoTは決してブームではない。製造業の大きなビジネス転換である。その導入に無関心ではいられない。しかし、中小企業の現状から明らかに大企業のIoT活用と同列に議論することはできない。IoTを推進するにあたり、中小企業が実施できる場合はどの様に進めるべきかを明確にし、併せてITコーディネータが中小企業に対してどのようなアクションを取るべきかについて言及してみる。

4-1. 中小企業の現状

中小企業の製造業は大企業に比べて生産性が低いだけではなく、OECDの調査でも欧米の中小企業と比べても生産性が低い。その一つの要因が作業の標準化が進まないことと、IT化が遅れていることが原因と考えられている。また、マス生産では発展途上国が有利と言われている。大雑把に表現してみると、

① 製造指図・製造記録の様なシステマティックな手順になっていない
② 顧客の要望に細かく応えるために、熟練工の手作業が中心的になっている
③ 多品種少量生産が多い
④ ロボットなどの自動化は行われているが一部に限られている
⑤ 作業上、自動化できない部分がある製品を製造している

等が挙げられ、システマティックな作業手順とは言いがたいことが、生産性向上の妨げになっていると考えられる。

日本の中小企業は１社で成り立っているわけではない。関連する中小企業が密接に連携を取って業務を行っている。ある意味持ちつ持たれつで仕事を行っている訳で、１社だけ飛び抜けるわけにはいかないという事情がある。また、実際のところ、地方に行けば仕事の割り振りの調整、つまり談合的な行為が一部で行われていると言われている。

多くの中小企業は仕事のやり方を他社とベンチマーキングしているわけではなく、そもそも自社の社員の行動や業務プロセス、資源の使い方について調査が行われていない企業が多い。自社の実態が把握されていないのである（独立行政法人経済産業研究所の調査）。IoT化は勿論、IT化の推進を行うにあたって、まず自社の見える化に取り組まなければならない。

中小企業庁の調査では、中小企業のIT化は進んでおらず、以前から懸念されていた。独立行政法人経済産業研究所の調査でも同様の結果であるが、その多くはITの担当者が不在、もしくは会計や給与パッケージの管理を兼任で行っている程度である。逆に表現すると、中小企業でもITを活用している会社は専任のSEが存在している。SEの専任者の設置に関しては、経営者自身が設置の決断をしている、という特徴を挙げることができる。中小企業では経営者の判断が大きな比重を占めている。

中小企業の生産性が低いということについては、当事者の中小企業よりは経済産業省や中小企業庁の方が関心を持って注視している。しかしながら、中央官庁は合理化推進と言っているが、そこには中小企業側の事情がある。例えば、ロボットの様な自動処理を行う機器を導入すれば合理化が可能と考えられるが、中小企業の場合は人件費の方が安いので機器の導入は高くつく。また、人手の場合は一つの作業だけではなく、他の作業もこなしてくれるので利用価値が高い。

中小企業の多くは自社の技術に付加価値を付けることで顧客の取り込みをはかり、利益を得ているため、自社の生産性の向上は二の次扱いになっていると思われる企業が多い。

4-2. 中小企業はIoTをどのように捉えているか

まず最初に、経済産業省が行った2016年の中小企業に於けるIoTの調査（三菱総研が受託）の結果を参照してみる（回答46社）。

（http://www.meti.go.jp/meti_lib/report/H28FY/000642.pdf）

それによると、以下の様な結果であった。

IoTの取り組み状況（N=53）

・すでに導入済み	７．０％
・導入を検討中	２３．３％
・何もしていない（調査中）	５１．２％

IoTに対する期待効果

・生産リードタイム削減	８社
・製品のトレーサビリティ向上	８社
・社内コミュニケーションの円滑・強化	７社
・新製品・新サービス開発	６社
・製品のカスタマイズ	５社

IoTを導入中に発生した課題

・社内リソース（特に資金）不足
・プロジェクトマネージャの不足（社長が代行）
・社員が積極的に取り組む雰囲気が無かった
・ソフトウェア・ハードウェアの技術者不足

IoT未導入の理由

・IoT導入の進め方が分からない	１１件
・導入効果が分からない・得られない	９件
・社内リソース（特に資金）の不足	８件
・他に優先順位の高い取り組みがある	７件

大まかに要約すると、導入の効果が分からないし資金も足りない、社内にこの作業に適した人材もいないし、他に優先順位の高い仕事があり、IoTなどは優先順位が低いので進んでいないと読み取れる。導入に関する効果でも、リードタイム短縮や社内コミュニケーションの向上など、先進大手企業が持っている製品の付加価値付与や顧客の利益向上による利益獲得などの認識が低いことが分かる。

大部分の中小企業の製造業は、その仕事の性質上IT化にはなじみが薄い。ましてや、殆どの中小企業はIoTに関心を持っていないことは、調査からも推察できる。

IoTがどういうものか理解できてない事は、実態が分からないということもあるが、社内にIoTを理解する人材がいないことも挙げられる。これも調査結果から読み取れる。従って、経営者にIoTの効用を伝える人材がいないため、経営者も関心を示すことができない。

中小企業がIoTを推進するためには、明らかに外部の支援が必要である。しかも、ほとんどゼロからの出発であるため、支援は時間をかけて継続的に進める必要がある。ITコーディネータにとってビジネスチャンスともとれるが、ゼロからIoT稼働までを支援する必要があるため、かなりの労力が必要と予想できる。特に導入のご利益が理解できていないし、個々の中小企業にとってのご利益も明確になっていないわけで、それらを明確にする過程も支援していく必要がある。

企業がIoTを導入するのは、自社の抱えている問題をIoTを通じて解決するためであり、経営上、IoT導入は決して必要なことではない。事実、スイスの高級腕時計会社RorexはIoTを導入しないと宣言している。

ただ、いくつかの導入事例を見てみると、社内のどこかで成功事例が生まれるとそれを横展開できるのではないかという提案が出される様で、まずやってみて成果に結びつけるためのスタートを切ることがポイントである。

中小企業のIoTの視点からのSWOT分析

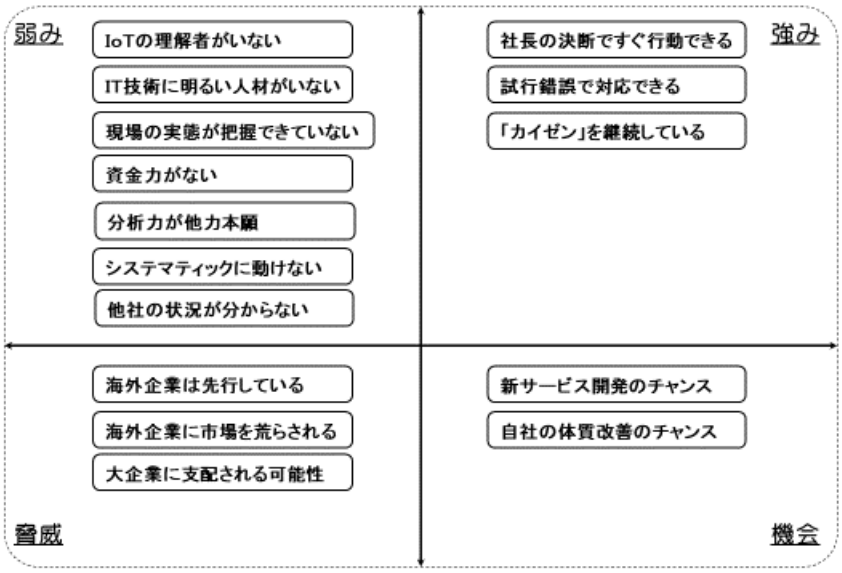

図 4－1

この項のまとめとして、なぜ中小企業で進まないのかというと、IoTに取り組んだ場合のコストや労力などの負担がどうなるかが分からないし進め方もわからない、どういう結果になるのかも見えないので、手が付けられないのである。

4-3. 中小企業のIT化の現状

前項までで述べたとおり、規模が小さい中小企業ほどIT化が進んでいない傾向にある。その大きな原因が、製造工程の作業自体がIT化になじまないものが多い為で

ある。

独立行政法人経済産業研究所の調査によると、IT化どころかそもそも自社の業務運用に関して、稼働状況のモニタリングが出来ていない企業が多い。つまり、業務がどのように進められているのかの実態を、経営者自身が把握できていない。これでは、IT化に着手するどころではない。まず業務の見える化に取り組まなければならない。

規模の小さな会社では、IT担当者と言っても会計や給与のパッケージ管理を兼任で行っている程度の会社が多い。例えば、いまだにFAXを使っていて何の疑問も考えない企業が多い。冒頭にも述べたが、その中でもIT化を行って成果を上げている企業がある。そういう企業は規模が小さくても専任のSEを配置している。経営者の決断で、そのような措置が取られている。IT化を行う上でも、IoT化を行う上でも人材がいないのが難点である。また、周囲の企業の様子を見て、他社がやっていないのなら何も自社が先頭に立ってやることはないという、ヒューリステックな反応をしたがる傾向も見逃せない。

IoTの取り組みを行う上でも、同様のことが要因として考えられる。

4-4. IoTを取り入れるためにどのように考えるべきか

IoTというものは分かりやすく表現すると、一昔前に流行っていたナレッジマネジメントを機器の稼働や工場のプロセス管理に応用しようというものである。つまり、今まで暗黙知だった情報を価値のある形式知にして、新しいサービス提供にビジネスをシフトしている。IT中心や機器中心ではなく、顧客の利益最大化の価値発見がポイントである。従って、IoTは機器の導入などと違って、先進企業を訪ねて結果を見せられても導入には結びつかない。なぜ導入しなければならないのか、更には導入していく過程が理解できないとまるで手が付けられない。

まず、IoTがどのようなものかを理解することから始めることである。大企業の様に、専門家を招いて調査分析をし、グランドデザインを行って導入していく、などということを行うわけにはいかない。未知のものに投資するわけにはいかない事情を理解する必要がある。

最初はコストをかけずに一部で実験的にやってみる事が大切である。インターネットを意識する必要もない。対象機器を選定し、汎用的で簡単な仕組みのセンサーを付けてデータを収集し分析してみる。データを分析し、結果を考察すると、利用の仕方が見えてくる。

センサーのデータを集めて解析し考察し、有効な利用方法を見つけられる、とい

う経験を一度体験すると、IoTということに対して一つのイメージがわいてくる。そうすると次々にアイデアが沸き上がって、次に展開できる対象を検討するなどということに発展し、段階的に拡大していけることが理解できる。社内全体にこの状態を作ることが大切である。その段階まで到達したならば、外部の専門家を招いて相談してみるのが一つの方法と言える。

この様に、自社の対象が洗い出せた段階で、IoTに取り組む手順を確認すると、以下の様な事柄が考えられる。

① IoT化可能な対象機器を洗い出す
② 自社全体の製造工程上、又は製品にマッピングしてみる
③ インターネット上のM2Mにデータを集約した方がいい機器と、単独で運用した方がいい機器とを仕分ける
④ IoTの専任者を選定する
⑤ 自社に適したM2Mサービスを選択する
⑥ 部分的に稼働させて結果を評価する
⑦ 段階的に拡大していく

IoTをどのように利用していくのかは、決まった方式があるわけではない。情報を集めればそこからナレッジが自動的に湧き上がってくるわけでもないし、他社の真似をすればよいというものでもない。やはりその都度、創意工夫が必要になる。他社の事例を参考にしながら自社の事業を考え合わせて、独自の利用方法を考え出す努力が必要になる。

IoT化は単にデータの収集を管理するだけではなく、解析結果を組み合わせて新しいサービスを生み出すことが大切である。その為には、社内にデータサイエンティストを育成する必要があり、専任者を選んでおかなければならない。

4-5. IoT等とブームになる前から中小企業でもIoT導入を行っている企業がある

事例については、IoT研究会の検討結果を引用する。

○愛媛県松山市にあるボイラの製造・販売・メンテナンスを行うM社。

ボイラの製造・販売メンテナンスを行っているが、普通に商売をしたら価格やサービスで大手に勝てない。1989年に社長の決断で、顧客に販売するボイラにセンサーを取り付け、通信回線を通してセンターで技術者が稼働状況を確認する仕組みを構築した。遠隔診断監視サービスである。異常が検知されれば、直ちに技術者を派遣して対応した。その為、ボイラが故障・停止する前に修理が行われる為に、顧客の稼働に影響を与えない。典型的な予防保守である。

故障しないボイラ、停止しないボイラとして評判を集め、多数のリピーターを

獲得することで、売り上げを伸ばしている。

4-6. IoT導入のプロセス

中小企業がIoTを導入する場合に、特別決まったプロセスがあるわけではない。大まかに以下の様な段階を踏んで進めていくとよい。

1）自社の現状を把握する

JQA（日本経営品質大賞）のチェックリストやバランススコアカードなどを利用し、自社の状況を見える化しておく。特に自社の抱えている問題を明確にし、社内で共有しておく必要がある。

2）IoTの教育を従業員に行う

集合研修、先進事例企業の訪問などで、IoTがいかなるものかの理解を深めておく。

3）自社の投資可能な範囲を決める

要員や資金的な制約があるので、投資可能な範囲を決めておく。

4）専任者・専任組織を選定する

5）部分的に試行する

手を付けやすい機器から始めるのが賢明である。

6）適用可能な範囲を決める

製造設備もしくは製品でセンサーを取り付けて管理できる範囲をマッピングしておく。

7）利用可能なサービスを調査する

日本のM2Mサービスはキャリア系（通信会社）が多いが、既にアメリカのGEのPredixなどもサービスとして提供されている。

8）全体の設計を行う

この作業は、外部の専門家に依頼して、設計してもらう。

9）部分的に導入し、結果を評価する

社内にデータサイエンティストを要請する必要があるので、外部の専門家の指導を受けながら、データ解析と結果の評価方法を学ぶ必要がある。

10）段階的に拡大していく

11）稼働結果を評価する

12）問題点を明確にし、フィードバックする

直ぐに対応する必要があるものと、後で対応してもいいものとを振り分け、順番に対応する。

IoTは特に決まった方法があるわけではないので、中小企業の場合は出来るところから行うことが賢明である。

4-7. ITコーディネータ側の問題点

IoTを中小企業に導入するにあたって、代表的なITコーディネータの可能性や問題点を考察しておく必要がある。

ITコーディネータの強みは端的に言って、

① IT技術やその導入技術に精通している
② 経営戦略と結びつけて考えることができる
③ IT関連の情報につき、情報交換や連携ができる
④ ITだけではなく、通信技術も合わせて理解している人が多い

であるが、IoTの導入を考えたときに考えられる弱みは、

① 工場の生産システムは自身の業務外で知識に乏しい
② IT技術のみでセンサーやAIの分かる人が少ない
③ IoT技術に対して理解の浅い人が多い

である。

生産システムはその多くが工場のエンジニアがシステムを構築することが多いため、基幹系のエンジニアはERPと工場システムの情報接続を行っているだけで、生産システム側の詳細知識に乏しい。これではIoTを進めることは難しく、生産システムを勉強する必要がある。

ITコーディネータがIoTを中小企業に導入するのであれば、更にクラウドの知識やデータベースの操作技術、データサイエンティスト（AIの機械学習や統計解析）の知識が必要であり、学習範囲が広いため、機会をとらえて継続的な勉強をする必要がある。

IoT製品を開発するためのシステム構成

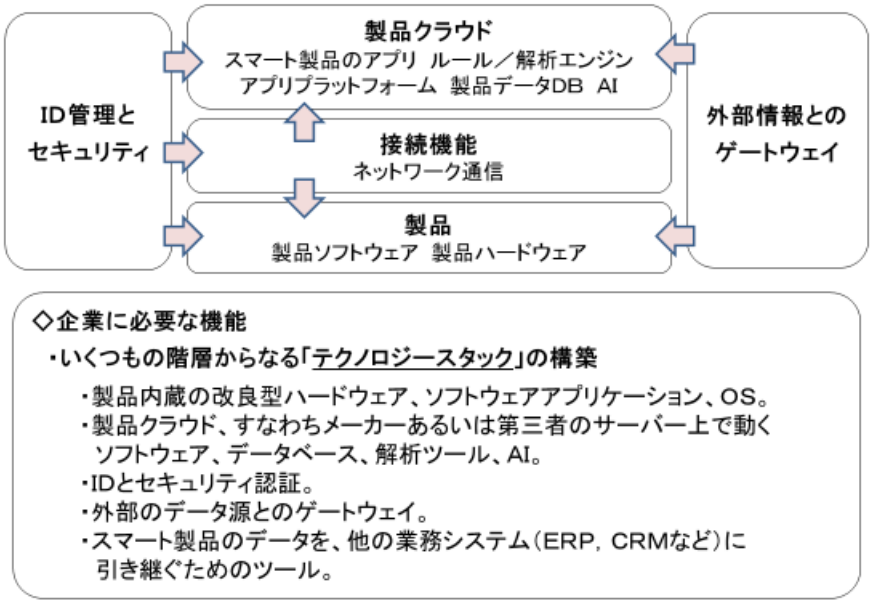

図 4－2

4-8. 中小企業のIoT化に対する経営者の役割

中小企業のIT化に成功している企業はいずれの事例でも経営者が決断し、先任者を設置しているという特徴がある。それは、IoTにもそのまま当てはまり、IoTを推進している会社はIoTの専任職・専任組織を設けている。

もう一つの特徴は、中小企業は経営資源に乏しいので自前で揃えるよりは外部調達に依存した方が効率が良いため、これらを明確に区分している。投資の指向と集中を決断しなければならない。

自社だけではなく共同で作業をした方が資源の有効活用が期待できるが、共同ビジネスを行うためには、そのグループ内で共通尺度を確立しておく必要がある。これも経営者の役割である。

IoTは機器の運用に関するナレッジ創出を前提にしているため、従来の考え方の延長を改める取り組みを行う。当然、従来のやり方から変わるので、同調できない従業員の社内的抵抗を受けることを予想しなくてはならない。それらを抑えて、IoT導入に社員を向かわせるのも経営者の役割である。

IoTは自社内に無い機能を利用しなければならないケースも出てくるので、当然ながら人材育成や技術調達は外部サービスを利用することになる。

再度やるべき事を整理して表現すると、以下の様になる。（IoT研究会資料等）

① 自社の改善したい点を明確にする
② ITの利用基盤を構築する
③ 自社で行うべきこととアウトソーシングすべきことを明確にする
④ 自社内でIoTの稼働を促進する専門チームを構築し、自社内連携を図る
⑤ 情報分析し、新たなビジネスモデル（ナレッジ創造）を創出する

5. 企業経営と IoT セキュリティ

これまでのセキュリティ対策が主に企業内を対象にしていたのに対して、IoTセキュリティは、インターネットを介した企業と企業、企業と社会を対象にしなければならないことから、サイバーセキュリティの観点で考える必要がある。そこで、まず我が国のサイバーセキュリティ戦略におけるIoTセキュリティの捉え方をおさえ、その上で企業経営におけるIoTセキュリティに述べる。

5-1.　サイバーセキュリティ戦略と IoT

2014 年 11 月に成立した「サイバーセキュリティ基本法」第１２条の「サイバーセキュリティに関する基本的な計画を定めなければならない」という規定に基づき、2015 年 9 月 4 日にサイバーセキュリティ戦略が閣議決定された。

サイバーセキュリティ戦略の目的は、「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の 活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会 の平和・安定及び我が国の安全保障」に寄与すること」としている。

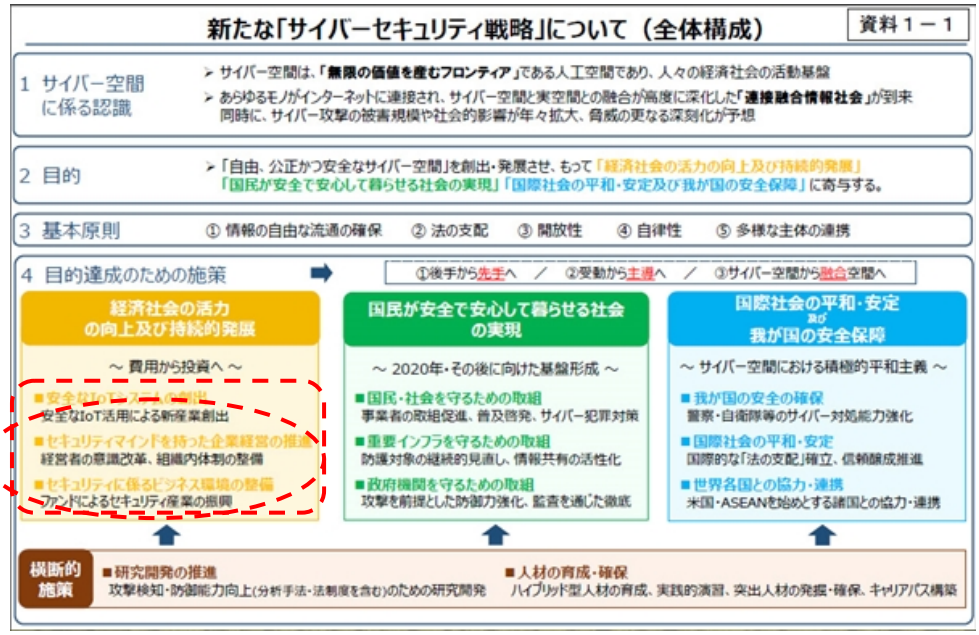

図 5-1　サイバーセキュリティ戦略全体像

この戦略の中で、IoT の重要性について次のように述べられている。

実空間のモノやヒトが、サイバー空間上の情報の自由な流通とデータの正確な通信により物理的制約を超えて多層的につながる（連接する） ことで、実空

間とサイバー空間の融合が高度に深化した社会、すなわち「連接融合情報社会」が到来しつつある。連接融合情報社会は、革新的なサービスを創出し、新たな値を幾何級数的に産み出すことができる社会である。
連接融合情報社会においては、パソコンのみならず、家電、自動車、 ロボット、スマートメーター等のあらゆるモノがインターネット等のネットワークに接続され、そこから得られるビッグデータの利活用等により新たなサービスの実現が可能となるシステム（以下「IoT システム」という。）が普及してくる。そして、この IoT システムの普及により、サイバー空間と実空間の融合が高度に深化する。今後、企業は、 こうした IoT システムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる。このため、我が国企業がこうしたビジネスチャンスを確実に捉えることは、我が国の経済社会の活力の向上及び持続的発展にとって極めて重要である。

こう述べた後、企業が、IoT システムを通じて新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「セキュリティ品質」が保証されていることが前提であるとし、IoT システムの提供するサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減していくことが、今後の社会全体としての課題（チャレンジ）となるとしている。

また、その具体的な施策として次の 3 つの視点から述べられ、IoT セキュリティの重要性が施策として取り上げられている。

(1) 安全な IoT システムの創出
(2) セキュリティマインドを持った企業経営の推進
(3) セキュリティに係るビジネス環境の整備

企業の経営を IT で支援する IT コーディネータとしては、「セキュリティマインドを持った企業経営の推進」が施策として取り上げられていることに注目すべきであろう。すなわち、IoT セキュリティはセキュリティマインド持った企業経営の推進とあわせて考える必要があると捉えるべきであろう。

これら 3 つの施策のなかで、IT コーディネータが考えるべきポイントとして、「(1) 安全な IoT システムの創出」、および、「(2) セキュリティマインドを持った企業経営の推進」を取り上げ論考する。

5-2. 安全な IoT システムの創出

安全な IoT システムを創出するには、IoT 機器やシステム、サービスの供給者及び利用者を対象として、サイバー攻撃などによる新たなリスクが、モノやその利用者

の安全や、個人情報・技術情報などの重要情報の保護に影響を与える可能性があることを認識したうえで、IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するする必要がある。

そのためには、まず、IoT とは何か、IoT にはどのような特性があるのかを理解する必要がある。

5-2-1. IoT 特有の性質

IoT の進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT 特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要である。一般的な IoT 機器特有の性質を次に挙げる。

（性質１）脅威の影響範囲・影響度合いが大きいこと

IoT 機器はインターネット等のネットワークに接続していることから、ひとたび攻撃を受けると、IoT 機器単体に留まらずネットワークを介して関連する IoT システム・IoT サービス全体へその影響が波及する可能性が高い。

（性質２）IoT 機器のライフサイクルが長いこと

IoT 機器として想定されるモノには 10 年以上の長期にわたって使用されるものも多く、構築・接続時に適用したセキュリティ対策が時間の経過とともに危殆化することによって、セキュリティ対策が不十分になった機器がネットワークに接続されつづけることが想定される。

（性質３）IoT 機器に対する監視が行き届きにくいこと

IoT 機器の多くは、パソコンやスマートフォン等のような画面がないことなどから、人目による監視が行き届きにくいことが想定される。

（性質４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること

IoT 機器側とネットワーク側それぞれが有する業態の環境や特性が、相互間で十分に理解されておらず、IoT 機器がネットワークに接続することによって、所要の安全や性能を満たすことができなくなる可能性がある。

（性質５）IoT 機器の機能・性能が限られていること

センサー等のリソースが限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合がある。

（性質６）開発者が想定していなかった接続が行われる可能性があること

IoT ではあらゆるものが通信機能を持ち、これまで外部につながっていなかったモノがネットワークに接続され、IoT 機器メーカやシステム、

サービスの開発者が当初想定していなかった影響が発生する可能性がある。

このように、IoT はこれまでのセキュリティ対策の知識・知見では対応できない特性をもっていることを IT コーディネータは十分認識する必要がある。

5-2-2.　IoT システムの特性

IoT は「モノ」がネットワークにつながって新しい価値を生むだけでなく、IoT が他の IoT とつながることでさらに新しい価値を生むという”System of Systems（SoS）”としての性質を持っている。つまり、「モノがつながった IoT(System)」と「モノがつながった IoT(System)」がつながることが System of Systems である。「モノがつながった IoT(System)」は単独で機能するし、つながっても独立して機能する。さらに、つながることにより新たな目的や機能を実現し、継続的に進化する特性を持っている。

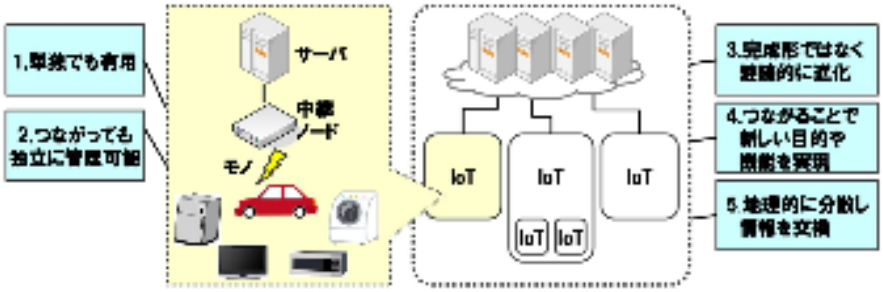

図 5-2　System of Systems のイメージ

つぎに、IoT をシステムとしてとらえた場合の特性を、人の視点から考えてみると、図 5-3 のようなイメージになるであろう。

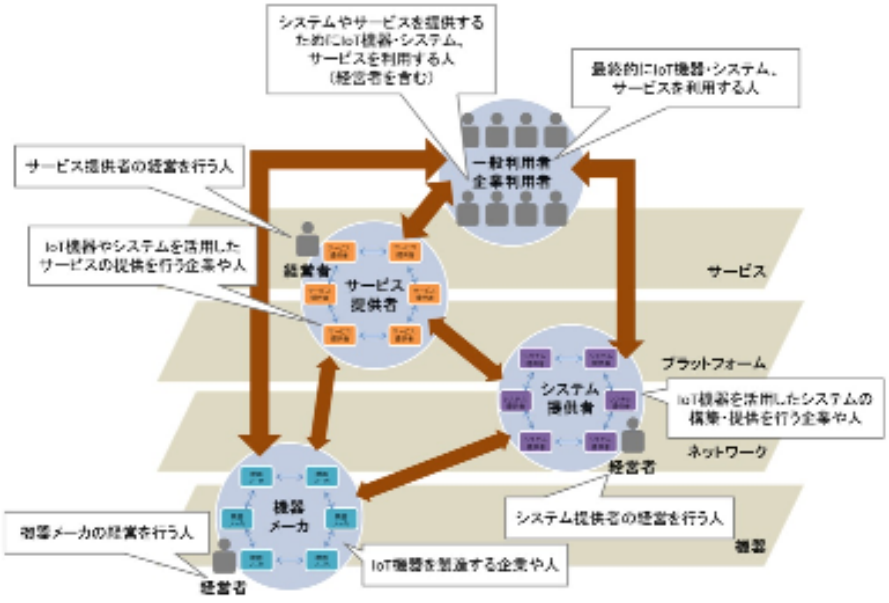

図 5-3　IoT システムに係る人のイメージ

このイメージから次のような IoT システムに関係する人が浮かび上がる。

①サービス利用者

一般利用者

最終的に IoT 機器・システム、サービスを利用する人

企業利用者

システムやサービスを提供するために IoT 機器・システム、サービスを利用する人（経営者を含む）

②サービス提供者

IoT 機器やシステムを活用したサービスの提供を行う企業や人、およびその経営を行う人

③システム提供者

IoT 機器を利用したシステムを構築・提供を行う企業や人、およびその経営を行う人

④機器メーカー

IoT 機器を製造する企業や人、およびその経営を行う人

IoT システムでは複数の IoT 機器・システムやサービスを相互に利用して、機能やサービスを実現することも多く、 システム提供者やサービス提供者はそれぞれが利用者であることも認識する必要がある。

たとえば、自動車産業の「コネクテッドサービス」を例にとると、「機器メーカー」は「自動車会メーカー」であり、「システム・サービス提供者および企業利用者」は「自動車メーカー」および「ネットワーク事業者」、「一般利用者」は「自動車の所有者、運転手」となる。

5-2-3.　IoT セキュリティ対策の指針

IoT 機器の開発から IoT サービスの提供までの流れを、「方針」、「分析」、「設計」、「構築・ 接続」、「運用・保守」の 5 つの段階に分け、さらにサービスの利用者として「一般利用者」を加え、それぞれの段階に対するセキュリティ対策指針が示されている。なお、既存の安全確保や性能に関する法令・規制要求事項が存在している分野については、それらを順守することが大前提である。その上で、それぞれの分野におけるリスクや事故発生時の対応を考慮し、実施の要否も含め、IoT セキュリテ

ィ対策を検討することが重要である。

セキュリティ対策指針の一覧を以下に示す。

	指針	主な要点
方針	IoT の性質を考慮した基本方針を定める	・経営者が IoT セキュリティにコミットする ・内部不正やミスに「備える
分析	IoT のリスクを認識する	・守るべきものを特定する ・つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	・つながる相手に迷惑をかけない設計をする ・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 ・安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	・機能および用途に応じて適切にネットワーク接続する ・初期設定に留意する ・認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	・出荷・リリース後も安全安心な状態を維持する ・出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える ・IoT システム・サービスにおける関係者の役割を認識する ・脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		・問い合わせ窓口やサポートがない機器やサービスの購入を控える ・初期設定身気を付ける ・使用しなくなった機器については電源を切る ・機器を手放すときはデータを消す

表 5-1 IoT セキュリティ対策指針一覧

IoT は、これまで論考してきたような様々な特性をもっていることから、IT コーディネータは、自らが支援する企業が IoT システムのどのような立ち位置にあるのかを分析したうえで、IoT セキュリティ対策を支援する必要がある。

詳しくは「IoT セキュリティガイドライン」を参照願いたい。

5-3. セキュリティマインドを持った企業経営の推進

前節では、サーバーセキュリティ戦略のなかでIoTセキュリティに関する重要施策とされている施策のひとつの「安全なIoTシステムの創出」について述べた。本節では、同じく重要施策である「セキュリティマインドを持った企業経営の推進」について述べる。

サイバーセキュリティ戦略では、IoTシステムによる連接融合情報社会における企業経営に当たっては、従前からのサイバーセキュリティ確保のための取組はもとより、新たなビジネスの創出等のためにも、これまで以上に、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることが必要であり、セキュリティマインドを持った企業経営を浸透させることを目指し、以下の取組を実施するとしている。

(1) 経営層の意識改革

セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、我が国の経済社会の活力の向上及び持続的発展のために必要であり、サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。

(2) 経営能力を高めるサイバーセキュリティ人材の育成

経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う橋渡し人材層の育成を推進する。

(3) 組織能力の向上

企業における製品・サービスの関係者がセキュリティ・バイ・デザインを共通の価値と して認識することを促していく。また、営業秘密保護や事業継続の観点から、リスク分析に基づく組織運営を行うよう促していくなど、有効な経営の在り方を発信・推進する。組織の壁を越えたサプライチェーン全体でセキュリティを向上するための方策を講じていく。

これらの具体的な策としてつぎのような施策が実施されている。

- 2015年12月28日、経済産業省が「サイバーセキュリティ経営ガイドラインVer1.0」を策定
- 2016年8月2日、内閣官房が「企業経営のためのサイバーセキュリティの考

え方」を決定。
・ 2017 年 11 月 16 日、経済産業省が「サイバーセキュリティ経営ガイドライン Ver.2.0」を策定。

経済産業省が策定した「サイバーセキュリティ経営ガイドライン」は、内閣官房が決定した「企業経営のためのサイバーセキュリティの考え方」の影響を受けている。「サイバーセキュリティ経営ガイドライン Ver.1.0」と「同 Ver.2.0」の違いは、冒頭の「サイバーセキュリティ経営ガイドライン・概要」にみることができる。「Ver.2.0」の概要には、「Ver.1.0」にはなかった次の記述がある。

・ IoT といった新たな価値を生み出す技術が普及しつつある中で、AI やビッグデータなども活用した、新しい製品やサービスを創造し、企業価値や国際競争力を持ったビジネスを構築していくことが企業として求められている
・ セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である
・ サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である

このように IoT は企業経営に大きく影響することが分かる。IoT は単にモノとモノがインターネットを介してつながることではないことを IT コーディネータは認識すべきである。また、有効な IoT セキュリティ対策を講じるうえで、IT コーディネータはサイバーセキュリティ経営ガイドラインに関する知見も求められるのである。

5-3-1. サイバーセキュリティ経営ガイドライン概説

経済産業省が策定したサーバーセキュリティ経営ガイドラインの背景には IoT システムの普及があることはすでに述べた。すなわち、IoT システムの普及により、サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大する。セキュリティリスクは目に見えないため、特別なものと見がちであるが、数あるリスク管理の一項目に過ぎない。また、サイバーセキュリティをやむを得ない「費用」と見る傾向があるが、より積極的な経営への「投資」と位置づけるべきである、という考え方である。

この考え方に基づき、今後のビジネス環境の変化とサイバーセキュリティの関係を考慮すると、次のことを認識して、企業経営の中でサイバーセキュリティに取り組むことが重要である。

① サイバーセキュリティは、利益を生み出しビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

② 全てがつながる社会において、サイバーセキュリティに取り組むことは、社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

このような背景でつくられたこのガイドラインは、「サイバーセキュリティ経営の3原則」と「サイバーセキュリティ経営の重要10項目」から構成され、これに現場担当者向けのチェックシートや具体的な対策方法をまとめたつぎの付録が付随する構成となっている。

付録 A 重要１０項目が適切に実施されているかどうかを確認するためのチェックシート
付録 B サイバーセキュリティ対策を実施する上で参考となる資料等
付録 C インシデント発生時に原因調査等を行う際、組織内で整理しておくべき事項
付録 D 重要１０項目と ISO/IEC27001、27002 の関係性

5-3-2. 経営者が認識すべき 3 原則

経営者は、以下の３原則を認識し、対策を進めることが重要であるとしている。
(1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
(2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開 示など、関係者との適切なコミュニケーションが必要

原則１は、経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施すべきであり、経営者自らがリーダーシップを発揮して適切な経営資源の配分を行うことが必要であるということである。

原則 2 は、自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきということである。

原則 3 は、平時からステークホルダー（顧客や株主など）を含めた関係者にサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきということである。

5-3-3.　経営者が認識すべき 10 項目

経営者は、サイバーセキュリティ対策を実施する上での責任者となる担当幹部に対して以下の重要１０項目を指示すべきであるとしている。

＜サイバーセキュリティリスクの管理体制構築＞
指示１　：サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２　：サイバーセキュリティリスク管理体制の構築
指示３　：サイバーセキュリティ対策のための資源（予算、人材等）確保

＜サイバーセキュリティリスクの特定と対策の実装＞
指示４　：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５　：サイバーセキュリティリスクに対応するための仕組みの構築
指示６　：サイバーセキュリティ対策における PDCA サイクルの実施

＜インシデント発生に備えた体制構築＞
指示７　：インシデント発生時の緊急対応体制の整備
指示８　：インシデントによる被害に備えた復旧体制の整備

＜サプライチェーンセキュリティ対策の推進＞
指示９　：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞
指示１０：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

これらの 10 項目の詳細は「経営者に対する問いかけ」「対策を怠った場合のシナリオ」「対策例」によって解説されている。また、問いかけはチェックリストと連動する形で提供されており、経営者とのコミュニケーションツールとして使うことができる。

5-3-4.　サイバーセキュリティ経営ガイドラインと ITC

多くのガイドラインがそうであるように、サイバーセキュリティ経営ガイドラインも記述を簡潔にしているため、内容の実践に関する具体的な記述は含まれていないので、経営者は具体的に何をして良いのかわからないのではないだろうか。IT 活用について十分に指示を出せていない状況で、サイバーセキュリティについてリーダーシップを取るというのは、経営者にとって負担でしかないように思える。そこで IT コーディネータの出番である。

本ガイドラインを経営者と IT コーディネータとのコミュニケーションのツールと

して使うのはどうであろうか。たとえば本ガイドラインの「サイバーセキュリティ経営ガイドライン・概要」と「1.はじめに」を資料にして、現在のクライアント企業の取り組みについて経営者と話し合い、サイバーセキュリティに対する考え方を教示しながら、目標と体制についてある程度の取り決めができればよいのではないか。

企業経営において求められているのはガバナンスであり、求められているのはセキュリティの維持ができていることの把握である。自らが設定したセキュリティ機能が維持されていることを常に把握しておくことが重要である。そのためには、セキュリティ機能の評価を行い、その評価の結果を定期的に、1 年という長いスパンではなく、もっと短期的に、できればリアルタイムに実施できるような環境を構築することが経営者に求められる。それを支援するのも IT コーディネータの役目である。

詳しくは「サイバーセキュリティ経営ガイドライン」を参照願いたい。また、同ガイドラインの実践に必要な具体的なことについて、IPA が「サイバーセキュリティ経営ガイドライン解説書」を作成している。この解説書は、同ガイドラインの中でも特に重要となる対策や考え方について具体的に説明されているので、そちらも併せて参照されたい。

5-4. 企業の視点による違い

企業が投資すべき対象や経営リスクは様々であり、各企業の人的・金銭的 資源にも限りがあることから、IT の利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある。このため、サイバーセキュリティに対する企業の視点別に分けると次のように分類できるであろう。

① IoT システムの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業 （IoT システムによる革新と高いレベルのセキュリティに積極的に挑戦するあらゆる企業）
② IoT システム・セキュリティをビジネスの基盤として捉えている企業（IoT システム・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）
③ 自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業（主に中小企業等のうちセキュリティの専門組織を保持することが困難な企業）

IT コーディネータは、自らが支援する企業がこれらのうちどれに該当するのかを見極める必要がある。これらの企業それぞれについて、経営者に求められる振る舞いとツールについて述べるので参考にしていただきたい。

5-4-1. IoT システムの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業

（経営層に期待される“認識”）

情報・データの積極的な活用に伴うリスクへの対応も含め、その製品やサービスの「セキュリティ品質」を一層高めるため、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組むことが必要である。また、この分類となる企業群は、決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。

（実装に向けたツール）

✓ 「IoT セキュリティに関するガイドライン。」

5-4-2. IoT システム・セキュリティをビジネスの基盤として捉えている企業

（経営層に期待される“認識”）

経営者自らが、担当者任せにすることなくリーダーシップをとって、セキュリティ対策を講じることが必要である。また、情報やデータが企業や国境を越えて共有されるよう、自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、委託先を含めてのセキュリティ対策が必要となる。さらには、平時及び緊急時のいずれにおいても、セキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要である。

（実装に向けたツール）

✓ 「サイバーセキュリティ経営ガイドライン」

5-4-3. 自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業

（経営層に期待される“認識”）

社会全体の IT 化が進む中、顧客に対する責任の観点から、サプライチェーンを通じて中小企業等の役割はますます重要となると考えられる。そうした中で、セキュリティ対策は不可欠であり、対策が不十分である場合には、顧客情報や取引先等から預かった機密情報の流出等によって、消費者や取引先との信頼関係を低下させ、取引の機会損失につながる。そのため、経営層自らが積極的にサイバーセキュリティに関心を持ち取り組むべきである。 一方、中小企業等においては、様々な経営リスクがある中で、使えるリソースには限界があることから、外部の能力や知見を活用しつつ、効率的に進める方策を検討すべきである。

（実装に向けたツール）

✓ 「中小企業の情報セ キュリティ対策ガイドライン」

６．そこでITｺｰﾃﾞｨﾈｰﾀのなすべきことは何か？

IoTの時代に中小企業を支援する立場であるＩＴコーディネータが新たに注力して持つべき技術として、以下の技術を指摘させて頂いた。

・IoTの基本的技術

・精算システム及びセンサー技術

・クラウド、データベース操作技術、データサイエンティスト(ＡＩの機械学習)の知識

更には、

・サイバーセキュリティに関する知識、も必須となる。

個々の知識を深いレベルで習得頂くに越したことはないが、不得手な分野は、それを補う専門家と組んで対応するなどの方策を採用されて、対応して頂きたいところである。

中小企業のIoT化に対する経営者の役割、経営者の決断は、自身が先頭に立つ強い意思表示と、迅速な対応であることは既に述べさせて頂いた。

この経営者の方たちを支援する立場にある、ITC の役割も理解頂けたのではないかと思う。

最後に、本論文が読者諸兄の役に立てれば幸いである。

以上

参考資料：

１．「サイバーセキュリティ戦略」(内閣サイバーセキュリティセンター)

２．「サイバーセキュリティ経営ガイドライン Ver1.0」(経産省、IPA)

３．「サイバーセキュリティ経営ガイドライン Ver2.0」(経産省、IPA)

４．「中小企業の情報セキュリティ対策ガイドライン（第 2.1 版)」(IPA)

５．総務省 サイバーセキュリティタスクフォース(第１回) 配布資料

６．Japan Security Vision 2017(3 月 2 日開催) NISC(内閣サイバーセキュリティセンター)
講演「わが国におけるサイバーセキュリティに対する取り組み」より

７．中小企業が IoT をやってみた（日刊工業新聞社)

８．IoT の衝撃（DIAMOND ハーバード・ビジネス・レビュー編集部)

９．「安全な IoT システムのためのセキュリティに関する一般的枠組」
(内閣サイバーセキュリティセンター)

10.「IoT セキュリティガイドライン」(IoT 推進コンソーシアム)

11.「企業経営のためのサイバーセキュリティの考え方」
(内閣サイバーセキュリティセンター)