インフラへの新しい脅威への対応

流通科学大学　商学部　１年

大澤　健太

目次

はじめに

2011 年は単独またはイントラとして働いてきた機器が IP を保持し、Intelligent Systems として IP の世の中に泳ぎだした。また、頭脳を持たないセンサーが IP を持ちクラウドにビックデータを運び、クラウドサーバーがビックデータの処理をするようになった。さらに人間を介在せずに勝手にデータを授受し、自らのデータと相手からのデータで勝手に判断し、方向性の修正をする機器も多数出回り始めた。

各企業はこうした機器を多数導入することにより、自動化を押し進め、ビックデータの分析と共に新しい企業活動の在り方を模索し始めている。そのため多くの新しいカテゴリーの機器が多数生み出され、機器は IP 接続ありきへと変貌を遂げた。

一方で 2011 年には新たな脅威が数多く*1生まれた年であった。標的型攻撃メール、スマートフォンやタブレットを狙った攻撃、特定できぬ共通集団による攻撃、予測不能の災害発生による IT システムの故障・業務データ消失などである。軍需企業や政府などを狙って攻撃をしたということで連日のように新聞をにぎわせた新しい攻撃のみならず、組み込み機器に対する攻撃が起こったという意味でも 2011 年は特殊な年であった。例えば 2011 年 9 月に東京都大田区のコンビニの監視カメラがサイバー攻撃の踏み台にされていたという今までにはあり得なかった事例*2が起こった。

こうした動きは 2011 年だけの特異な動きではなく、今後さらにエスカレートしてくるものと考えられる。ひとたびサイバー攻撃がインフラに及べば社会生活は維持不能となり、企業の事業継続性も脅かされるので早急に対処策を構築する必要がある。

ここでは IP 接続される機器の発展と企業活動がどう変化していくのかを推測し、それら機器の導入によって引き起こされる脅威や影響について考察する。

1. 組み込み機器の発展

マイクロソフト社の Windows には Embedded というものがある。15 年前から販売しているので決して制御系、生産設備系に近年急速に入りだしたというわけではない。最新の累計数量をマイクロソフト社は公表していないようであるが、2007 年発表の資料*3によると 2004 年には 12 億台であり、2009 年には 23 億台になる旨予想していた。よって、現在はもっと多いものと容易に推察できる。

Microsoft の Embedded OS が組み込まれている製品としては、銀行 ATM 端末、電話交換機、POS、MFP*4、キオスク端末、デジタルサイネージ、工業用制御機器、NC マシーン、靴下編み機、アーケードゲーム機、医療機器、電子黒板などがあり、多種多様のインフラ設備も網羅している。

Linux、Android、μITRON などの組み込み用に特化した OS や一般的な PC 用の Windows ではなく Windows Embedded OS が使用される点としては、主に（1）動作させるためのドライバ、周辺機器、プラットフォームが標準の PC 用のものを流用できるか、最小限の変更で済むため開発期間および開発コストが削減できる点、（2）OS 機能構成を変更できるため機器に不要な部分は組み込まないで済む点である。最低限の機能を残して OS を構築すれば数 10MB 規模で Windows Embedded Standard が構成できるので、PC を使用するより軽く、小さくなる*5。

工場にある機器は 1984 年に GM が MAP というプロトコルを定めた時から LAN で相互接続されていた。日本でも住友金属工業が改良し S-NET*6として自社工場に採用し、外販もしたことがある。それにも係らず工場の機器はウイルスとは無縁であり続けた。長い歴史の中で、「組み込み機器は情報機器ではないのでセキュリティと無縁」と勘違いされて来た。また、組み込み機器はそのファシリティ内ではネットワークにより相互接続されているが、外部との接続はされてこなかった。そのため、現在においてもそれらの機器の 5%しかセキュリティ対策がなされていない。今までの組み込み機器は単独で動くか工場内 LAN で動いていたので Windows を使用した PC のような構成であるにかかわらず、ウイルスからの脅威には直接あわなかったと言える。しかしながら、WAN 接続されていない工場機器の LAN であっても、機器メンテナンスの人間によるバージョンアップなどが USB メモリまたは USB-CD で行われることにより、マルウエアの攻撃にあったことが発表*7された。こうした組み込み型の端末が IP とつながり急速にその数量が増加したことにより、格段に効率・機能が上がった一方でウイルスからの脅威も増加したのである。

2. Intelligent Systems

長年続いた Embedded(組み込み機器)という名前が、昨年あたりから Intelligent System とよばれるようになってきた。マイクロソフト社では 2011 年 11 月 16 日に東京ビックサイトで開催されたシステムコントロールフェア 2011 において、「Intelligent Systems」を披露し、組み込み市場へ新たな提唱[*8]をした。マイクロソフト社によると「Intelligent Systems とは、ネットワークとつながることで機器自身が抱えている情報をその機器自身やシステム環境の改善に活用するだけでなく、企業活動全体に役立てることが可能なシステム」[*8]ということになる。

図 1　マイクロソフトが提言した例　(ITmedia)[*8]

ここで披露したのは、野菜ジュースの製造現場を想定した Intelligent Systems であり、工場の制御機器、工程表示用ディスプレイ、サーバーが接続されている。各機器からのデータをリアルタイムに収集し、グラフィカルに表示する。Windows Phone からリモートで工場内の装置の停止などを行い、サーバー上の生産管理データを閲覧できる。効果としては工場内の人員コストの削減や作業の効率化が図れる。また、クラウドベースでも稼働する為、東日本大震災やタイの洪水のような予期せぬ出来事が起こった場合でもデータを喪失することはない。

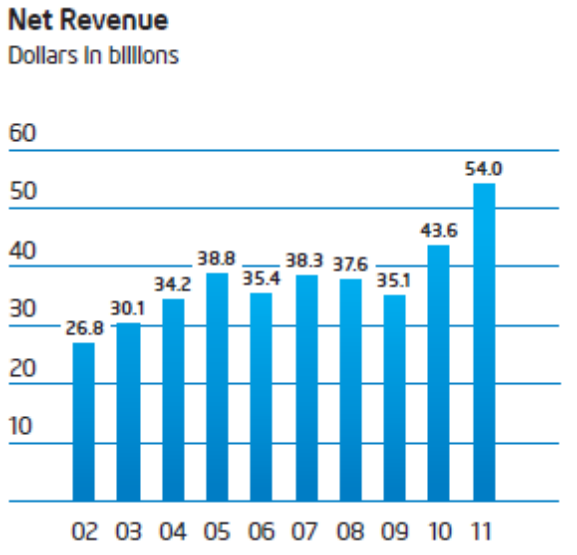


図 2　インテル社の売り上げ推移(2011 年 Intel Annual Report)[*9]

時を同じころに、CPU を販売する Intel も同様に Embedded Computing Group(組み込みコンピュータ事業部)を Intelligent Systems Group に名称変更した。

インテル社の決算年度は 1 月 1 日から 12 月 31 日と暦年と同じなので、誰もが 2012 年当初のインテル社決算発表は史上最低の業績になると予想した。というのは、2011 年に世界中がスマートフォンの波に飲み込まれ、企業ユーザ以外で PC を買うものはいないというぐらい脱 PC ブームが起こったのである。そのため、インテルの売り上げも利益も今までになく落ち込んでいるものと予想した。ところが蓋を開けてみると、左図のように史上最高売上かつ史上最高利益を出したのである。売り上げは 2010 年の 436 億ドルから 2011 年は 540 億ドルとこれまで以上の伸びとなった。

売り上げの内訳を見ると、次図の通りである。予想通りPCCG(パソコンプラッフォフォーム)が 2009 年 2010 年の 68%から 2011 年は 64%へとシェアを落としている。しかし、金額的には 2010 年の約 300 億ドルから 346 億ドルへと伸ばしている。

シェアを大きく伸ばしたのは Others とカテゴライズされている Flash メモリである。2010 年のシェア 14%から 2011 年は 19%へと、金額的にも 61 億ドルから 103 億ドルへと大きく伸ばしている。

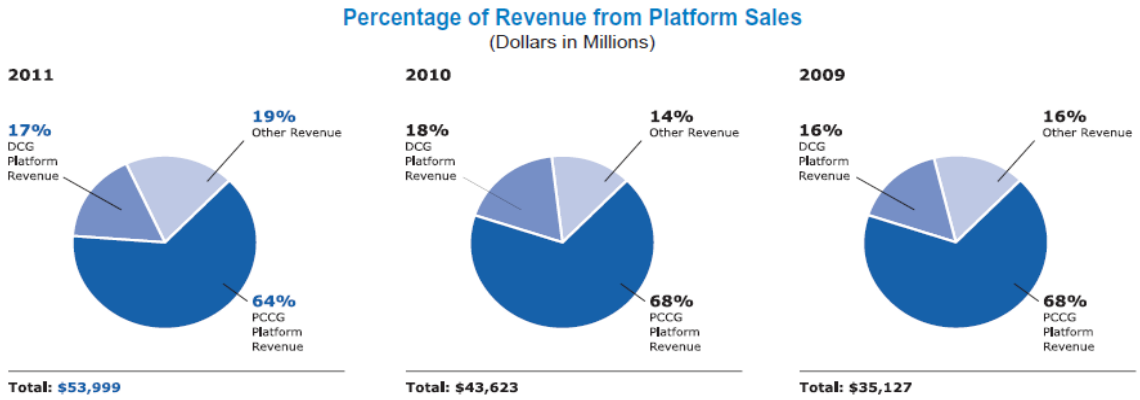


図 3　プラットフォーム別の売上推移（2011 Intel Annual Report より）[*9]

フラッシュメモリはスマートフォンのストレージとして多く使用されている。スマートフォンは PC と同じような機能を持つが、HDD が振動に弱いため使用できないので、HDD の代わりにフラッシュメモリを使用しているのである。残りの DCG(データーセンタグループ)のプラットフォームはサーバーであるが、これはシェアを 18%から 17%へと少し落としてはいるが、金額的には 79 億ドルから 92 億ドルと大きく伸ばしている。

つまり、スマートフォンの登場により今までのように PC 市場には大きな伸びは期待できないが、スマートフォンが売れれば売れるほどサーバーが必要となり、PC 用プロセッサより高価なサーバー向けプロセッサ製品が売れるということが明らかになった。スマートフォンは今までの電話とは異なり、音楽、映像、ゲームといった膨大なパケットが流れるので、売れば売れるほどサーバーが必要となるのである。さらにスマートフォンなど大量のデータをストアする必要のある端末は内蔵フラッシュメモリも膨大に消費するのである。こうして、Wintel(Windows + Intel)PC がなければ成り立たないインテルという立場からから、PC がなくてもインテルはやっていけるとわかったのが 2011 年である。

そしてスマートフォンと同様にパケットを大量に流し、サーバーを必要とするアプリケーションの開拓に乗り出した。それが、Intelligent Systems である。ET2011 でのインテル社アーキテクチャー事業本部副社長兼インテリジェント・システム事業部長のトン・スティーンマン氏の説明[*10]によると、「Intelligent Systems とは、自分自身(デバイス)だけで判断するだけに留まらず、他の場所にあるデバイスとネットワークを介してシームレスに接続され、他のデバイスから情報を取得し、その取得した情報を分析して予測される状況に応じた対応が可能なシステム」ということだ。前述のマイクロソフトの定義と似通っている。

インテルによると、1015 年には 150 億個の Intelligent デバイスが IP 接続される[*11]と予想している。ビックデータの世の中となり、データおよび機器の全てを人間が全てを管理するのは不可能となる。このとき、Intelligent Systems は集めたデータを「知識」として処理し、処理した結果を人間に可視化して提示する。

インテルの津乗氏は言う「単にデータをためるだけでは埋もれてしまいます。あふれ出る膨大なデータに埋もれてしまうのではなく、そこから価値のあるデータをきちんと抽出し、ビジネスに生かせるデータとして利用できるようにするための仕組が必要です。それこそが『インテリジェント・システム』なのです」[*12]。

インテルの提示する 1 つのコンセプト例がメディカル部門のベットサイド・ターミナルである。各種医療機器とネットワーク接続された PC が患者のベッド脇にあり、測定結果の表示、ナースステーションへの通知、点滴やインシュリンの指示、電子カルテの表示、テレビの視聴、Web の閲覧、電話、SNS によるコミュニケーションも可能な入院患者のための IT 機器となっている。使用例としては、国立育成医療センターでは患者にリストバンドをしておき、看護師が点滴や薬剤投与の際に患者リストバンドと薬剤のバーコードをベッドサイド端末のスキャナで読み取ることにより、電子カルテから良否判定し、○や×を表示することにより誤投与を防ぐ使い方が実際になさ

れている*13。また、慈恵医大*14では専用の体温計入れに測定済み体温計を入れると自動的に電子カルテに体温が記入されるということで手間を省く効果も出ている。また、テレビの視聴、インターネット、電子メールサービスは有料であるが、病室内テレビしかなかった頃の利用料金より課金収入が2～3割アップし、収入増にもなっている。今後の展望としては病院食を端末から選択できるサービスを検討しているという。

インテルが挙げるもう一つの例*10では、Intelligent Systemsを搭載した自動販売機の監視カメラが火災を検知し、データ共有する他のIntelligent Systemsが適切な避難経路を自動販売機のディスプレイに表示し、消防署への通報を行うということが可能となるのだという。ここでは火災発生を人間が認知する前に消防車の出動が可能ということで、被害の拡大を最小限にできるというメリットがある。

Intelligent Systemsは蓄積したデータを知能としていくため、開発当初予定していた処理能力や機能でシステムを構築するのではなく、システム自身が学習して知識や機能を増やしていくための余裕度を考え、当初からIntel Corei5プロセッサ程度の高い処理能力をシステムに持たせることが必要になるとトン・スティーンマン氏は主張する。

インテルが考えるインテリジェント・システムの説明はYouTubeのインテルチャンネル*15に動画で掲載されている。

3. M2M

M2M(Machine to Machine)というのは、センサーや産業用設備などをネットワークで接続し、機器同士がデータを交換することで高度な制御を利用しようというサービスである。一番の特徴は、人間からの要求ではなく機器が勝手にある機器に向かって情報を発信することである。判りやすく自動車で説明すると、障害物センサーが前方に人間を発見し、警報装置に伝達する。警報装置はアラームを流すが、そのスピード、距離から人間がブレーキを踏むのが間に合わないと判断し、ブレーキ制御装置に伝達し、ブレーキをかける。場合によってはハンドル回避するというようなことができる。一つ一つはカメラセンサー、スピードセンサー、距離センサー、ブザー、ブレーキのようなノンインテリジェントなセンサーであるが、コネクトされた全体が有機的に動くことにより効率よく働くというのが、M2Mの概念である。但し、この自動車の例はネットワーク接続されていないのでM2Mではない。各機器がデータの受け渡しにネットワーク経由でこのような働きをし、効果を発揮するのがM2Mである。

平成24年版情報通信白書には下図のように接続のイメージが描かれている。

センサーの集合体でも、システム全体として働いたときは前述のIntelligent Systemsと同じ働きをすることができる。M2Mにより、単体では成し得なかった高度なサービスが可能となる。

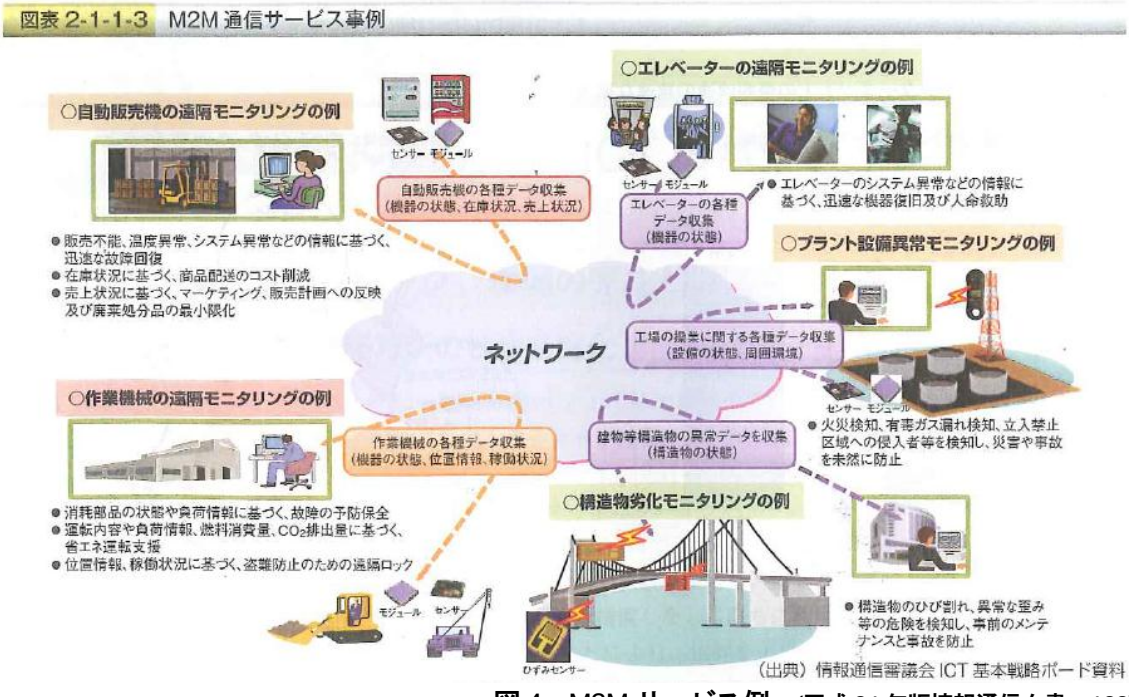


図4　M2Mサービス例　**(平成24年版情報通信白書** p.138)

以下に M2M サービスの代表例であるコピー機器の複合機(MFP)の例を挙げる。

MFP はオフィスの中にあるが、PC と接続され、スキャナとしても使用できるし、PC の文書を印刷することも可能である。つまり、社内 LAN に接続されている。しかも Fax としても使用可能なことから、外部とも接続されている。また、保守用 IP を持ってコピー機メーカーのサービスセンターとも接続されている。大阪の社員が間違って、東京の本社の MFP に印刷命令をしたところ、いつまで待っても印刷されず、何度も印刷命令したところ、本社から同じものが何部も印刷されていると連絡があったというのはよく聞く話である。また、ある会社では朝社員が出社した時にコピー機メーカーのサービスマンが会社の前に立っており、どうしたのかと聞くと、コピーが壊れているという。社員がコピー機の故障を知る前に交換部品を持ってサービスマンが到着していたという事例を以前聞いたことがある。どこが故障しているのか判っているので、交換部品もあらかじめ持参でき、MFP が使えない時間を最短にするというメリットがある。

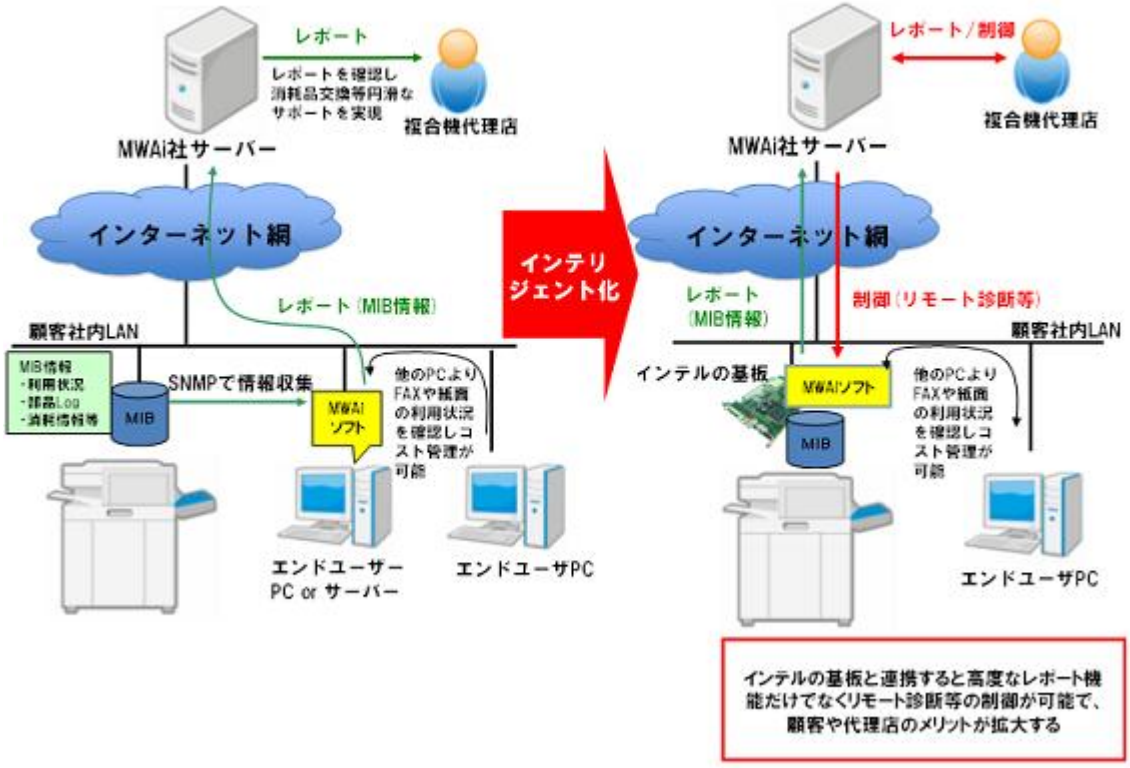


図 5　米国 MWAi 社のシステム構成(新世代 M2M コンソーシアム　2012 年 1 月 11 日)*16

上図はアメリカのアリゾナ州に拠点を置く MWA Intelligence,Inc.の例*16 である。同社は異なるメーカーの MFP を管理する共通プラットフォームを構築し、複合機メーカー及び代理店を顧客にアセット管理、サービスの自動化、マネージドプリントサービスを拡充するためのソリューションを提供する会社である。M2M サービスの結果、顧客からのコールを 50%以上回避する効果を実現した。機器代理店としては 300 台を 5 人で管理する場合、3 年間で 72 万ドルの削減ができ、投資回収期間は 1.4 か月であった。十分投資に値するということになる。また、エンドユーザーのメリットとしては、MFP 用紙の利用状況が把握でき、コスト管理が可能、消耗品が亡くなる前に代理店より部品の供給が可能、円滑な故障対応および故障回避が出来るため故障頻度が減少したというメリットが報じられている。

日本においてもリコー社は@Remote*17という管理サービスで似たようなサービスを実現している。機能としては、「デジタル複合機やレーザープリンターをインターネット経由でリモート管理する新しいサポート。ネットワーク上にある機器の状況をリアルタイムに把握できるため、必要に応じたサービスをスピーディーにご提供いたし

ます」[*17]となっている。このサービスの特徴として、「(1)機器の故障未然防止―定期的な機器の診断や、機器の状態に応じた点検の実施により、故障の未然防止がはかれる。(2)クイックアクションによるダウンタイム短縮―故障時の自動通報、状況確認の実施、迅速な CE 手配、修理依頼作業の簡素化を行うなど、機器のダウンタイムを最小にとどめる。(3)機器管理業務へのお役立ち―トナー注文など機器に関わる業務の簡素化および業務代行をはかり、機器の出力状況に関する報告をする」[*17]。となっており、機器がインターネットに接続されていることにより情報がリコーに集約しており、それを元にサービスの提案ができるようになっている。

4. IoT (Internet of Things)

IoT というのは Internet Of Things の略で、Things(物)に固有の IP を与え、これを Internet に接続することで、あるサービスを行うということである。

インテルが IDF2011 で発表した内容によると、IoT サービスの内容としては、公共的要素のセーフシティ、ITS、e ヘルス(医療機器同士の連携)、スマート農業、スマートグリッドなどのスマートホーム、スマートビルがある。e ヘルスは Intelligent Systems の説明でも良く出てくるが、その差異は定義されていない。

セーフシティというのは、文字通り「安全な街」であるが、これは電信柱、店舗、自動販売機等の各所に付けられたセキュリティカメラにより、街を監視することにより犯罪の起こりにくい街を作り出すことが目的である。ひとたび犯罪が起これば、その人物をリアルタイムで警察に届け、逃走している犯人の映像を各所のカメラが切り替えながら追い続ける。

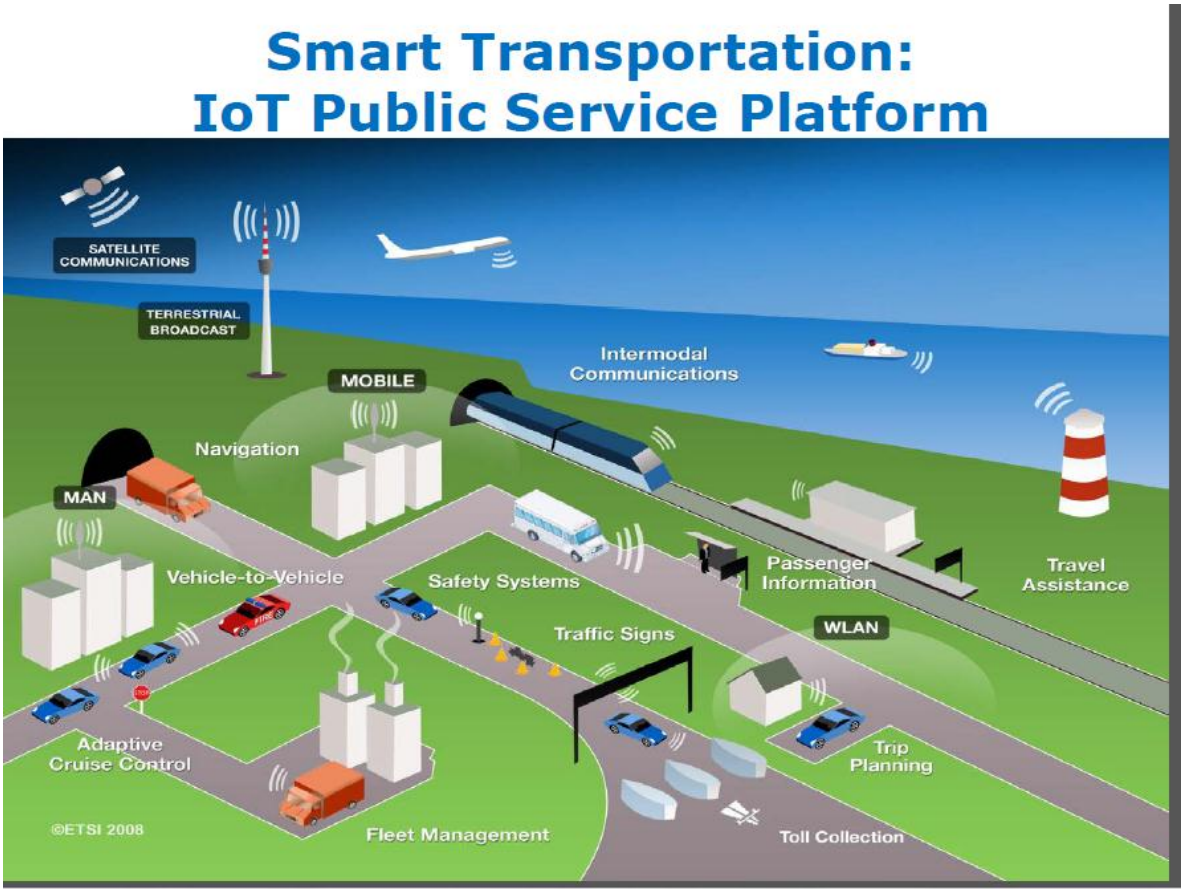


図 6　IoT の例 (Intel IDF 2012)[*18]

上の図にある IoT 公共交通サービスの例を示すと、自動車はお互いの自動車と通信し、一か所に自動車が集中しないよう渋滞を回避するルートを選択する。車々間通信はお互いの距離・スピード情報のやり取りも行い、急ブレーキからの追突も回避する。トラックは積荷の種類、量、自分の位置をセンターに知らせながら走行する。

通ったルートにより有料道路が課金する。信号は一定の時間ごとに青赤を繰り返さないで、自動車の交通量に合わせて多い方の青を長めに、少ない方の青信号を短めにするということができ、渋滞回避とエネルギーの節約ができ、CO2 排出削減効果がある。ユーザからしても時間やエネルギーが節約でき、事故になりにくいのでメリットは十分にある。バスがどのくらいしたら来るのかはバス停に表示され、バスは先のバス停に何人が待っているかが判る。電車もスケジュール通りに来るのか駅に情報を通知する。

こうした情報は今までも専用回線で行っていることもあったが、IoTでは全て直接接続や専用回線ではなく、インターネット経由になっていることが特徴である。インターネット経由にすることにより通信機器部分の汎用化が図れるため、技術的レベルが低くなり、コストの低減が可能となる。

IoT ネットワークの階層としては、一番下のセンサー部分が巷にあふれ、それが認識可能なワイヤレスセンサーネットワークに接続される。この間のプロトコルは、ZigBee、WiFi、IR、RFID 無線タグ、非接触 IC カードなどがある。

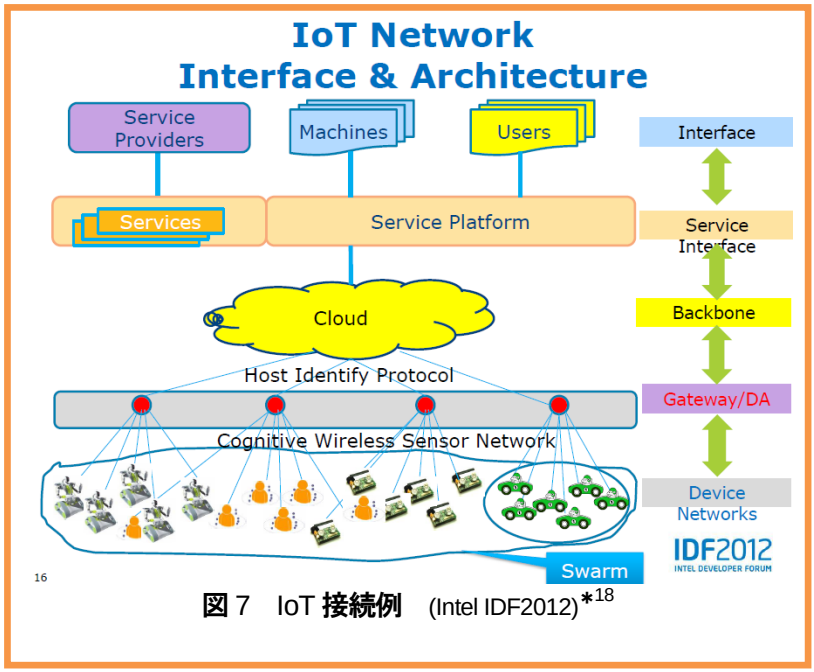


図 7　IoT 接続例　(Intel IDF2012)*18

それらが上位階層のクラウドに接続され、サービスを司り、データの収集・分析するソフトウエアに接続する。そのソフトウエアが該当するユーザ、機器、サービスプロダイバーに連絡するということになる。

企業としては自社内でこれらすべてを用意しなくとも、欲しいセンサーからのデーターを集計したデータをサービスプロバイダーから欲しい時期またはリアルタイムに入手して経済活動に役立たせるということが可能である。センサー情報がトラックの GPS データ(現在地)、顧客の荷物情報(顧客名・運搬先・中身・納期)、倉庫の空き情報である場合には全て自社の情報となるが、それにルート計算(道路混雑情報、有料道路料金、一般道路をどの程度走らせると高速道路料金を節約できガソリン代が増えずに時間に間に合うかのバランス計算)を加えるとサービスプロダイバーからの情報が必要となる。

これらを上手に使用できると、合理化(預かる荷物の最大量予測可能)、コスト削減(高速道路代およびガソリン代の削減)、実車率の向上、顧客満足度の向上(時間丁度に着き、値引きができる)につながる。

5.　ビッグデータ

本来ビックデータは通常のデータベース管理ツールなどで取り扱うことが困難なほど巨大なデータの集まりのことであり、データの内容も定型的・構造的ではない。パッケージソフトで扱うことが難しいため、数十から数千のサーバーで並列処理することになっているが、ビジネス上ではこの定義に拘らず、リアルタイムに吐き出される数十から数百テラバイトの構造化したデータを取り扱うことを言っている場合が多い。

つまり、単に今までの自社機器から吐き出されるデータ量より非常に多いデータを扱うということだけである。この場合、メッシュデータに変換してマーケッティングに活用されているものもある。そういったサービス用にビックデータを地図上のメッシュデータにするサービス会社も出てきている。

携帯電話は誰の持ち物か決まっているので、今現在誰がどこにいるのか判っている。これを個人ということではなく、属性ということで集計すると、マーケッティングに使用できる。例えば、渋谷駅周辺のスマホ属性を調べてみると、20 代女子が 40%いたとした場合、その場での広告宣伝は 20 代女子に合わせたものが効果が高い。駅のサイネージでも良いし、近隣のビルの電光掲示板でも良い、今現在 20 代女子が得をするようなキャンペーンを表示し、顧客を誘導し、ふらっと渋谷に来た潜在顧客に物を売るということが可能となる。逆に 20 代女子

用の製品を販売する会社は、今どこでキャンペーンをするのが効果的なのかメッシュデータから調べ、それが新宿であれば新宿でキャンペーンを張るということも可能である。

また、渋谷の 40%が 20 代女子ということが判れば、なぜかを調べ、近隣の大学の下校時間なのか、近隣のコンサートホールでコンサートが始まるところなのかで、対応が変わる。コンサートで集まっているところなら嗜好が似通っていることが推測できるので、そのコンサートで集まる人が好きそうなものを対象としたマーケッティングを行うのである。例えば、そのコンサートの演者のストラップをプレゼントするとか、コンサート終了後に集客する場合、半券を見せると 2 割引するとかをコンサート前に告知することである。

ファーストフード店では顧客誘導に割引券を配ることが多いが、このメッシュデータを活用すると、サラリーマンが多い時はコーヒー無料券、10 代学生が多い時はポテト無料券などターゲットに合わせた無料券にすることで無駄な割引券を配布しなくて済む。このコーヒー券でセットを買うとコーヒー分の 100 円引きとなるなどとすると、セットがより売れる。ポテトもセットで買う時だけポテト分が値引きされるような券にすると誘導しやすい。

6. IP 機器を使う企業活動の変化

このように、ヒトとヒトの結びつきから、モノとモノの間での結びつきが強まり、モノも自社内のモノだけでなく、グローバルな結びつきへと変革してきている。

Intelligent Systems や M2M や IoT といったものの概念をきちんと線引きしている企業は余りないが、こうした範疇に垣根を持たず、様々な機器に埋め込まれたセンサーがネットワークを通じて人間を介さずに相互情報交換をし、ビックデータの活用とあいまって企業業務活動の改善に役立てる動きが顕在化してきている。また、今まで見てきた以外にも BEMS、HEMS やスマートグリッド、エコネットなどでも IP を利用したサービスを目指している。

自社内での処理では何の意味も与えられなかったデータが知識へと変貌することで、データを活用でき、新たなビジネスチャンスが生まれていくことになる。

機器を上手に活用することにより、商売のチャンスだけでなく、効率改善によるコストの削減、人件費の削減ができ、増収増益が期待できる。また、顧客満足度の向上にもつながる。

7. IP 機器に対する新たなる脅威

ところが、こうした IP 機器が情報処理システム系ネットワークと接続され、それが制御系や設備系にも接続されているので、攻撃者には格好のターゲットとなり、攻撃が開始され始めたが、対策は後手に回っている。

ここで、何の変哲もなくオフィスに存在している MFP からハッカーが侵入できるという例を示す。

MFP のネットワーク接続は会社から見ればバックドアであり、攻撃者から見るとセキュリティホールが放置されているのと同じ状態であるが、ユーザは全く気にしていない。但し、MFP メーカーは気づいているようで、リコー社の@Remote サービスはこうしたことを念頭にセキュリティ対策されているような説明がされているし、シャープ社の MFP は McAfee 社のセキュリティ製品を搭載済みである。

MFP メーカーが対処したところで、ハッカー向けの検索サイト「SHODAN」を使うと、簡単に MFP の管理画面にアクセスできてしまう*19。情報としては IP アドレス、MAC アドレス、プロキシサーバー、デフォルトゲートウエイなどが見えてしまい、企業ネットワークの構造を把握できてしまう。見かけはただのコピー機の様であるが、内部は PC 基板が使われており、Windows OS まで乗っていてはウイルスの格好のターゲットとなる。踏み台となり他のネットワークを攻撃することも、自社内のデータを漏洩されることも、社内設備を制御されることも可能となるのである。

MFP はどこのオフィスにもある。また MFP だけが外部に接続されているのではなく、必ずオフィス内もしくは工場内のネットワークに接続されている。一度 MFP 経由で侵入されると、ATM、POS などは金銭を動かされ、制御盤やメディカルなどを操作されると人命にかかわることになる。

図 10　SHODAN の画面(日経 BP 社　ITPro)*19

その他にも、起動するとATMで処理される取引データを盗聴してログファイルに記録し、特殊なクレジットカードでATMを制御する[*20]ことも簡単にできる環境となった。

2012年1月、米国デジタルボンド社が製品の脆弱性を見つけ、光洋電子工業に警告したが改善されなかったとして、ハッキング手法をネットで公開すると通告を受け、対応に追われた。もし、悪用されれば半導体工場の生産が止まったり、火災が発生したりする可能性があるという。

ロシアのベンチャー企業であるグレッグ社は2011年3月に米国GE社およびドイツ シーメンス社など12社製品の攻撃ソフトを販売した。これにより水道や電気を止めることも可能とのことで、攻撃者が購入した可能性もある。ビル管理コンピュータに侵入され、温度制御されると、急上昇により人間が活動困難となり、サーバーなどの情報処理装置は故障する。

最近はセキュリティ対策をしていないことが丸見えである端末が狙われるようになってきた。インフラシステムがこのような経路で侵入されれば、インフラをいたずらに混乱させることも可能である。原子力発電所の監視用IPカメラから侵入し、でたらめに制御し、制御コンピュータが対応不可能となり、インシデントに発展するということである。

各国はこれを進化させたサイバー兵器を研究[*20]しており、相手国をサイバー攻撃することができる技術の蓄積中という。戦争が起こっても爆弾は1発も要らず、蓄積したデータとプログラムを稼働させるだけで相手国の原子力発電所を全て異常もしくは停止に陥れることが可能である。マンガのような話ではあるが、Annonymousや LulzSecなどの攻撃集団が発生し、国際的に猛威を振るっている以上、新たな脅威として対策を打っておく必要がある。

今まで組み込み機器はPCではないので、ウイルス対策をしなくても良いという風潮があった。ウイルス対策用ソフトウエアを入れるとソフトウエアの動作が遅くなり、機器制御のタイミングが合わないなどの理由により、ウイルス対策されてこなかったこともある。95%の組み込み機器がウイルス対策されていないとも言われ、未対策機は多数巷にあふれている。また、対策済みの機器をメーカーが出荷したとしてもパターンファイルのアップデートが行われずに出荷時の状態のまま放置されている機器も多い。

M2Mの項にある図を再びご覧いただきたい。全てのインフラはネットワーク経由で接続されているのであり、これら機器同士は有機的に接続され、人間を介在せずに情報をやり取りし、修正をかけながら自動的に働くのである。

便利になったIP機器の一部がウイルスに侵され、異常行動を始めたらどうなるのか。インテリジェント・システムは人間が気づくより圧倒的に速い速度で異常に気付くため、あっという間に世界中に伝搬する。ウイルスのみならず、誰かのミス操作によっても、自己を守る制御が働き、その結果を多くのネットワーク上デバイスに撒いてしまう。ブラックマンデーで世界中の株が暴落したようなことが起こる。株が暴落すると現金を求めて自動決済システムが銀行から預金を引き出そうとし、銀行の現金が足りなくなり、その情報が他の情報機関に流れ、格付けを下げ、他行からの融通・融資が止まり、倒産する。自動販売機の制御システムに侵入し、災害モード移行を発令すれば、日本中の飲料がタダで買えるようになる。全ての飲料メーカーは回収が不能となり倒産する。災害モードになった自動販売機は近隣の避難所に避難するよう指示する。何もわからない人間が避難所に殺到する。信号機は自動販売機から災害モードであるという情報を受け取り、日本中の信号が赤信号となり、交通が混乱する。各方面の社会インフラにスパイラル状に波及していき、社会は混乱し、全てのインフラは機能しなくなる。

コンピュータを手動に切り替えたり、ネットワークから外したりといった作業には数日かかり、終わったころには日本は元の状態とかけ離れた経済状態となり、立ち戻ることは困難となる。元々の原因が悪意にしろ、偶然にしろ、些細なことから始まり、全てが終わる。

8. 情報処理システム系に対する新たな脅威

2011年に起こった新たな脅威のうち一番世間を騒がせたのは、標的型攻撃メールであるが、これは防ぐことができない。というのは、メールソフトがメールを開く前に、メールサーバーIPやメールアドレスを確認できる構造となっていないからである。これらを見ようと思えば一旦メールを開いたうえでプロパティから詳細情報を見なければならないが、そもそもプロパティを開いてインターネットヘッダーを開いても、IT系の職務に携わる人か、情報系に造詣が深い人でない限り何が書いてあるか理解できない。メールを開く前のメールソフトにリストとして表示されるのは「表示名」であり、これはメールアドレスと全く関係のないものでも良いのである。実際、セキュリ

ティ上、家からのメールは会社ものとは別のメールアドレスを使用しているという人は多い。その時に相手から自分を認識してくれないと困るので、どのドメインを使っても表示名は同じにしてあることが多い。表示名は任意に誰でも付けることができ、メールアドレスのように重複を排除するものでもない。この表示名が自分の会社の上司だったりすると、必ず開いてしまう。標的型攻撃メールは事前に周辺の人間関係やメールアドレスを徹底的に調査してから行うので、普段からメールのやり取りをしている人の表示名を使用するのである。無差別攻撃と異なりピンポイントでメールを送るので、迷惑メールにも分類されず、メールが到着してしまう。こうなると、バックドアが即座に開かれ、ホワイトリストの通路として認識するので、ファイアウォールは役に立たない。

そうなると事前には防げないので、どうしたら標的型攻撃メールを防ぐかということではなく、標的型攻撃メールを開いた後をどうするかということに焦点を絞るように考えがちである。しかしながら、開いてしまえば対策は完全にはできない。従い、一刻も早くバックドアを見つけ、それを閉じることであるが、相手はこちらの組織を熟知しているので、再び他の人宛にメールを出してくることは容易に想像が付き、イタチごっことならざるを得ない。攻撃が収まるまでにどれだけの情報が抜き取られるか想像しがたい。

これに対応するためには情報処理用の基幹系ネットワークとメールサーバーを分離したネットワーク上に置き、バックドアから侵入されても全てを失わない状態のシステムを構築するしかない。

9. 新しい脅威に対する対策

従来、情報処理技術者試験の教科書でも次図のような構成が載っているように、情報処理担当はこの構成をとった上で如何にファイアウォールを強固にするかということしか考えてこなかった。しかし、標的型攻撃メールではホワイトリストとして侵入してくるのでファイアウォールは全く役に立たず、しかもその直後に作られたバックドアは公的な VPN として作動するのでファイアウォールから見れば、安全な経路として認識してしまう。各種のサーバーは同じファイアウォールにぶら下がっているので、ひとたびファイアウォールが破られれば全滅である。

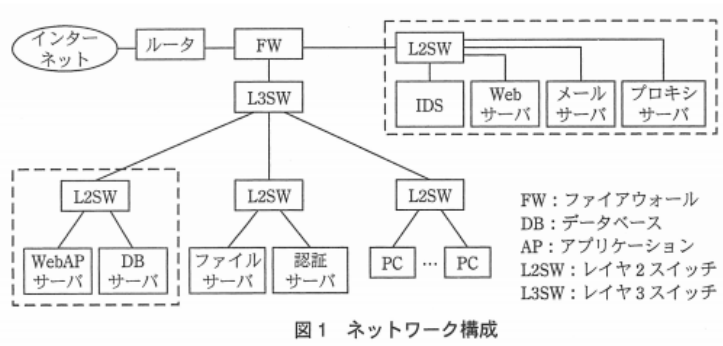
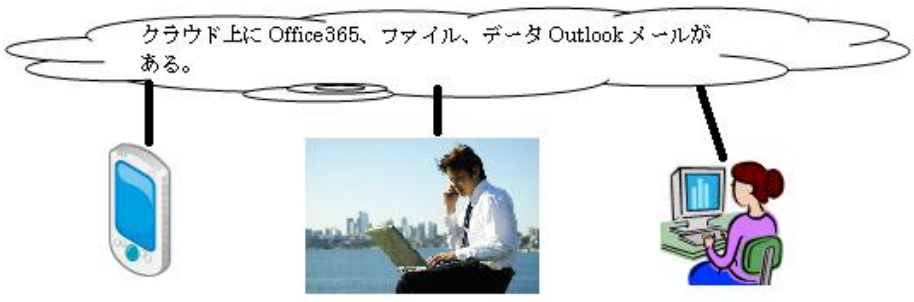


図１　ネットワーク構成

図 11　ネットワーク構成　(平成 24 年度春期応用情報技術者試験 午後問題9)[*22]

情報処理系に対する新たな脅威へ対策はわりと簡単である。Web サーバーはレンタルサーバーを借りて外部委託し、社内ネットワークと切り離す。こうすることにより、DDoS 攻撃などで Web が閉鎖されたとしても基幹ネットワークと接続されていなければネットワークのトラフィックによる基幹業務の影響は出ない。

また、メールサーバーはマイクロソフト Office365 のようなクラウドにすることである。こうすれば、メールアドレスから社内サーバーに入り込まれることはない。但し、過去メールが流出する恐れがあるので、不要になったメールは頻繁に削除すべきである。この時、肝心なのは社内の基幹系ネットワークはインターネットと接続しないイントラネットにしておくこと

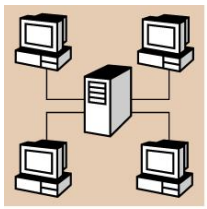


スマートホン　　外出先ノート　　会社デスクトップ

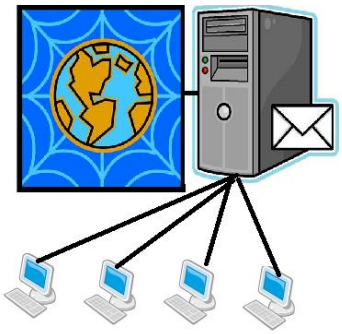
Local にはデータは無い。デバイスを変えても同じものを見に行くだけ。

図 12　Office365 導入図（筆者考案）

だ。



社内業務（シンクライアント・イントラ接続）



Web アクセス、メールアクセス（外部接続専用 PC 使用、イントラには接続しない）

外部からのアクセス用自社広告 Web サーバー（外部委託サーバー・自社イントラには接続しない）

外部から見えるサーバーは自社イントラに接続しないので、サイバー攻撃に合っても広告用サーバーのダウンかメールの遮断だけであり、基幹業務・社外秘資料に影響が及ばない。

図 13　サーバーとの接続　（筆者考案）

企業のデータが損失するだけではなく、社会全体が転覆するようなことが起こらないためにも、情報処理系と制御系をまったく別のネットワークとすることである。

一昔前の PC が 1 台 20 万円していた頃の習慣で、メール、Web ブラウズ、業務を 1 台の PC で行っている会社がほとんどであることに問題がある。現在は OS 込みの PC が数万円で入手可能なので、Web ブラウズとメールは同じ PC でも構わないが、少なくとも業務用はもう 1 台別にイントラ専用端末を用意すべきである。その構成としては、ローカルにデータを保持できず、USB も挿せないシンクライアントにすべきだろう。こうして、複数経路を持ち、各サーバーに個別のファイアウォールを持てば、新たな脅威から全滅に陥られることはなくなる。

ネットワークが社内に 1 系統でファイアウォールが 1 か所しかないという状態は早急に脱した方が良い。プラットフォームが PC のものは早急に PC 用のウイルス対策を導入すべきであり、ARM などマ

イコンベースのものは、ウイルス対策ベンダーの対応製品を投入する必要がある。

さらに、データ授受を行っているサーバーなどは端末が横から外部からのデータを受け取らないように監視し、自らもチェックした高信頼性のデータのみを送るようにしなければならない。

会社としては、メールサーバーおよび社外向け Web サーバーの外部委託、社内にイントラ用サーバー構築が必要である。イントラをシンクライアントにすることによって USB メモリによるマルウエアの浸入を阻止することができる。社内業務用とメールおよび Web アクセス用に 1 人 2 台の PC が必要であるが、昨今の PC 価格を考慮するとさほど高コストではない。Web アクセスおよびメールアクセスはタブレットやスマートフォンでも良い。社内の人間に業務データを連絡するときはデータそのものをメールに添付することではなく、リンク先を教えるに留める。データはサーバーから出さないことが必要である。

10. おわりに

Intelligent Systems、M2M、IoT、BEMS、HEMS、エコネットライト、スマートxxと称して、色々なものがつながる世の中は何でもできて、バラ色な世の中となるかのように官民あげて歓迎しているような風潮がある。逆に攻撃側からすると攻撃ターゲットが多様化する。攻撃に対するリスクが非常に多くなるので、便利にもならない端末は安易にネットワークに接続しないことである。

しかしながら、今までの例でわかるとおり昨今の機器は IP 接続ありきで作られているため、各企業の自主性に任せていては国家の安全保障にかかわる。IP 機器の多様化により企業活動はより一層便利になることは確実で、各企業ともに多種多様な機器を導入するのであろうが、導入と同時にウイルス対策も怠らないようにする必要がある。ウイルスの被害は自社のみが受けるという話ではないからである。政府は国家の一大事ととらえ、早

急に各企業を指導し、対策を講ずる必要がある。各企業はこうした事態を早急に認識し、対処しなければならない。

参考文献

＊1　情報セキュリティ白書 2012　独立行政法人情報処理推進機構(IPA)　2012

＊2　コンビニから攻撃指令　読売新聞　2011 年 9 月 24 日

＊3　Windows Embedded 市場予測　大原隆広　マイクロソフト株式会社　Windows XP Embedded 概要　MEDC2007

＊4　Multi-Function Printer：複合機と呼ばれ、コピー、ファックス、スキャナ、プリンタが一体型となった機器

＊5　Windows Embedded Standard 組み込み OS 構築技法入門　石黒一敏他　日経 BP ソフトプレス刊　2009 年 12 月 21 日

＊6　S-NET（総合化を進めるシステム間インターフェースの展望＜特集＞）－（工場総合化における LAN の動向）　山崎郁太郎　道岡良　登坂宗平　工業技術社　計装 29　p14-21　1986 年

＊7　激変するセキュリティ対策の「今」を知る　ZDNet Japan
http://japan.zdnet.com/extra/soliton_security_201112/3501134/
例えば、Stuxnet は Windows の脆弱性を利用して、USB メモリー経由でイランの核施設ネットワークに深く静かに侵入し、感染に気付かれないように工作をしながらウラン濃縮作業に必要な遠心分離器の駆動装置に深刻なダメージを与え、イランの核開発計画を妨害したと言われている。

＊8　データの可能性を最大限に引き出す！！近未来の製造業向けシステム　ITmedia
http://monoist.atmarkit.co.jp/mn/articles/1111/19/news013.html

＊9　2011 Intel Annual Report

＊10　組み込みだけど Atom じゃない　自動販売機に Corei5 を載せる理由　ITmedia
http://plusd.itmedia.co.jp/pcuser/articles/1111/16/news109.html

＊11　ESEC2012 スペシャル・プレビュー：インテルが提唱する「インテリジェント・システム」ITmedia
http://monoist.atmarkit.co.jp/mn/articles/1204/17/news001.html

＊12　インテルが提唱する「インテリジェント・システム」で実現できるもの　ITmedia
http://monoist.atmarkit.co.jp/mn/articles/1204/17/news001.html

＊13 医療安全をとりまく動向・ここに注目！　医療安全推進者ネットワーク
http://www.medsafe.net/contents/recent/63bedside.html

＊14　ベッドサイド端末 MediClient を導入し、患者サービスをさらに充実。タッチパネルにより、誰もが簡単にインターネットや電子メールを利用可能。Microsoft
http://www.microsoft.com/ja-jp/casestudies/jikei.aspx

＊15 インテリジェントシステム　～組み込みコンピューティングの新時代
http://www.youtube.com/watch?v=0Z1UNWu8vb4&feature=relmfu
http://www.youtube.com/watch?feature=endscreen&NR=1&v=DKemWWdMAwg

＊16 複合機のコール回避を大幅に改善する米国発のサービス・インテリジェンスソリューション
新世代 M2M コンソーシアム　2012 年 1 月 11 日
http://www.ngm2m.jp/jirei/MWAi/MWAi.html

＊17 出力機器のリモート管理サービス「@Remote」リコー　http://www.ricoh.co.jp/remote/

＊18 Intel IDF2012 北京

＊19 進化するサイバー攻撃-[2] 複合機が丸見えになる恐れ　山崎文明　日経 BP 社　ITPro
http://itpro.nikkeibp.co.jp/article/COLUMN/20120220/382087/?SS= imgview&FD=-346286100

＊20 銀行の ATM に感染するマルウエア　McAfee 社ブログ
http://www.macafee.com/japan/security/macafee_labs/blog/content.asp?id=1102

＊21 サイバーウォーズⅡ 攻撃者たち7 「兵器」対応遅れる日本　読売新聞　2012 年 7 月 19 日

＊22 平成 24 年度春期応用情報技術者試験　午後問題9