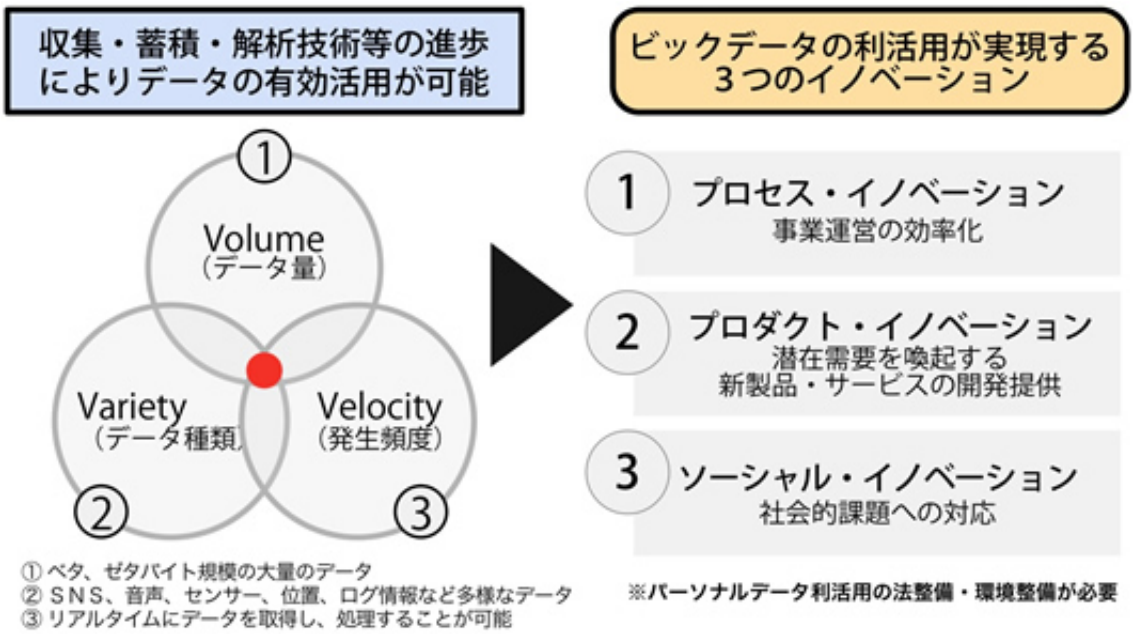
1-1　コンピューティング能力の進化と脅威

以前から「ビッグデータ活用」が何かと話題になっていましたが、「IoT（Internet of Things）」や「人工知能／機械学習 = AI（Artificial Intelligence）」が進歩する中で、ビッグデータ活用もようやく具体化しようとしています。

そしてその活用は、データ駆動型社会と言われる「CPS（Cyber Physical System）」（現実とサイバー空間との相互関係）によって、社会のあらゆる領域に実装され、大きな社会的価値を生み出していくとされています。

データの収集、蓄積、解析の全ての面において、ICTインフラが高度化し、ようやく「ビッグデータ」が「サイバーフィジカルシステム（CPS）」として活用可能になるのでしょうか。



ビッグデータとは、以下の３Vを基にしています。

1．Volume（データ量）
　ベタ、ゼタバイト規模の大量データ
2．Variety（データ種類）
　SNS、音声、センサー、位置、ログ情報など多様なデータ
3．Velocity（データ発生頻度）
　リアルタイムにデータを取得し、処理することが可能

この３Vで得られたデータをAI（人工知能）で解析、活用することで以下の３つのイノベーションが実現するとしています。

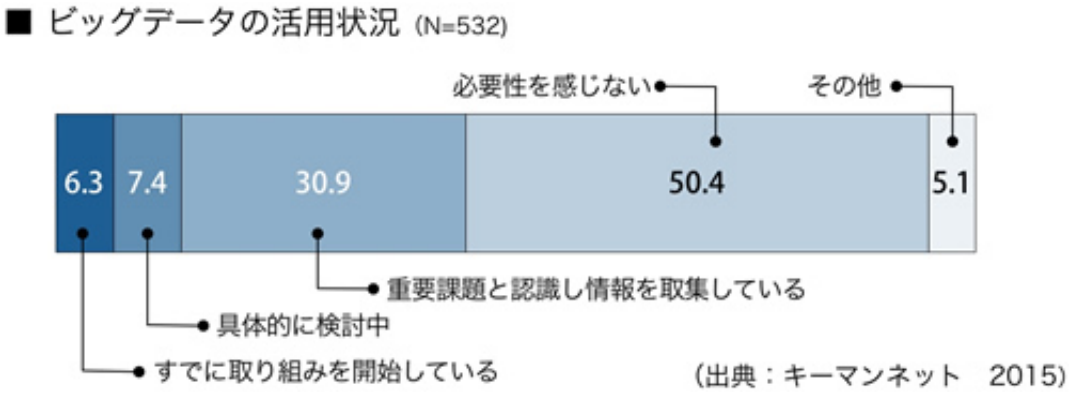
1）プロセス・イノベーション（事業運営の効率化）
　例：山崎製パンは、大量の受注情報をリアルタイムで一元管理することにより、予測に頼らず、受注した数量に見合う生産を可能とし、製品廃棄ロス等を約4割減少させ、コスト削減を実現させました。
2）プロダクト・イノベーション（潜在需要を喚起する新商品・サービスの開発・提供）
　例：あいおいニッセイ同和損保は、車載器からの走行データを受信することで、顧客の走行距離に応じた保険料を算出し、1キロ単位の走行距離に応じた合理的な保険料により、自動車ユーザーの車両維持費低減を図っています。

3）ソーシャル・イノベーション（社会課題への対応）

例：予防医療や、個人にあったオーダーメイド治療、ヘルスケア、そして低コストで効果的に、犯罪・事故・災害を抑えることを可能にします。

このように「ビッグデータ」という言葉は、ICT関係者や企業だけではなく、一般層にも知られ、一部の大企業やICT関連企業では積極的に活用されていますが、一般企業にはIoTの基盤整備や利用ノウハウが十分普及しておらず、まだ幅広く浸透するには至っていません。

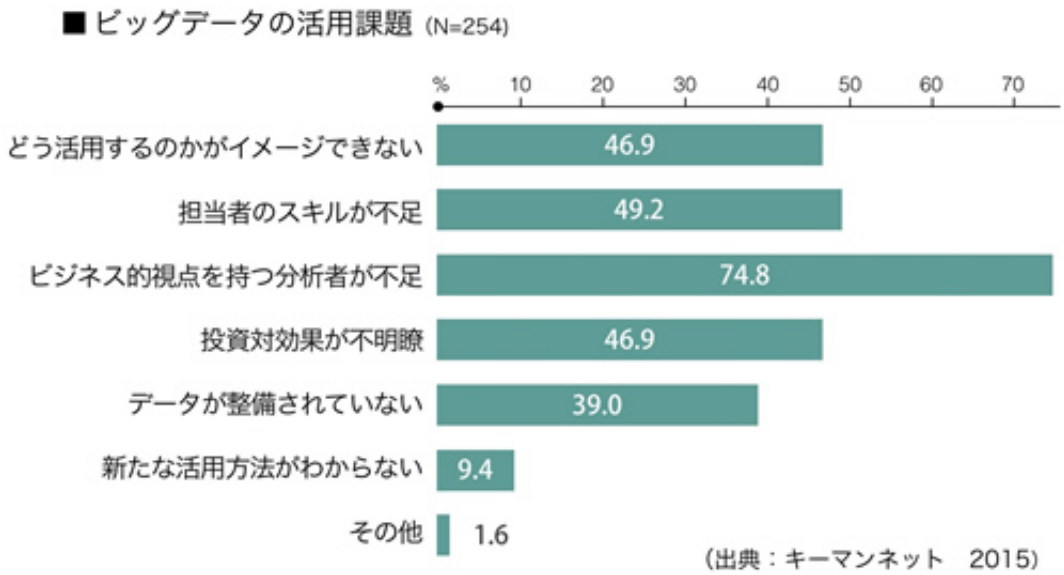
以下のアンケート結果でも、「既に取り組みを開始している（ビジネスの中で活用している）」企業が6.3%で、「情報収集中」という段階まで含めれば、ビッグデータ活用に前向きな企業は全体の4割強ということになりますが、その一方で、「必要性を感じない」という回答が約半数を占めているのが現実です。



また、ビッグデータ活用の課題としては、「どう活用するのかがイメージできない」「投資対効果が不明瞭」といった "活用以前" の段階の問題も見受けられます。最も多い回答は「ビジネス視点を持つ分析者が不足」、次いで、「担当者のスキルが不足」があげられています。

業務担当者と分析者が連携するだけにとどまらず、業務担当者が分析スキルを身につけるか、分析者がビジネスを理解するか、いずれにしても、分析結果をビジネスに直結できるような人材もしくは、その機能（AI等）が求められています。

また、ビッグデータ活用を既に実践もしくは検討している企業に対して、どのような検討体制をとっているのかをたずねた質問においては、「既存の各部署内で検討」という回答が６割近くを占めており、「社内の横断プロジェクトで検討」というところは２割程度にとどまっています。



しかし、ビッグデータ活用のための準備は整いつつあります。いままで「端末機器」「ネットワーク」「コンピューティング」という３分野で各々進化してきた能力が集結し、中小事業者においても情報活用による新しい価値創造（イノベーション）を生み出す可能性は十分考えられます。

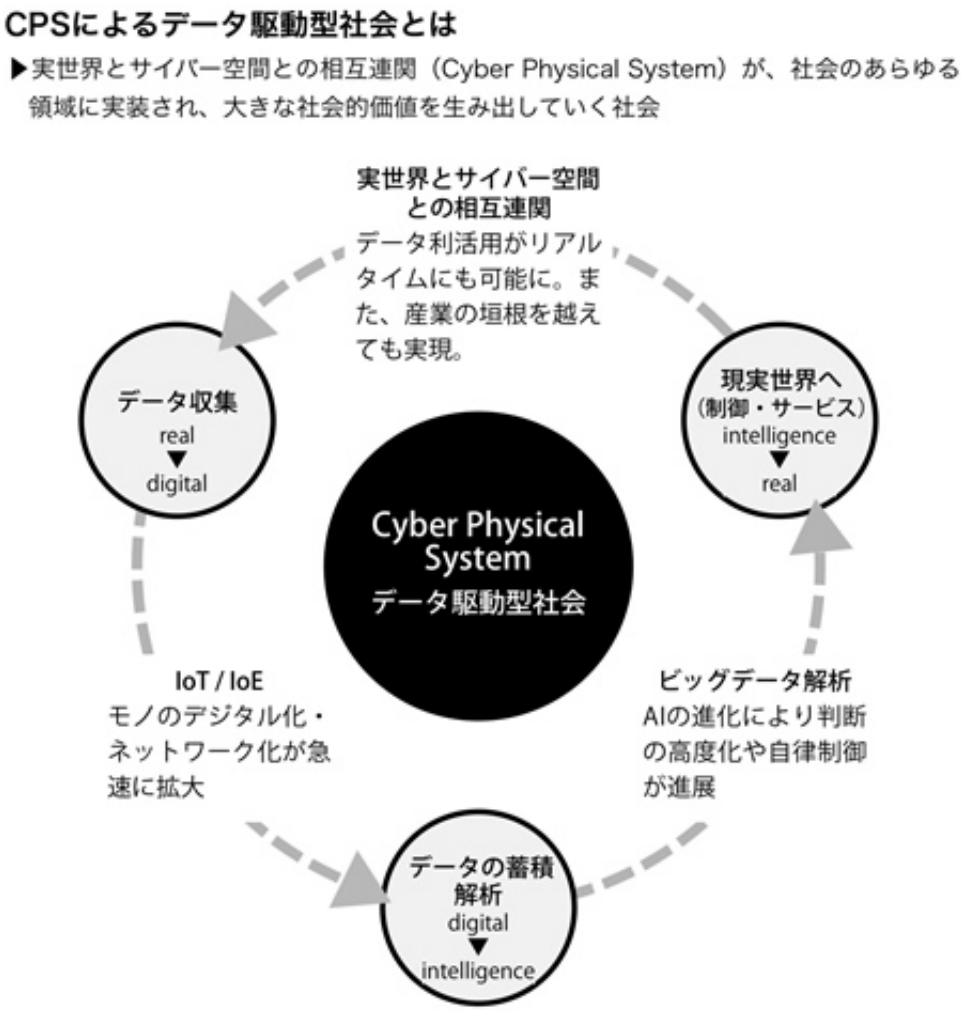
その背景には、半導体の集積密度が18～24ヶ月で倍増するという「ムーアの法則」があります。1995年と2015年の20年間を比較すると、CPUの高速化（0.2→31.5GHz）やHDDの大容量化（2→6000GB）を実現しました。そして、ネットワークの高速化はMbpsからGbps（メガからギガ）へとレベルアップしています。

これらの変化は、クラウドコンピューティングやスマートデバイスの進展と普及をもたらせ、仕事だけではなく、人の生活に様々な変化を及ぼしています。

そして、ICTインフラの進展とセンサーの技術進歩が相まって、あらゆるモノがネットにつながること、すなわちIoT（Internet of Things）という技術によって、膨大なデータがリアルタイムに集積可能となり、その利活用によってビックデータ時代がより現実的なものとなりつつあります。

さらに、加速的に進歩する機械学習／人工知能（AI:Artifical Intelligence）の発達は、人間の脳構造に近いニューラルネットワークの出現によりデープラーニング（深層学習）という手法を実現しました。近い将来（2045年頃？）１台のコンピュターが人間の脳の能力を超える「考えるコンピュータ」が出現するといわれています。

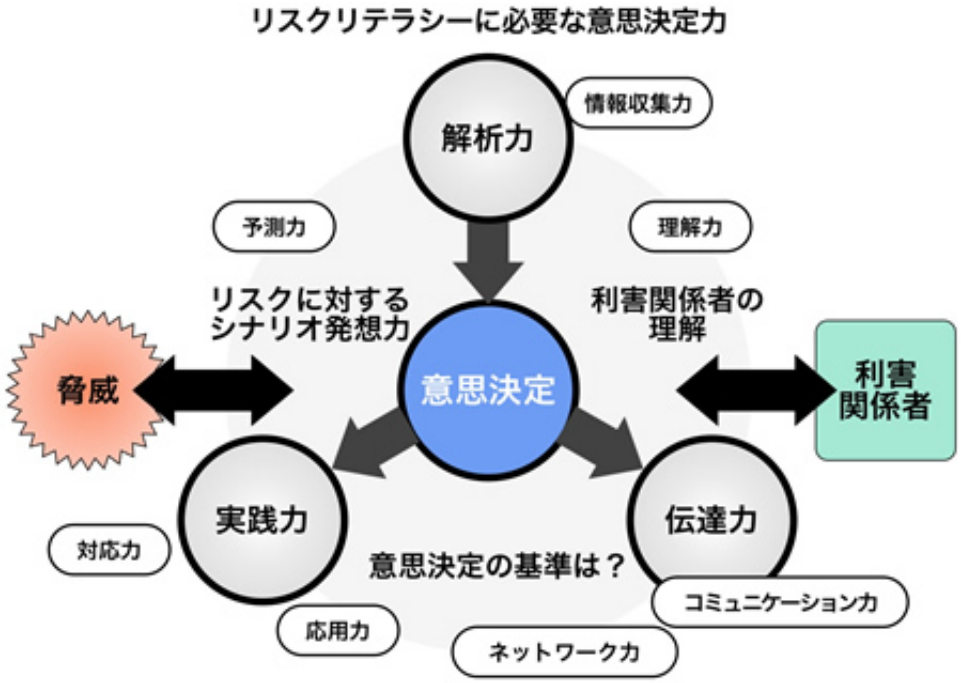
「ビックデータ」と「考えるコンピュータ」、この２つが機能するIoT時代を「CPS（Cyber Physical System）」と呼び、ICTに第３の波（第１の波：1960年代からのIT化。第２の波：1980年代のインターネット普及）を引き起こし、今までの常識を劇的に変化させ、ビジネスや組織だけではなく、社会環境にも大きな影響と変化を与えると考えられています。



同時に、これらの変化（パラダイムシフト）は利便性だけではなく、そのインパクトと同様に大きな脅威をはらんでいることを忘れてはなりません。利便性を享受するためには、それに似合ったリスク対応が必須です。

リスクを適切にコントロールできなければ、メリットを享受することはできず、かえって大きな事故

や被害に遭うことを避けることは困難になります。そのためには、組織としての情報リスクへの取り組みも必要ですが、従業員各々が情報リスク（セキュリティ）を適切に、素早く判断し対処できる能力（意思決定力）、すなわち「情報リテラシー能力」を持つことが重要です。



一般的にセキュリティとは、安全、保安、防衛、防護、治安、安心、保障、などの意味を持ちます。そして情報通信技術（ICT）の分野では、データやシステム、通信路などを暗号や防御ソフト、アクセス制御機構などを用いて技術的に保護し、機密漏洩や外部からの攻撃・侵入、盗聴、改ざんなどの危険を排除すること、といわれています。

最近は特に、サイバー攻撃、個人情報漏えい、マイナンバー制度導入等の視点から、どちらかというと機密性保護に偏重した視点で話題になるケースが多いように感じられます。

しかし、情報セキュリティマネジメントの本質は、単に情報漏えい等の機密性を確保するためのセキュリティという側面だけではなく、情報の有効活用のための仕組み（フレームワーク）として、情報資産を機密性、完全性、可用性という３つの側面からそれぞれのリスクに対して評価・意思決定・対策し、組織事業の目的・目標達成のために多様な情報を安全かつ有効に活用することにあることを忘れてはなりません。

1-2　2015年のセキュリティ10大ニュースからICT環境変化と脅威を知る

JNSA（日本ネットワークセキュリティ協会）では、毎年その年に話題となった情報リスク（セキュリティ）の出来事や事故・事件についてまとめ、発表しています。

私たちは、これらの出来事や変化が決して他人事ではなく、自分たちの身の回りでも起こる事と捉え、考え、予防のための対策・行動を起こす材料とすることが大切です。

情報に関する事故や事件、出来事から多くのことを学び、リスクリテラシー能力を高めることは現代を生きる人にとって避けては通れないことであり、それを怠りセキュリティ対策を進化させることができない人や組織は、対策する人・組織との格差が広がり、世の中から取り残されてしまいかねないことになります。

2015年のセキュリティ10大ニュース（出来事）

【第1位】	6月1日	日本年金機構で125万件の個人情報が流出
【第2位】	1月9日	サイバーセキュリティ基本法全面施行
【第3位】	9月25日	米中サイバーセキュリティ合意はサイバー戦回避
【第4位】	2月2日	解消されないセキュリティ人材不足
【第5位】	9月11日	国がCSIRTの実効ある体制強化を勧告
【第6位】	7月28日	9億5千万台のスマホに影響をあたえる脆弱性が発覚
【第7位】	7月11日	Flash Playerに対する脆弱性攻撃の増加
【第8位】	10月26日	標的型サイバー攻撃相談件数6倍に
【第9位】	10月5日	マイナンバー制度施行、通知カードの送付も始まる
【第10位】	6月9日	SECCON 2015の開催概要を発表、CTF盛況

【第1位】6月1日　日本年金機構で125万件の個人情報が流出

～詳細な調査結果を公開、事故前提社会に向けた情報共有の先例となるか～

日本年金機構から、機構が保有する個人情報約125万件が、不審メールに起因する不正アクセスにより外部に流出しました。流出件数の多さもさることながら、年金情報という厳重に管理されていたはずの個人情報が標的型攻撃メールにより漏えいした事案として報道などで大きく取り上げられただけでなく、政府のサイバーセキュリティ戦略への影響など社会的な影響が大きな事件でした。

サイバーセキュリティ戦略本部から厚生労働大臣に対して、サイバーセキュリティ基本法第27条第3項に基づき、CISO、CSIRTなどの体制整備、情報システムの分離などの技術的対策、役割に応じた責務遂行のための教育・訓練の組織、技術、人の3つの側面から対策勧告がされましたが、行政組織の体質改善がそう簡単に進むとは考えられず、国民の不安は払拭されていないように思われます。

【第2位】1月9日　サイバーセキュリティ基本法全面施行

～期待の基本法の施行、今後の推進が課題～

日本の今後のサイバーセキュリティの方向性を規定する「サイバーセキュリティ基本法」が全面施行されました。

それまで情報セキュリティに関する法律は、不正アクセス禁止法、個人情報保護法等がありましたが、サイバーセキュリティを国の根幹をなす重要課題としてとらえた本法は、諸外国に比べや

や遅きに失した感はあるものの、画期的な法律として高く評価されています。

さらに8月19日「新たなサイバーセキュリティ戦略～政府機関等のサイバーセキュリティ対策の抜本的強化～」が発表されました。本戦略は内閣官房サイバーセキュリティセンター（NISC）の法的裏付けと機能強化、CSIRT体制強化を含む政府機関における取組強化、対象組織の独立行政法人等への段階的拡大、重要インフラに関する取組強化を内容としています。

最近の情報関連の大きなリスクは外部からのサイバー攻撃と、組織内部の内部不正・ミスの２側面に集約されているといっても過言ではなく、この両側面への早急な対策が望まれます。

【第３位】9月25日　米中サイバーセキュリティ合意はサイバー戦回避

～サイバー戦争が国の安全保障問題のひとつになる時代に突入～

米国のオバマ大統領と中国の習近平国家主席の首脳会談で、両国は相互にサイバー攻撃を行わないことで合意しました。

これは2011年7月米国防省が陸、海、空、宇宙に次ぐ「第5の戦場」と宣言したサイバー空間における一種の不戦合意で、サイバー空間における攻撃が人命含めた国家レベルの被害になりうると米中両国家で相互確認された結果であると考えられます。

サイバー空間は、戦争（攻撃）を仕掛ける者にとって非常に都合のよい場所であり、戦争に必要な人・物（兵器・食料等）を確保、輸送する必要もなく、匿名性が高く、さらに自分たちが傷つく恐れもない。実際今年２月にハクティビスト集団「アノニマス」がイスラム国に対し宣戦布告を行ったが、これもサイバー戦争が現実的にどこでも起こり得ることを意味しています。

ICTが普及し、情報が重要な戦略の意思決定をつかさどる世界では、情報収集やスパイ行為は多くの国で国策として行われています。日本では守りばかりが目立ちますが大丈夫でしょうか。

【第４位】2月2日　解消されないセキュリティ人材不足

～許すまじ、攻撃者の快勝～

日本情報システム・ユーザ協会（JUAS）は、「企業IT動向調査2015」を発表しました。それによると、調査に回答した国内上場企業及びそれに準ずる企業約1100社のうち、インシデント対応者、セキュリティ機器の運用者など６つに分類したセキュリティ人材カテゴリのすべてにおいて、６割から８割の企業が「人材が不足している」と回答したとのことです。

セキュリティ人材を数多く育てるには、何が必要なのでしょうか。

それには、経営層がセキュリティを正しく理解し、情報リスクマネジメントを重要な経営課題ととらえ、社内制度の整備や社員の意識向上に努めることが肝要です。

【第５位】9月11日　国がCSIRTの実効ある体制強化を勧告

～CSIRT構築はゴールではなくセキュリティ活動の出発点～

内閣のサイバーセキュリティ戦略本部は、日本年金機構の個人情報流出事故をうけ、厚生労働大臣に対して情報セキュリティ対策の改善を勧告しました。

その中で、CSIRT（Computer Security Incident Response Team：情報セキュリティインシデント対応チーム）の実効ある体制強化など、情報セキュリティの確保及び情報セキュリティ事案の対処のための省内体制の見直しを指示しました。

セキュリティ対策は、発生してから行動するのでは手遅れ。平時から情報を収集し、分析し、発生する可能性のあるセキュリティ事象とそれにより引き起こされる事態を予想し、事前対策、事後対策を検討し、具体的なアクションプランを策定し、体制を整備し、組織内への普及啓発活動を行う必要があります。

この事案にみるように、CSIRTの構築や強化が多くの組織でなされるようになっている。しかし、CSIRTの構築はセキュリティ活動のゴールではありません。それは出発点です。

これはISMS / ISO27001（情報セキュリティマネジメントシステム）にも言えることです。認証の取得や維持がゴールではありません。そのフレームワークを活用して、いかに組織の目的・目標を達成するのかが大切です。

【第６位】7月28日　９億５千万台のスマホに影響をあたえる脆弱性が発覚

～どうなる？どうする？IoTデバイスに深刻な脆弱性が見つかった時～

全てのAndroidデバイスに影響をあたえる脆弱性に関する情報がCERTより発表されました。標準搭載されているメディア再生エンジン「Stagefright」にバグが見つかりました。Android 2.2以降5.1.1まで、対象となるデバイス数は９億５千万台におよぶといわれています。

Googleはすぐに対応パッチをリリースしましたが、問題はデバイスベンダによるセキュリティ対策が施されたファームウェアの配布に時間を要したり、古い機種については対策が施されない場合も多いことにあります。

また、12月15日には、警察庁から、インターネットに接続されたデジタルビデオレコーダー等のLinuxが組み込まれたIoT機器を標的とした攻撃の観測の報告と注意喚起が出ています。日本においてもスマートフォンを含むIoTデバイスの脆弱性は「今そこにあるリスク」なのです。

IoTが進むにつれて、スマートフォンだけではなく、多くのウエアラブル機器や産業用デバイス、センサー等がネットワークにつながることになります。抜本的な対策がなされなければ、ICTの健全は発展を望むことは困難です。

また、最近ではリリース時に審査があり安全だと思われていた、App Store - iOSにも多くの不正アプリが見つかっていますので、スマートフォンユーザーはアプリに対する情報収集ををするなどをして、確認してからインストールするようにしましょう。

【第７位】7月11日　Flash Playerに対する脆弱性攻撃の増加

～デファクトのディフェクト（欠陥）で大苦闘～

2015年に入ってFlash Playerの深刻な脆弱性が次々と明らかになり、この脆弱性を突いたサイバー攻撃が爆発的に増加しました。９月４日にIBMが発表した調査レポートによれば、2015年に発生した「ドライブ・バイ・ダウンロード攻撃（Webサイトを閲覧したユーザに不正プログラムをダウンロードさせる攻撃）」のうち、実に99%がFlash Playerの脆弱性を利用していると言われます。

Webコンテンツのデファクトスタンダードとなったflashがサイバー攻撃者の標的になるのは或る種の「必然」であり、一昨年から昨年に掛けて集中攻撃を受けた
「JRE（Java Runtime Environment）」と同じ状況です。

今後、FlashからHTML5への移行が進むとしても、それは同時に攻撃者のターゲットがHTML5に移行することを意味します。すなわち、サイバー攻撃全盛の今日においては「セキュリティ強度が低いプラットフォームは、例えデファクトとして普及したとしても、早期にライフサイクルの終焉を迎える」という厳しい現実が示されていることになります。

【第８位】10月26日　標的型サイバー攻撃相談件数6倍に

～正月に　不審なメール　アケマシテ～

IPAが発足させた標的型サイバー攻撃の被害拡大防止を支援するサイバーレスキュー隊（J-CRAT）が、2015年上半期（４月～９月）の活動状況を発表しました。

それによると、「2015年度上半期の支援件数は昨年の同時期（2014年４月～９月）と比較すると、相談件数、レスキュー支援件数がおよそ６倍、オンサイト支援件数もおよそ５倍となりました。特に、公的機関の情報漏えい事案のあった６月以降は大幅な増加が見られた」と発表されています。

標的型攻撃の多くは自組織でその侵入に気づいておらず、情報漏えいその他の兆候を外部から指摘されて初めて気が付くことが多いのが特徴です。

原因として、「攻撃が巧妙になっていること」「対策が追い付いていないこと」「セキュリティ基礎体力の欠如」があげられることから、組織のトップがセキュリティに対しコミットし、組織の構成員のすべてがセキュリティについて自分が何をするべきか理解し実施することでセキュリティに対する組織の基礎体力を向上させる必要があるとしています。

当たり前のことですが、これができていないのが日本の組織の現状です。もう一度、コミットメントの意味を理解する必要がありそうです。

【第９位】10月5日　マイナンバー制度施行、通知カードの送付も始まる

～社員のマイナンバーをクラウドに預けて放置すると、一発くらうど～

マイナンバー法は個人情報保護法と比較すると罰則規定が厳しく、不正に漏えいした場合は４年以下の懲役又は罰金200万円以下が課せられます。この事が「不正な勧誘や個人情報の取得」に繋がっているとの指摘もあります。

一方で、マイナンバー登録等の運用プロセスを、クラウドサービスを利用することで社内にマイナンバー情報を保持しない安易な仕組みが人気を集めているようです。クラウド環境は安く利用できるメリットもあるが、社内でマイナンバーを扱う責任を回避したい企業の姿勢が透けて見えます。

しかし、クラウドサービスを利用した場合でも、マイナンバー情報が漏えいした場合に免責されるわけではなく、情報管理に対する企業の考え方が厳しく問われることに変わりはありません。

税・年金以外のマイナンバー活用の広がりと会社業務との関係がまだまだ不透明な状況で、他人にマイナンバー情報を預けるリスクをどう評価するか、まさに企業の情報リスクに対する姿勢が問われおり、組織がしっかりリスク対策し、セキュリティ人材を育成していく姿勢・考え方を持つことが望まれます。

しかし、現実的には中小事業者では余裕がなく、なかなかそこまで手が回らない現実があります。どうすれば良いのでしょうか。個人情報保護やマイナンバーなど法律で決められたことにコンプライアンスすることは組織の義務ですが、行政はICT国家を目指し、制度を押し付けるだけではなく、情報セキュリティ対策支援で、利用者が安心できるように積極的な支援を行うべきだと考えます。

【第10位】6月9日　SECCON 2015の開催概要を発表、CTF盛況

～セキュリティのいいとも増やそう、正義の輪！～

特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）は、世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材（ホワイトハッカー）の発掘・育成を最終目標とした国内最大規模のコンテストである「SECCON 2015」の開催概要を発表しました。

今回から、CTF for ビギナーズがスタートしたほか、「攻殻機動隊 REALIZE PROJECT」と共同で女性限定のCTF大会を開催など、新しい取り組みも増えて大きく注目されています。

コンピュータ（情報）セキュリティにおけるキャプチャー・ザ・フラッグ（CTF）とは、コンピュータ（情報）セキュリティ技術の競技です。CTFは通常、参加者に対しコンピュータ（情報）を守る経験に加え、現実の世界で発見されたサイバー攻撃への対処を学ぶ教育手法として企画され、「ハッカーコンテスト」「ハッキング大会」「ハッキング技術コンテスト」「ハッカー大会」などともいわれています。

政府も2020年のオリンピックを目指して17年に新たな国家資格「情報処理安全確保支援士（仮称）」を創設し、試験制度を導入し、20年までに３万人の資格取得を目指し、政府関係機関や重要インフラ機関に配置していく予定です。

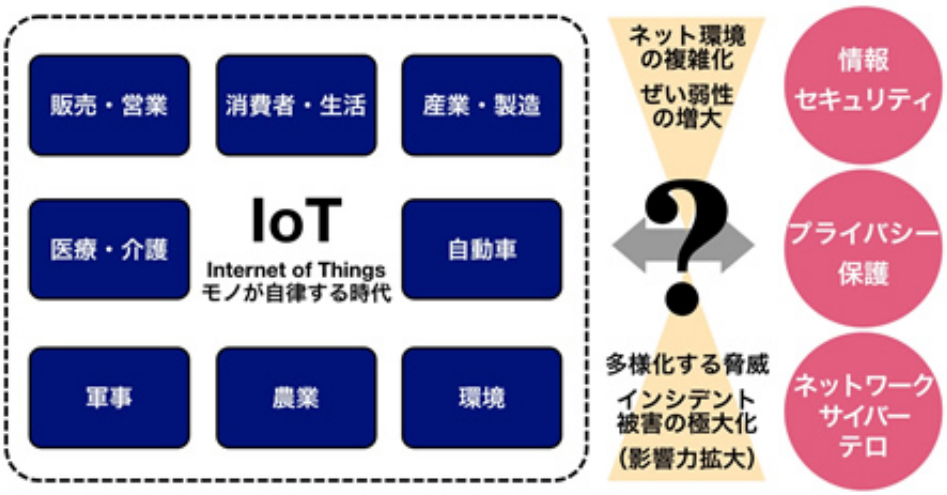
若い人たちが、積極的にサイバー空間でのセキュリティ能力やリテラシーを身につけることは願ってもないことです。そして組織では、売上に貢献する人ばかりではなく、セキュリティ能力を持つ人材をもっと評価することが望まれます。

現在の教育機関でもある程度の情報倫理についてのカリキュラムを実施しているようです。しかし優秀な人材がいたとしても、まず受け入れる組織が変わらなければなりません。

セキュリティ対策は組織を運営するために必要不可欠なインフラコストと考えなければなりません。費用がかかるばかりで、利益獲得に役立たないと考えているような経営方針であるとしたら、ICTが事業戦略上大きな役割を占める今、生き残ることが困難になると思われます。

2-1　IoT（Internet of Things）時代の到来

IoT（Internet of Things）って何でしょうか？日本では「モノのインターネット」という少し理解しづらい表現がされていますが、その目的や実態はどういったものなのでしょうか？



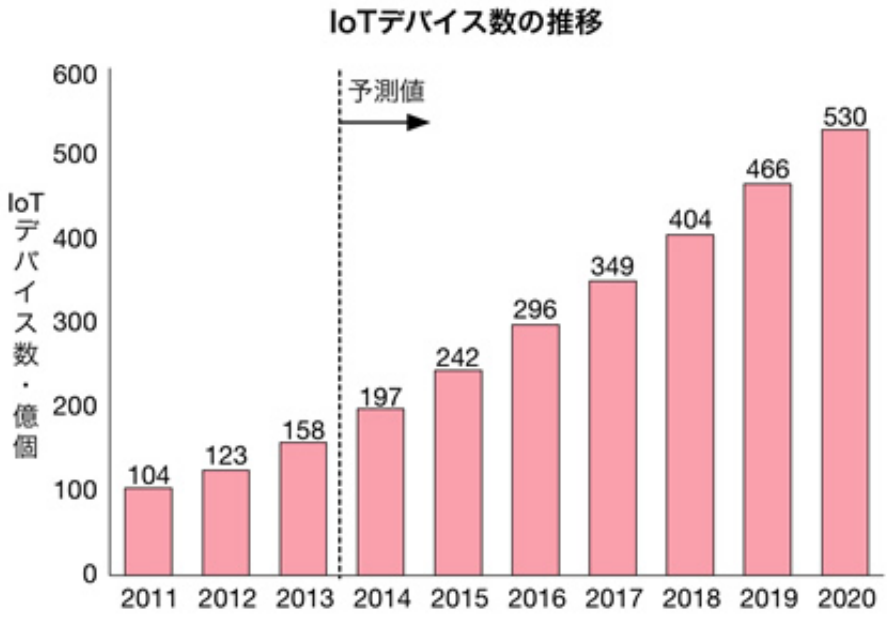
●IoTが実現すること

「IoTはICTに “第３の波” を引き起こす。過去にインターネットが登場したとき、それはユニークな（目新しい）存在だった。しかし、インターネットが汎用的なインフラになった今、ユニークになっているのは、インターネットに接続された “モノ” のほうだ。そのインパクトは、過去の50年間に発生した第１の波／第２の波のインパクトをも凌駕し、スマート・コネクテッドプロダクト（Smart Connected Product）を可能にした」（マイケル・ポーター：経営学者）と期待されています。

どう理解すれば良いのでしょうか。ここ数年の間にICT、IoT/IoE技術の発展により、ビックデータを本格的に活用できる社会がもう目の前まで来ており、サイバーフィジカルシステム＝CPS（実世界とサイバー空間の相互連関）が実現し、さまざまなモノと利用者の間で、大きな価値変革が起こるというなのでしょうか。IoTによる今後の変化のシナリオを想像してみましょう。

●IoTの背景

IoTは、ICTインフラの進化やセンサー技術の発展とコストダウンによって、さまざまなモノをネットにつないで、データを収集することが可能になり、期待も大きく、急速に実装が伸長しているようです。IHS社（技術・環境・部品情報コンテンツサービスプロバイダー）の推定によれば、2013年時点でインターネットにつながるモノ（IoTデバイス）の数は約158億個であり、2020年までに約530億個まで増大するといわれています。



多種多様なモノからさまざまなデータが出力されます。しかし、そのデータを有効に活用するためには、あらかじめその利活用目的やデータ解析能力が重要になります。

また、つながれた各々のデバイスが生み出すデータの質はまちまちですし、種類も豊富で、莫大な量になります。またデバイス自体のサイバー攻撃に対する信頼性もまだ不十分と考えられます。しかし、IoT技術で得られるデータが新しい価値を生み出すことを疑う人はおそらくいないと思われます。

それは、あらゆる製品（モノ）にセンサー、プロセッサー、ソフトウェア、ネットワーク等のコンピューティング機能が組み込まれ、常時接続でクラウドにデータを蓄積し、そのデータの分析結果を製品とやり取りすることで、製品の機能を飛躍的に向上させることができ、利用者、社会に貢献できると考えられているからです。

さらに、そのデータ分析に機械学習・人工知能（AI）を利用することで学習、認識、識別、判断、予測、行動を続け、さらに自立的に学習することも可能になり、人の能力を超えた知見を得ることができると言われています。

ポーター（経営学者）は、これらのネットにつながった製品を「スマート・コネクテッドプロダクト」と命名し、モノの本質を変化・進化させることに大きな価値があり、今までの製品ライフサイクルや顧客との関係性、組織のあり方にも大きな変化をもたらすと言っています。

そして、そのプロセスを「モニタリング」「制御」「最適化」「自動化（自立化）」に分け、以下のように説明しています。

「モニタリング」
センサーと外部のデータリソースを活用し、製品の稼働状況や外部環境の変化などを把握／監視する。たとえば、外気温が設定以上の温度になったら、アラートを出すといった機能。

「制御」
製品に組み込まれたソフトウエアやインターネット経由での遠隔操作で、製品の動作や搭載機能をコントロールする仕組みを指し、人が行きにくい場所にある重機を組み込みソフトで制御したり、遠隔で操作したりといった機能。

「最適化」
モニタリング機能と制御機能を基にしたアルゴリズムで、製品性能の向上や故障予測など、「常に製品を最適な状況に維持する」ことを目的とした機能。

「自動化（自立化）」
さらに、それらのプロセスを「自動化」することで「適切な最適化を行えば、企業はアフターサービスやメンテナンスに費やしていたコストや人件費などを大幅に削減できる」と言ってい

ます。内容的には「サイバーフィジカルシステム」と同様と考えることができます。

●事例

日本企業での事例として早い時期から有名なのが、建設機械をグローバルに供給するコマツの「KOMTRAX」です。

建設機械にGPSやセンサーを取り付け、携帯電話や衛星通信を経由して機材の状況を遠隔で確認するシステムで、既に2001年から標準装備化されており、適切な点検や部品の交換時期、効率的な配車計画や作業計画、燃費改善等による利用者のコスト削減に貢献できる他、故障原因を推定して迅速に修理したり、遠隔操作でエンジンを停止することすることも可能にしました。

さらに、稼働状況から製品の需要動向を予測するなどさまざまなルートを通じて、経済価値を生み出しているとしています。

IoTの発展的な提案として、「スマートコンストラクション（SMARTCONSTRUCTION）」という概念で、施工現場全体を見える化し、モノからコトへ発展的にコントロールを図ることで、「お客様のかかえている課題（労働力不足等）を解決（ICT活用機器導入等で）する」としています。

●IoTの適用分野の例

分　野	適　用
施設	・施設内設備管理の高度化（自動監視・制御等）
エネルギー	・需給関係設備の管理を通じた電力需給管理 ・資源採掘や運搬等に係る管理の高度化
家庭・個人	・宅内基盤設備管理の高度化 ・宅内向け安心・安全等サービスの高度化
ヘルスケア 生命科学	・医療機関／診察管理の高度化 ・患者や高齢者のバイタル管理 ・治療オプションの最適化 ・創薬や診断支援等の研究活動の高度化
産業	・工場プロセスの広範囲に適用可能な産業用設備の管理・追跡の高度化 ・鉱業、灌漑、農林業等における資源の自動化
運輸・物流	・車両テレマティクス・追跡システムや非車両を対象とした輸送管理の高度化 ・交通システム管理の高度化
小売	・サプライチェーンに係る高度な可視化 ・顧客・製品情報の収集 ・在庫管理の改善 ・エネルギー消費の低減
セキュリティ 公衆安全	・緊急機関、公共インフラ（環境モニタリング等）、追跡・監視システム等の高度化
ICT ネットワーク	・オフィス関連機器の監視・管理の高度化 ・通信インフラの監視・管理の高度化

出典：総務省「グローバルICT産業の構造変化及び将来展望等に関する調査研究」（平成27年）

このように、IoTを起点としたシステムは様々な産業や分野への普及を通じて、大きな経済的効果をもたらすと予想されています。

2014年に約6,500億ドルだった世界のIoT市場規模が、2020年に1.7兆ドルになると予測され、Cisco社では、IoTのさらに次のコンセプトとして、「IoE：Internet of Everything」（ヒト・モノ・データ・プロセスを結び付け、これまで以上に密接で価値あるつながりを生みだすもの）の到来を提唱しています。

そして、IoEは2013年から2022年にかけて全世界の企業において14.4兆ドルの経済価値を生み出すと予測しています。そのうちの9.5兆ドル（約66%）はスマートグリッドや工場などの製造現場のスマート化を図った「スマートファクトリー」などの業界に固有の案件の改革から生み出され、残りの4.9兆ドル（約34%）は市場投入までの時間短縮やビジネスプロセスのアウトソーシングなど業界横断的な案件から生み出されるとしています。

これらのようにIoTの時代は、その有効利用によって製品にサービス価値を付加することが可能となり、利用者に新しいサービス価値を提供するイノベーションの起爆剤として期待されています。これからが本当のビックデータ時代のスタートとなるのでしょうか。

●IoTのセキュリティ課題

しかし、課題がないわけではありません。それは、さらなる技術開発による効率化、企業間仕様の標準化、行政のオープンデータ連携、プライバシー保護への社会的合意形成、サイバー攻撃等に対するセキュリティ保護等多岐にわたります。

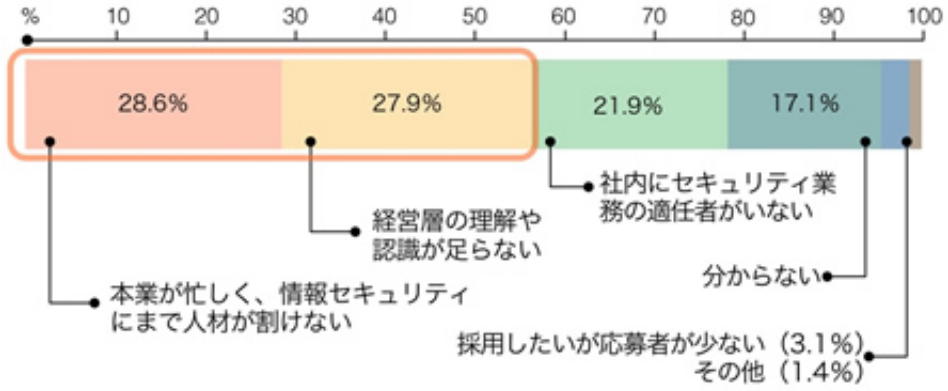
セキュリティの側面では、「攻撃にさらされる機会の増加」（サイバーテロ等）、「デバイスの安全性」、「アクセス制御」、「ファームウェアのアップデート不備」、「セキュリティ対策レベルの不統一」、「利用者のリテラシーレベルの問題」等、解決しなければならない問題が山積しています。

そのため、デバイスの識別や認証、通信プロトコルやインターフェースの共通化、デバイスのセキュリティ評価や検証、安全性の認証といったルール作りも必要となり、企業だけではなく、サービス提供者や業界団体、行政が連携し、官民一体となった取り組みが求められています。

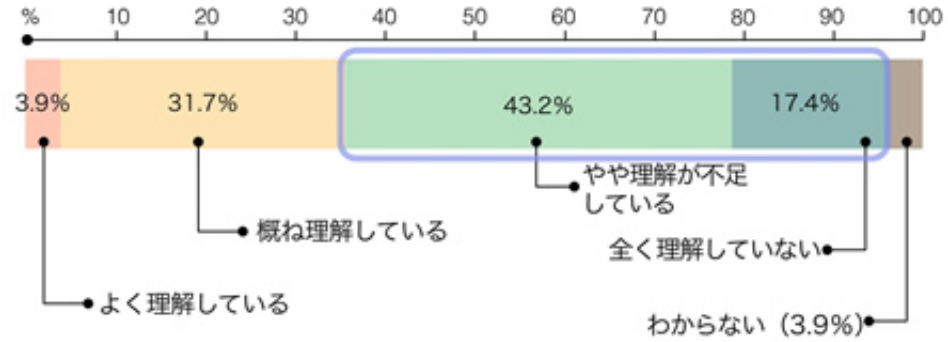
しかし、多くの組織で、情報セキュリティに関する業務に従事する人員が不足してるのが現実です。原因として、本業が忙しく、情報セキュリティ人材まで人材が割けない」「経営層の理解や認識が足らない」の２つで56.5%を占めています。また、「経営層の理解が不足している」という意見が60.6%となっており、経営層の理解が課題となっていることが伺えます。

これからのICTを活用した事業展開を考える上で、情報セキュリティ対策は避けて通れないテーマです。経営層の理解によるセキュリティ人材の育成や雇用拡大が望まれます。

■ 情報セキュリティ人材不足の原因 (N=1,736)



■ 経営層の情報セキュリティに対する理解度 (N=経営者以外の2,731)



（出典：IPA 情報セキュリティ人材の育成に関する基礎調査 2012.4）

2-2　インテリジェントICT

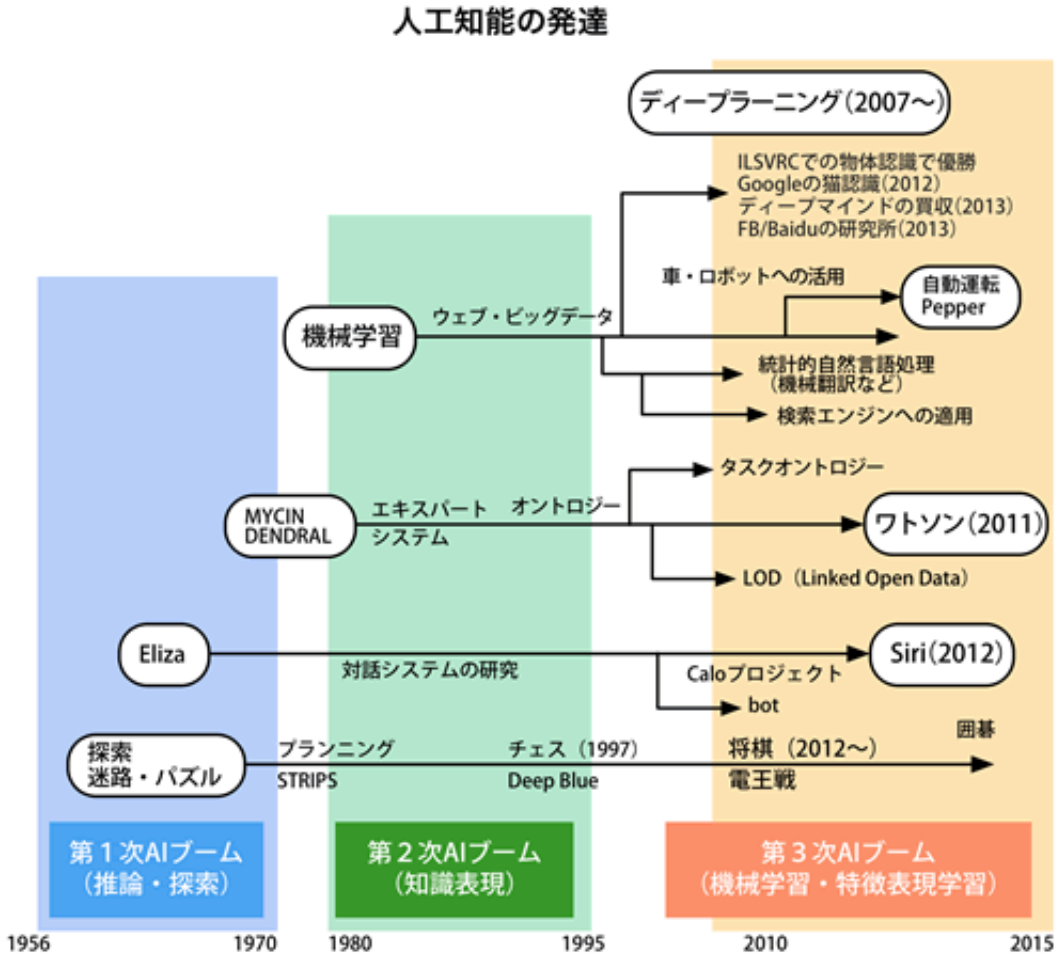
IoT（Internet of Things）やCPS（Cyber Physical System）に欠かせないのが分析・解析機能であり、機械学習／人工知能（AI）を利用してインテリジェント化されたICTによりさらに大きな影響を及ぼすことが考えられます。

人工知能（AI：Artificial Intelligence）というと、IBMのワトソンはすでに、日本国内の金融・保険等さまざまな分野で利用され、一部無料・低価格でのサービス提供もされています。

また、スマートフォンの音声ナビとして使わているiOSのSiriもそのひとつです。私たちの生活の中にも、いつの間にか入り込んで意識されずに利用されています。今後、自動運転や医療・ヘルスケア等だけではなく、多くの生活やビジネスシーンの中で利用されることでしょう。

ここでは、IoTやICTはどういうように進化していくのか。そして、私たちは社会人としてまた一個人として、どのような影響を受けるのかを考えると、楽しみでもあり、一方不安もあります。

さまざまな想像をふくらませることで、これからの仕事や生活の変化について思考することも大切なことです。さて、私たちとICTの未来は・・・・？



これからのICTを活用した社会変革は、コンピュータや通信ネットワーク、それらの上で動く人工知能や活用される多様なデータ、これら技術と人間との間のインターフェイスを可能にします。これら技術の高度化等によってもたらされる変化を「ICTインテリジェント化」といい、また、そのような能力を発揮する技術やシステムの総称を「インテリジェントICT」といいます。

例えば、自動運転車技術に繋がる安全運転支援システム、無人飛行機（ドローン）を用いた商品配送、エンターテイメント業界における完全没入型のバーチャルリアリティ技術、医療分野での遠隔手術、リアルタイムの自動音声翻訳などが既にサービスとして登場しています。

さらに、ロボットを用いた遠隔からの会議参加、スマートフォンで随時呼び出し可能な無人タクシー、脳によって制御可能な義肢・義足も近い未来に実用化するであろうと予測されています。

また、眼鏡や腕時計を高度化し、ネットワークにつながるウェアラブルデバイスが普及の兆しを見せており、遠からず、これらに搭載された各種のセンサによってリアルタイムで人の脳・生理情報や行動情報が取得され、個々人の身体的状況に合わせた健康管理や個別ニーズに合わせた各種サービスの提供なども実現すると考えられています。

●インテリジェントICTによる変化

ICTインテリジェント化の更なる進展によって、人間の社会はどのように変わっていくのでしょうか。これを次の４つの段階を経る変化として見てみましょう。

（１）インテリジェントICTが人間を支援
（２）インテリジェントICTのネットワーク化による協調が進展し、支援の付加価値が向上
（３）人間の潜在的能力が人工知能によって引き出され、身体的にも頭脳的にも発展
（４）人間とインテリジェントICTが共存する社会へ

（１）インテリジェントICTが人間を支援（人工知能同士が独立して機能）

人工知能の進展により、チェスや将棋といった定型化された領域において、人間を上回る能力を有する人工知能が出現しています。また弁護士事務所における判例探索、医療分野における症例検索、保険業界における審査、銀行での認証等、より広範な知識や判断力を必要とする問題についても、既に知識の量や探索の速度において人工知能が人間の能力を上回りつつあります。

今後、ディープラーニング技術等によって「自ら考える」能力を有するコンピュータが普及し、音声や画像の認識、行動結果の予測等を自ら学習し判断することで、人間が行う業務の軽減や代替、人間の知的活動の支援が更に進むと考えられています。

既にGoogle、Amazon等が厖大なコンテンツ情報や行動履歴、検索履歴等を蓄積し、そこに含まれるパーソナルデータも含めて活用を進めていますが、今後、人工知能が自ら特徴量を抽出できるようになることで、医療や農業といったきわめて変数の多い分野においても活用可能となり、個人の判断（行動の選択、交流する相手の選択、進路の決定等）、企業の意思決定（経営判断、生産性向上、商品開発等）、インテリジェントな社会インフラの実現（防災、犯罪捜査等）など、人間生活のあらゆる側面で人間をサポートするようになると予想されています。

（２） インテリジェントICTのネットワーク化による協調が進展し、支援の付加価値が向上（人工知能の相互連携）

インテリジェントICTが備える知能の分散配置が進展し、情報連携の範囲が大幅に拡大するとともに、調達や製造の効率的な自動調整や安全で安定的なロボット活動が実現します。
この段階では、ネットワーク上に多種多様な能力を有する人工知能だけではなく、異なる専門的能力を持った複数の人工知能を融合して取りまとめる能力を持つ人工知能も出現し、それらの連携、協調が進み、人工知能間で学習結果の交換、統合も自動的に行われることで人間をサポートし、日常生活や業務における生産性が飛躍的に高まり、人への高い
QOL（Quality of Life）が提供されます。

（３）人間の潜在的能力が人工知能によって引き出され、身体的にも頭脳的にも発展

例えば、脳情報を外部に出力できるようになり、人の意識で義手義足、ロボット等を動かすことが可能となるばかりか、自宅に居ながら遠隔地のオフィスにいるロボットを操作し勤務できる可能性もあります。また、ウェアラブルデバイス等を用いた精緻でリアルタイムな健康管理

が一般化することで、人間のコンディションの調整が容易になり、心身の一層の能力向上が可能となると考えられてます。

さらに、ユーザーフレンドリーな人工知能が登場し、コミュニケーションがより高度になることで、人は情報入手に留まらず思考や行動においてもインテリジェントICTを活用して生活するようになりそうです。

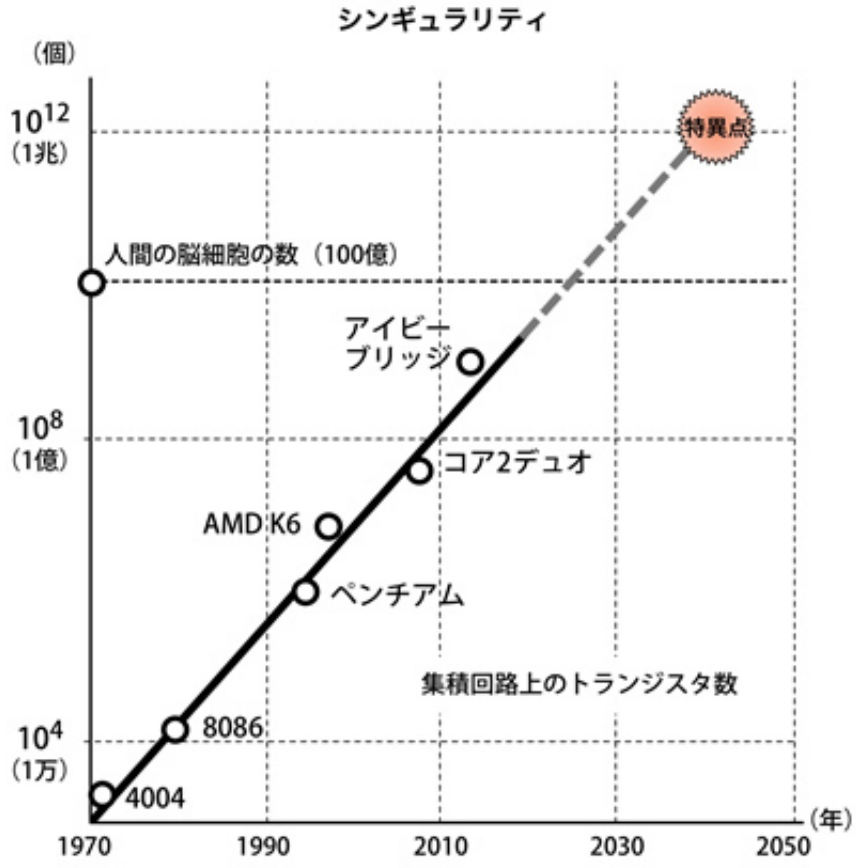
最近の動向では、トヨタ自動車が2016年１月米カリフォルニア州パロアルト（シリコンバレーの中心地）に人工知能（AI）の研究・開発を行う新会社「トヨタ・リサーチ・インスティテュート（TRI）」を設立しました。ここでAIを活用し、自動運転車の実現を目指すとのことです。また、スタンフォードやマサチューセッツ工科大学の両大学とAI研究で提携し、すでに屋内用ロボットの開発を含む約30のプロジェクトを立ち上げています。

2-3　シンギュラリティ（技術的特異点）とは

ある時点で人工知能がその自己学習能力により自らの能力をわずかでも自ら（自立的に）より高めることができるようになると、人工知能の自己再生産による加速度的能力向上が起こり、未知の技術進化が始まると考えられています。

●30年後のコンピューター技術

この時点（特異点）をシンギュラリティと呼び、2045年にシンギュラリティに到達するのではないかと予測されています（米グーグルのエンジニアのレイ・カーツワイル）。具体的には、１台のＰＣ（コンピューター）が2045年に全人類の能力を超え、全てのＰＣが生み出す知能が全人類の知能の10億倍となると考えられています。



コンピューターのCPU上のトランジスタ数は、初期インテル4004や8086から最近のアイビーブリッジに至るまで、10年で100倍、20年で1万倍になった。近い将来、大脳の神経細胞（100億）を上まる可能性がある。

このような人工知能がロボット技術、ナノテクノロジー、遺伝子操作技術等と融合すると、人間を介さない人工知能とロボットによる企画、実験、研究開発、設計、部品から製品までの自動生産等があらゆる分野で実現する可能性があるとされています。

これはSFの世界の話ではありませんが、「2001年宇宙の旅のHAL9000」のように人間を超える知能を持ったロボットの出現で、人間が支配されたり、反乱が起こったり等と少々心配になったり、「WALL-E（ウォーリー）」のような、優しい感情のような能力をもったロボットの出現を期待する人がいるかも知れません。

しかし、最も重要なことは、シンギュラリティに到達するか否かではなく、「（人間に匹敵する可能

性のある）高度な認知や判断、さらに創造を行う力をもった人工的な知性が近い将来に実現する」ことは確実であり、今後の社会制度設計、政策立案は、これを前提に進めていく必要があるということです。

今後、私たちの仕事や生活は大きく変わることになると思われます。しかしその時になってみないとわからないことも事実です。いずれにしてもインテリジェントICTが人間を包むように存在し、インテリジェントICTと人間がシームレスに連携する世界が実現することで、人間とインテリジェントICTが共存する社会となっていくことを期待したいものです。

変化の先が見えないとき、人は少し不安になりますが、技術進歩は止まりません。私たちが好む、好まないにかかわらず、これまで見てきたような未来が到来する可能性は高く、技術が進歩することを前提に、将来を考える必要があります。

そして、ホーキング博士は今後100年以内に人工知能が人間を超えるだろうと警告しました。人工知能が人類を超えるとき、短期的には「誰が人工知能をコントロールするかが問題」となりますが、長期的に見れば「人工知能をコントロールできるかどうか自体が問題」になるとしています。また、科学者と技術者が人間のコントロールを超えない人工知能の調整を行い、人工知能に人類と協力する目的を持たせるべき必要があり、私たちの将来は技術の新興勢力（人工知能）と技術を利用する知恵（人）の争いになると語っています。

●今後の課題

しかし、この技術が良い方向ばかりに活用されるとは限りませんし、この発展の影には大きな脅威があることは誰が考えても明らかです。今後、インテリジェントICTを健全に発展させ、使いこなすための以下のような課題について取り組みを、早急に始めなければならないとしています。

（１）インテリジェントICT研究・開発に係る原則

この高度な機能は、人や社会がよくなるためという、基本原則のもとに進められる必要があります。そのためには、インテリジェントICTの研究・開発に係る原則を明らかにするとともに、発生しうる負の側面（脅威）を限りなく小さくする仕組みを構築する必要があります。それには、プライバシー保護を確実にすることや、リスク分析・評価と対策・管理を行うこと等が考えられます。

人工知能を持ったロボットが出現するのは時間の問題だと考えられますが、これは過去から想定されていました。小説家、ノンフィクションライター、科学者等様々な肩書きをもつアシモフのロボット３原則は、映画や漫画等でもよく引用されているので聞いたことがある人が多いと思います。

アシモフ博士のロボット工学3原則（参考）

第一法則：ロボットは人間に危害を加えてはならない。またその危険を看過することによって、人間に危害を及ぼしてはならない。

第二法則：ロボットは人間から与えられた命令に服従しなくてはならない。ただし、与えられた 命令が第一法則に反する場合はこの限りではない。

第三法則：ロボットは前掲の第一法則、第二法則に反するおそれのない限り、自己を守らなけれ ばならない。

（２）社会実装に向けた倫理、法律上の課題

これまで人間が最終判断していた分野において、判断能力の高まったインテリジェントICTにどこまで判断権限を委ねて良いか、また、その判断結果の責任をだれが取るのかが問題となると考えられます。欧米の先進国ではすでに検討が進められており、米国スタンフォード大学が中心となって進めている活動では、倫理、法律に加え、犯罪、幸福、機械との協調等18項目に係るホワイトペーパーが発表されています。

（３）プライバシー保護の在り方

インテリジェントICTは、厖大なデータを収集・蓄積・分析・活用することで、人間社会をサポートし、人々のQOL（生活の質）を向上させることを目的にしています。当然、医療、ショッピング等幅広い分野に於いて、パーソナルデータの提供を前提とするカスタマイズド・サービスが広がり、サービス享受のためのパーソナルデータ提供が広がることは避けられません。

また、既に各国企業等において多様なパーソナルデータの蓄積が進み、アマゾンやグーグルのような特定の企業は検索や電子商取引、SNSといったサービスや、モバイル端末に係るプラットフォームを活用して大規模にパーソナルデータを収集・活用しているのが現実です。

日本でも、現在パーソナルデータ活用やプライバシー保護に向けて様々な検討がされていますが、時代の流れには逆らえないまでも、国民の納得の行く法整備が望まれます。

（4）インテリジェントICTとの共存を前提とした社会設計

ICTインテリジェント化の進展に伴い、人間の行動や思考形態も変化していくと考えられますが、そのような時代に係る社会設計において、何に重点を置いていくべきか、今後、様々な視点からの研究が必要になりそうです。

さまざまな課題に直面すると思われますが、人間とインテリジェントICTの共存が進む中で、人間とは何か、人間にとって豊かさとは何か、人間の尊厳とは何か、人間らしさとは何か、正義とは何かという、人間にとって本質的な問いに答えることが求められていくと考えられますが、グローバルで考えると、各々の国益や宗教観の違いもありなかなか難しい課題となるでしょう。

（5）インテリジェントICTが社会・経済に及ぼす影響等の評価（インパクトスタディとリスクスタディ）

いずれにしても、インテリジェントICTが社会・経済に及ぼす影響や発生しうるリスクの評価・分析を行う必要があります。インテリジェントICTを使いこなし、利便性やQOLを享受するためには、発生しうる負の側面を正しく把握することが不可欠になります。

例えば、様々な側面を有する異なるインテリジェントICTがネット上で混在することで意図しない事象が発生するリスク、悪意を持った人間の使用によるリスク、人工知能が何らかの理由で暴走するリスク等、様々なリスクの存在可能性は否定できません。

いずれにしても、最終的には私たち自身がそのリスクについて正しく評価し、責任を持った意思決定をするだけのリテラシー能力（判断と意思決定能力）を身につけることが大切です。

（出典・参考：総務省「インテリジェント化が加速するICTの未来像に関する研究会」平成27年）

第２講はこれで終了です。次は第３講です。