経営経理研究　第 124 号
2023 年 10 月　pp. 15-30

〈論　文〉

情報と社会

── 情報セキュリティの事例より ──

金　山　茂　雄

要　旨

技術の進歩には，様々なものがあり，その一つが IT（情報技術）である。IT をコアとなしている社会が一般的に情報社会と呼んでいる。IT は，産業活動そして我々の日常生活を支える重要な社会基盤である。しかし，IT に依存すればするほど，IT に対する脅威は直ちに，自分たちの経済活動や社会生活そのものへの脅威に転化する。情報セキュリティへの取り組みは，自分たちの脅威を無くし，安心して安全な利活用できるネットワークである。そのためには，情報セキュリティの重要性と必要性の認識がなくてはならない。2023 年現在，イノベーションにより IT から ICT，IoT，そして AI が登場した。様々な技術がイノベーション等で実用化され世の中に登場し，それを利活用している。その際，人々はメリットやデメリットについて考える。この点についていくつかの大きな問題が予想される。人々は，ビジネスで得たモノを守ろうとする。ここに，セキュリティの重要性と必要性が生じる。以上のことを踏まえ，セキュリティの重要かつ必要であることを指摘し主張することが目的である。

本研究では，情報セキュリティの実装と実施に関して，ICT の利活用等の研究報告（調査含む）や文献を概観する。その際，2015 年現在を中心に，時系列的な分析を行い，社会の変化（2006 年と 2015 年）を明確にする。次に情報セキュリティに関し，概念の提示とリスク事例の紹介および問題意識から情報セキュリティの現状把握，認識，重要性等に関して再認識し若干の考察を行いたい。

キーワード：セキュリティ，サイバー犯罪，リスク事例，ICT，IoT

1. はじめに

技術の進歩には，様々なものがある。その一つが IT（情報技術）である。IT をコアとなしている社会が一般的に情報社会と呼んでいる。我々の日常生活は，情報システムや情報通信の発展のおかげで飛躍的に便利になった。IT は，産業活動を通して我々の日常生活を支える重要な社会基盤である。しかし，IT に依存すればするほど，IT に対する脅威は直ちに，自分たちの経済活動や社会生活そのものへの脅威に転化する。そして，高度情報化社会の恩恵を享受するために，情報セキュリティへの取り組みが強く求められる。ここに，情報セキュリティの重要性と必要性が生じるのである。その後，イノベーションにより IT から ICT，IoT，現在では AI が登場した（2023 年現在）。

2003 年 10 月に経済産業省が発表した「情報セキュリティ総合戦略」においても「IT が社会を担う時代となった今，個人や個別の企業のリスクが全体的・国家的なレベルのリスクに変貌しうる」と述べている。情報セキュリティは，国家や政府の力だけで実現できるものではなく，企業の従業員や個人等インターネットを利用するひとり一人が，情報セキュリティの確保のために真剣な取り組みを行う必要がある。また，企業の経営や組織の運営に携わる者が，経営資産を防衛する一環として，あるいは社会基盤の一部を担う立場として，情報セキュリティをどのように考慮するべきかについても考えなければならない。

情報社会の進展は情報通信技術を土台とした通信インフラと利用端末を生み出すハードウェア，そして情報コンテンツを生み出すソフトウェアの協調的進化に支えられている。これらの先進的な技術がビジネス界にとって重要であり，これらを支えるビジネスモデルが大いなる役割を果たしていることは，携帯電話の普及の過程で実証された。その特徴は，ビジネスモデルが利用者の意識で大きく変わること。次に利用者の利用意欲の向上によってビジネスも大きく左右される一面があること。最後に日常生活の中で自分の置かれている様々な環境と条件が次に進むヒントになることである。特に，最後は，はじめの二つの項目に大きく影響を与える。つまり，人は何かを利用する場合，社会環境の変化に対して利用者が現状維持に意識しているのならば，経済は活発に活動しない。これらは，ビジネスに連動している。そして新しいビジネスの創出には，今日の社会がどんな社会で，どのような状況にあるのか，を把握し認識することであり，そのためにはこれまでの史的展開が不可欠で社会変化の概観が必要となる。さらに近年，セキュリティに関する諸問題が多く発生している。したがって，ここでは情報セキュリティの重要性と必要性について，ICT の利活用調査や事例を概観する。その際，5 年，10 年，15 年，20 年と 5 年刻みの時系列的な分析が必要となる。ここでは，2015 年現在，を中心に，社会の変化（2006 年と 2015 年）を明確にする。次に情報セキュリティに関し，概念の提示，リスク事例の紹介，問題意識から情報セキュリティの現状把握，認識，重要性等について再認識し若干の考察を行いたい。

2. 産業社会と変化

現在では，デジタル社会の象徴のようなｅコマースや物流で世界的に知られているサプライチェーンマネジメントが主流である。産業の成長には，競争力と密接に関係するイノベーションが必要になる。米国では，2008 年イノベーションが活発に行われ，単なるイノベーションではなくイノベーションを起こすことによって社会的な価値が変わっていくことや価値基準への変化も示していた。しかし，従来の考え方からでは，イノベーションの評価基準が労働生産性の伸び率，資本生産性，技術進歩率または，全要素の生産性の伸び率から判断されるケースが多かった。

イノベーションは，インターネットの活用によるものが多い（総務省「平成 15（2003）年版通信利用動向調査」[1] 総務省「平成 16（2004）年通信利用動向調査」[2]，総務省「平成 27（2015）年度版情報通信白書」[3] を参照のこと）。また，インターネットの活用により，社会やその環境も変化している。経済不況下においてもインターネットの利用は，IT 企業と他の業界とを比べても成長している。“Yahoo”や“Google”といった企業は，社会での存在感を増している。

総務省（2016）『平成 27（2015）年版情報通信白書』によると，通信業界は産業界でも近年目覚

ましい発展を遂げた分野である。1985 年の通信の自由化から約 30 年間で，民間の事業者を中心に積極的なネットワーク投資が行われた結果である。その結果，インフラ（ハードウェア）が大都市圏だけではなく日本全国のほぼ全域でブロードバンドが利活用可能になった。情報は，インフラの整備やコミュニケーションツールから情報の生成，蓄積，処理，加工，そして付加価値を生み出す要素（経営資源）へと変化した。主に，ハードウェアではセンサー技術などの発達で，M2M 通信が現実的になり，スマートフォンの普及が個人をネットワークの世界へと導いた。その結果，産業界の活性化と発展は，この個人のネットワークへの接続と利活用によるものであると認識しなければならない。その際，個人に対しては，個人情報保護やプライバーなどの法律にも及ぶ。よって，安全性と保護の重要が個人まで対象として考えなければならない。また，ICT の高度化に伴い，安心と安全な利用環境の整備が必要である。

2020 年代の世界最高水準の ICT 社会の実現のためには，世界最高レベルの通信インフラの整備が必要である。また，そのためには料金低廉化とサービスの多様化のための競争環境の整備，消費者保護ルールの充実した内容の検討とその対応，制度化などの課題が山積みである。総務省では，2014 年度より「ICT サービス安心・安全研究会」を開催し，次の三項目について検討している。①消費者保護ルールの見直し・充実，② ICT による 2020 年代創造のための青少年保護・育成のあり方，③ ICT サービスの進展に応じた課題への対応の三つである。これらは，通信業界が三つのグループ体制にほぼ固定化したため，事業者のグループ化から一歩進み，ICT から IoT の世界実現に進みはじめた現れである。この IoT の世界は，2030 年を見据えた新たな通信産業への政策と発展への期待もある。ここでは，予測と推測の考え方から 2023 年の安全なネットワーク利活用のためには，いくつかの情報通信白書等を概観し現状の把握，理解，そして重要性を認識する必要がある。

2.1　21 世紀初頭の社会背景（2005 年版情報通信白書より）

高度情報化社会は，我々の人間関係や社会にどのような影響を与えるだろうか。その問いに対する答えらしきことが『「いつでも，どこでも，何でも，誰でも」ネットワークにつながり，情報の自在なやりとりを行うことができる社会』（『平成 17（2005）年版情報通信白書』(2006)[4]）であろう。

過渡期である現在，重要と思われるのが，「選択」というキーワードである。いつでも，どこでも，何でも，ネットワークにつながる。つまり，全てがネットワークにつながっている「ユビキタスネットワーク社会」において，実際に「いつ，どこで，誰とつながるのか」を選択しなければならない。つまり，その自己決定が問題となる。既にインターネットの普及が社会における流通情報のあり方を変えたと言われている。自分たちがどのように情報収集をするのか，考える必要がある。

日常の Web 利用の多くは，ニュースや天気予報などはもちろん，仕事や学業，必要な情報を探す。IT の発達やデジタル化社会は経済面でも「光」と「影」の格差が生じ「明」と「暗」,「勝ち組」と「負け組」など二分化している。その中で情報社会は人間の知的な活動領域を拡げ，お互いの競争を通じて個人の能力を伸ばす。個人の能力の強化は，企業や国家，家庭の価値や社会倫理の後退を招く結果へと進んでいる。教育等高等機関も同様なことが言える。

この選んで探すという情報収集活動はインターネット以前からあるが，デジタル情報が検索性に優れているから，より顕著な傾向となっている。この選んで探す傾向の増加は，自ら選ばない情報

収集にも影響をもたらす。

1985 年頃は，90％以上の人が毎日，新聞を読んでいた。しかし，1995 年～「新聞離れ」といわれているとおり，若年層を中心に毎日読まない人が増えた，2005 年には 10 代～20 代が 50～60％程度になった。30 代でもかなり増えた。この変化の一因には 1995 年から 10 年間で急激に普及したインターネットが挙げられる。もちろん，インターネットでもニュースが読め，「電子新聞」も増えた事実もある。インターネットを利用したことが生活時間や行動頻度も変化させた。その他，睡眠時間が減った，テレビ視聴時間や雑誌閲読時間が減った。その理由として考えられるのは，インターネットの利用によって，それらのメディアからの情報収集が不要になったこと，あるいは，単純に時間がなくなったこと。このことは，マス・メディアが提供するような画一的情報よりも自分で選択した情報を好きな機会に接触するような人が増えたと捉えられる。また，「同じ時間に同じテレビ番組をみんなが見る」といった「メディアを介した同時体験」が，近年減少しつつあるということである。このことは，近年高視聴率を取る番組が顕著に減っていることからも裏づけられる。1979 年には年間 1,860 回もあった視聴率 30％以上の番組が，2003 年には 10 回にまで減少している。テレビの平均視聴時間自体は毎日 3 時間～3 時間半と 30 年間ほぼ変化していないが，視聴が特定番組に集中せず分散化している。それはここ数年普及しているモノの一つとしてハードディスク・レコーダーがある。あらかじめ自分が設定したキーワードに関連する番組を自動的に録画する機能もある。機器面からも自分の好きな情報しか収集しない方向性が助長されている。

ケータイ（情報端末）やインターネットの普及は，自分たちの人間関係にも同様の影響を与えている。これも「選択」というキーワードから観ると，ケータイ（情報端末）やインターネットで「誰かに連絡を取る」また反対に「誰かから連絡がくる」というのは，選び選ばれた人間関係といえる。偶然街ですれ通ったり，たまたま会社や学校で席が隣り合ったりしたことでコミュニケートするのではなく，自分のケータイに登録されている中から，あるいは知っている電子メールアドレスの中から，自分で選んだ人とコミュニケートする（総務省「平成 21 年通信利用動向調査」[5]，総務省「平成 17 年版情報通信白書」[6] 参照のこと）。近年の情報化投資で情報の蓄積はあるものの，その活用方法が見つからない。また，その影響は労働力不足にも現れている。

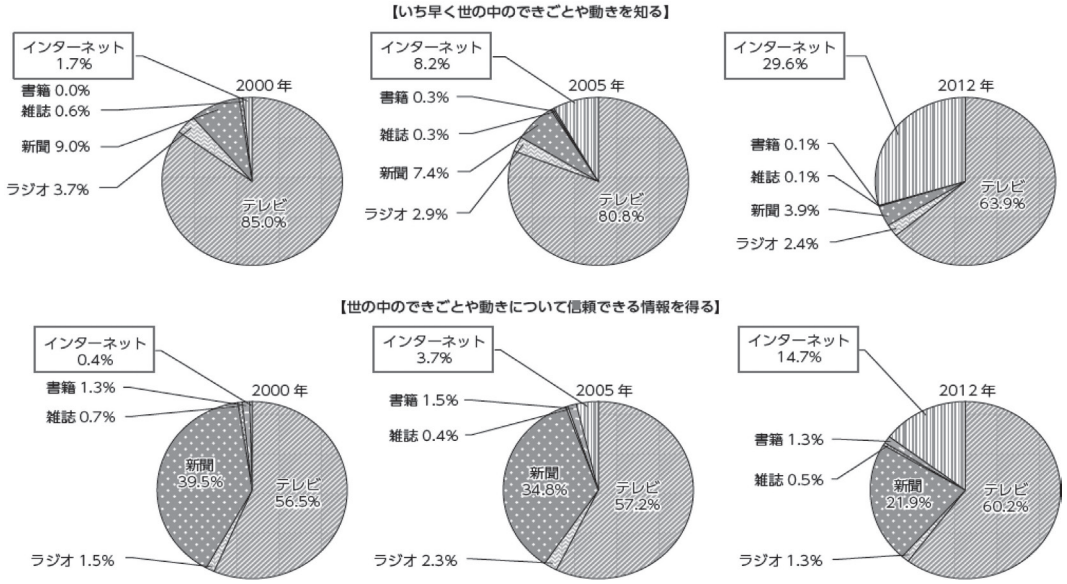
2.2　社会の変化とインターネットの活用（2015 年版情報通信白書より）

社会の変化は，新しい科学技術の誕生とその実用化された商品が日常生活の中で利用されることで把握することができる。現在では，IT の普及や ICT の利用で社会変化の現象が捉えられる。つまり，インターネットの利用がそうである。また，紙の新聞（通常の新聞）が電子版として登場している。通常の新聞の場合，1 頁目の紙面全体，1 頁をめくって 2 頁と 3 頁を目にする。その際，自分が意識しなくても無意識に情報が入ってくる。しかし，ネットショッピングの場合は，自分の必要なモノを探し選択する。つまり，自ら選択しなければならない。情報通信に関するネットワークの現状は，情報を一つのキーワードとして把握，認識し，あらゆるモノを捉える必要がある。ここでは，ネットワークの現状が一つはインターネットの普及が着実に進んでいること。二つ目はブロードバンド化が進んでいること。三つ目は携帯電話によるインターネットの活用と放送のデジタル化の進展であることである。これらは，通常の紙の新聞から電子版の新聞の実行可能性を示している。

図表 1 は，2015（平成 27）年の「情報通信白書」からのデータである。質問は「いち早く世の中のできごとや働きを知る」に対しての回答結果が，インターネットが 2000 年は 1.7%，2005 年は 8.2%，2012 年にはついにほぼ 3 割の 29.6%に達している。また，次の質問では「世の中のできごとや動きについて信頼できる情報を得る」に対しての回答結果が，インターネットが 2000 年は 0.4%，2005 年は 3.7%，2012 年には 14.7%である。このふたつの質問の回答結果からインターネットの利用頻度が増えていることがわかる。利用頻度が増えれば，その分リスクも増える。この調査結果からも分かるように年々インターネットの利用が増えている。利用が増えている原因・要因には，地図（地理）情報の利活用が挙げられる。例えば，車のナビゲーションシステムの利用である。紙媒体の地図の他，PC，カーナビゲーション，スマートフォンがあり，その中でもスマートフォンが増えている。スマートフォンが他の情報端末機より優れている現れである。手軽に持ち運びができるものはなかなか見つからない。もちろん，スマートフォンが他の三つの機能を兼ね備えていることである。最近，新たに飲食店の情報サイトが加わった。

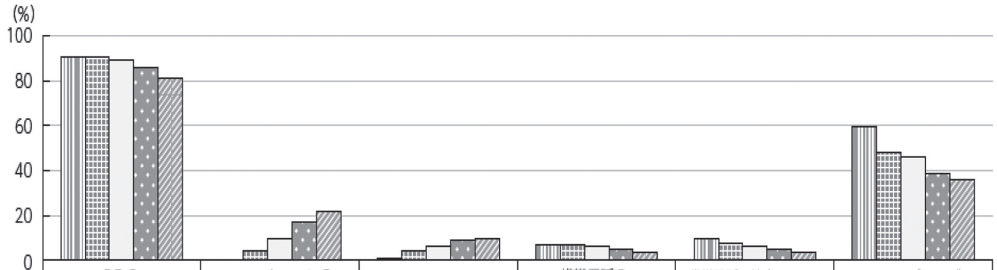
図表 2 のようにインターネットサイトの利用が PC や携帯が減る傾向にある。また，紙媒体のフリーペーパーや雑誌なども減る傾向である。その代わりスマートフォンが増えている。このようにインターネットの普及がいろいろなところで利活用されている。さらに，大学生は，就職活動にも大いに活用している。以前は，就職サイトへアクセスし情報を得ていたが，最近では，企業のホームページに自社情報がある。もちろん，就職活動している大学生にとっては，就職サイトより各企業のホームページから情報を得ることができる。よって，就職雑誌の利用は減り，スマートフォンが有効に活用されていることが分かる。その分，従来からの情報収集方法は，変貌を遂げることとなる。インターネットは，一般社会の中で服を着るように人間の生活の中に浸透している。このように，インターネットが個人の生活に大きく影響していることが分かる。

図表 2 や 3 は，消費者の行動の変化が分かるデータである。特に，インターネットが消費行動の



図表 1　頻繁に利用するメディアの推移（目的別）

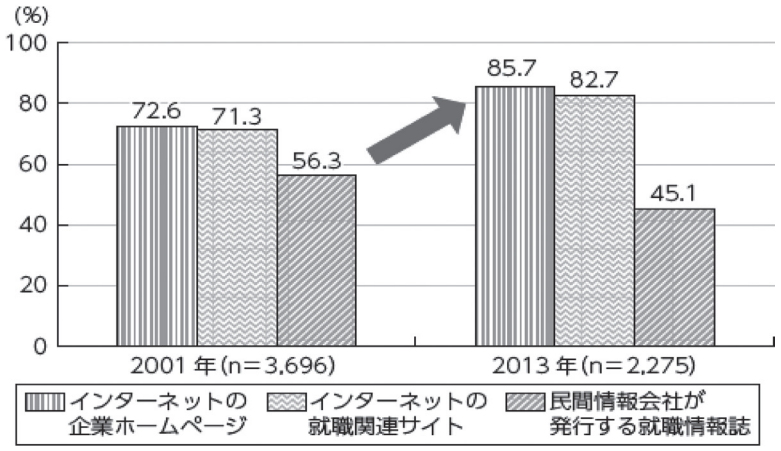
出所：総務省「平成 27 年版情報通信白書」p. 64 より抜粋。



	PCのインターネットサイト	スマートフォンのインターネットサイト	スマートフォンアプリ	携帯電話のインターネットサイト	携帯電話の検索メニュー(iエリア、EZナビウォーク等)	フリーペーパーやグルメ雑誌等の紙媒体情報
2010年3月	91.0	–	1.3	6.8	9.9	59.6
2011年8月	90.8	4.2	4.2	6.8	7.4	48.0
2012年8月	89.4	9.9	6.4	6.4	6.6	46.4
2013年8月	85.9	17.0	8.9	4.7	5.2	39.0
2014年8月	81.6	21.6	9.7	3.9	3.8	35.8

図表２　飲食店の情報を調べる際の情報源の変化

出所：総務省「平成 27 年版情報通信白書」p. 65 より抜粋。



図表３　新入社員における就職活動の利用情報源の変化

出所：総務省「平成 27 年版情報通信白書」p. 64 より抜粋。

情報源になっていることが分かる。2003 年当時は，「ぐるなび」等の飲食店情報サイトの利用率が約 2 割に達していた。2010 年には，PC のインターネットサイトを利用するのが 9 割を超えている。また，インターネットは，就職活動の際の情報源としても利用されている。以前，就職を希望する大学・短大・専門学校生は，学校へ行き，求人票や企業から送られてきた採用案内などの資料・パンフレット等が紙媒体であった。しかし，今では企業案内などはデジタル化されインターネットであらゆる企業情報が手軽に入手できる。1990 年代後半は「リクナビ」等の就職情報サイトが登場し，いち早く利用する者もいた（図表 3 を参照のこと）。その後，就職情報サイトは，エントリーシートの提出や企業が実施している説明会の予約等も就職情報サイトから経由して行うようになった。したがって，このような手軽に情報収集ができる環境にセキュリティの重要さが見えてくる。

3. 情報セキュリティの基本

3.1 情報社会の様相

企業はじめ，組織や個人は，ICT をコアとするネットワークへとイノベーション等により変わっていく。生産，流通，市場などは，非常に高性能なコンピューター，高速通信網の実現によって情報交換が高速に行われる状況にある。さらに，コンピューターと通信技術が持続可能性を伸ばし，そして通信と多様なソフトウェア，高度なハードウェアの組み合わせが様々な分野，領域に影響を与えた。社会環境の変化は，20 世紀の従来型の生産社会においては，市場があまり顧客重視ではない。21 世紀に入り，顧客は，製品のコンセプト，カスタマーの要求や条件を提示し，それが密接に連携する必要があった。既に自動車業界ではバイヤーが理想の自動車をオンラインのスクリーン上で構築し，それからプロダクションのプロセスが始まるというシナリオが進められている。これが実現すれば，カスタム・メイドの車が迅速に納車されていくことになる。

情報社会のネットワークの長所には，普遍的で差別のないネットワーク・プラットホームの構築がある。それによってあらゆるサービスがシームレスな形で提供できるようになる。このことは，グローバルな競争環境の中でネットワーク事業者が成功していくための絶対条件となっていた。将来の情報通信ネットワークはフレキシビリティの高いものではなければならない。全ての産業や全ての情報社会は，効率的な情報処理や高度なハードウェアとソフトウェアおよび通信に依存する。そして，情報通信網は非常に高い性能と信頼性を提供する必要がある。このようなインフラの構築と世界的なシームレス・サービスの提供にあたっては国際協力，国際協調が急務となり，過去から明かなとおり，事業者がそれぞれ独立独歩で進めば，決してシームレスなネットワークを実現することにはならない。もちろん標準化に関し，既に開発された製品やサービスをさらに研究開発を積み重ねてきたという実積が企業側にあること。あるいはそれぞれの社会においてインフラの要件が異なっていること。そして，それぞれのエゴイズムがそこに存在する。そのために，調整ができず，いわゆるデファクト標準が出現することになる。これは他の標準化の結果でも明らかなとおり，結局は市場が決定を下すことになる。このような開発や展開というのは，時としてリスクを伴うことになる。

21 世紀への企業の新展開は世界をリードする先端技術の開発，そのサービス化を世界に向けて実用化することである。もちろん，総合力によるシナジーの発揮とグローバルなネットワーク・アンド・アライアンス（N & A）を図っていくことである。このことは日本の今後への通信産業の発展への最大の課題である。

現代社会，つまり情報社会といわれている今では，情報が氾濫し，自身に必要な情報が手に入れにくくなっている。それは，情報の多さもあるが，正確な情報であるのか，それとも不正確な情報なのか，判断しにくい状況になっているからである。物事に対する決定が出来ないのもこの点にある。したがって，逆の情報が社会に伝わることや身のまわりにも同様な状況が発生する場合もある。また，情報は，受信者によって内容の理解が異なる。特に，現代社会では，自身に都合のよい情報に思ってしまう場合もあり，意図的に間違った情報を伝えて，社会不安を発生させ，あおることもある。いわゆる，パニックである。一般的には，日本ではパニックが起こる可能性は低いが，他の

地域では現実に起こり，社会不安に陥っている。社会は不安な状態が長く続くと人は普段と異なった結果を導き出す傾向にある。この状況で，少し情報を流すだけで不安を増大させ，急激なパニック状態に陥るのである。したがって，情報は量と質が共に重要であることが分かる。そして，情報の使い方が最も重要であるといえる。そのために，情報セキュリティが必要となる。ISO27001 は，ISMS の情報セキュリティマネジメントシステムの強化したものである。ISMS とは「マネジメントシステム全体の中で，事業リスクに対する取り組み方に基づく，情報セキュリティの確立を行い，導入と運用，そして監視と見直し，さらに維持し改善を担う部分」と定義されている[7)]。このマネジメントシステムには，組織構造や方針，そして計画作成，責任，さらに実践，手順，過程や経営資源が含まれる。

情報社会は，普段の生活で Web 利用されている多くは，ニュースや天気予報などはもちろん，仕事や学業に関することが必要な情報として探されている。その中で情報社会は人間の知的な活動領域を拡げ，お互いの競争を通じて個人の能力を伸ばしている。個人能力の強化は，自己が関わっているあらゆることの価値を高めている。しかし，その一方では，社会倫理の後退を招く結果へと進んでいる。

インターネットは簡単に情報を得たり，発信したり，e メールや携帯電話の普及により個人と個人の関係が強くなっている。また，文章を気軽にやり取りできることは「インターネットのすばらしさ」を表している。ブロードバンド時代の到来が双方向通信を可能にし，誰でも情報の発信者になれる。つまり，インターネットの利活用も重要であり，かつ単に利便性だけではないことを十分理解しなければならない。

このように社会環境の変化は，個人，集団，文化，習慣，価値をも変える。情報の価値観が従来は有形だけであったが現在は無形も含めて捉える。つまり「ハードからソフトまで」価値観が拡がっている。その現象は IT による労働，つまり知的労働や自己改革の必要性，協調性の欠如など，様々なところに及んでいる。さらに「ストレス」が感情の変化とともに日常生活に入り込み，個人生活も変えた。そして，今では自己の未来に対する自己実現への意識と意欲が欠けてきている。社会や個人等を守るためにもセキュリティに対する把握，認識しなければならない。IPA でも PC 等の情報機器や端末等を利活用している者は，十分理解し認識しなければならないと指摘している。よって，情報セキュリティは重要であり，次に基本概念，情報収集，モノネットワーク等のセキュリティを概観し重要性に再度認識する。

3.2　情報セキュリティの概念

情報セキュリティとは，「正当な権利を持つ個人や組織が，情報や情報システムを意図通りに制御できること」である。情報セキュリティマネジメントシステムの国際標準である ISO/IEC17799 には，「情報の機密性，完全（保全）性，可用性の維持」と定義されている[8)]。これらが情報セキュリティの三大基本理念ある。

(a)　機密性

認可された者だけが情報にアクセスできるようにすること。つまり，データの保護である。情報の漏えいを防ぐことで確保される。具体的には，ID やパスワードの設定などによって，

組織の内外の者が組織内の情報へアクセスできないようにする，あるいは，機密情報については，組織内の者であっても限られた者だけがアクセスできないようにすることである。最近は，個人悄報の漏えいが大きな問題になっているが，権限のない者に情報が渡ることで，様々問題が発生している。

(b)　完全（保全）性

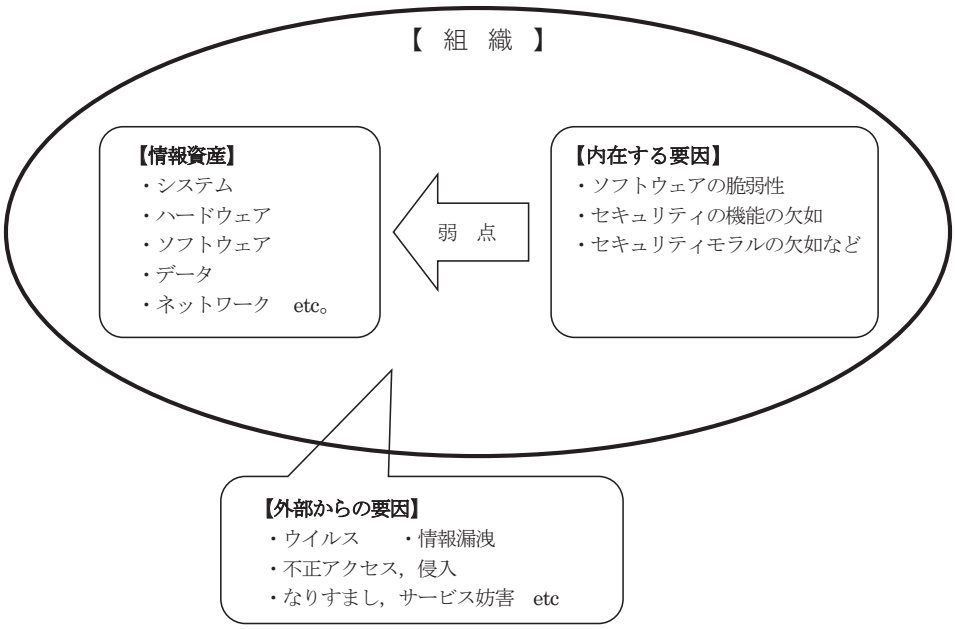
情報や情報の処理方法が，正確で完全であるようにすること。つまり，正確性と完全（保全）性の維持である。不正アクセスによりホームページの情報が改ざんされ，情報システムが勝手に変更されないように，適切な保護を行い，決められた取り扱い手順を守ることにより確保される。情報が，権限のない者によって勝手に変更されたり，削除されたり，破壊されたりすると，情報の安全（保全）性が損なわれ，情報の正当性や情報そのものの価値が失われる。

(c)　可用性

許可された者が，必要な時に情報や情報資産にアクセスできることを確実にすること。つまり，利用・制御ができることである。コンピューターのウイルス感染や白然災害によるシステムダウンなどで情報が使えなくなる，などといったことを防ぐことで確保される。

役所や銀行の窓口業務が止まると，大きな社会的混乱を引き起こすことになる。悄報システムが必要な時に使えないのは，社会問題になることである。

以上，「情報の機密性，完全（保全）性，可用性の維持」について示した。その他に「情報資産，リスクとインシデント」についても知っておく必要がある。また，この三つの要素（用語・言葉）



図表 4　リスクの要因

出所：経済産業省「海外事業活動基本調査 ── 平成 20 年度実績 ──」より。

の頭文字をとって「情報セキュリティの CIA」と呼ばれている。情報セキュリティを推進したり，評価したりする際，上記の三つの視点のバランスをとることが重要である。外部に情報が漏れたことを恐れているあまりに情報を参照することができなくなっていては情報資産を有効に活用しているとはいえない。つまり，情報セキュリティの機密性と可用性とのバランスが重要ある。また，情報を管理する場合，その更新が行われ，完全（保全）や正確性が維持されるような仕組みになっているかどうかも重要であり，これが完全（保全）性である。その他には，情報資産とリスクとインシデントがある。

(d) 情報資産

資産には，不動産や商品など，目に見える資産もあれば，財務情報，人事情報，顧客情報，戦略情報技術情報などの目に見えない資産もある。これらを情報資産と呼んでいる。個人および組織には多くの情報資産が蓄えられている。それらは，システム（ハードウェア，ソフトウェア），ネットワーク，データ，ノウハウなど，様々な形態をとる。IT の普及に伴い，悄報の価値は非常に高くなっている。

(e) リスクとインシデント

リスクとは，情報資産を脅かす内外の要因によって情報資産が損なわれる可能性を言う。これに対し実際に情報資産が損なわれてしまった状態をインシデント（incident：セキュリティ事故）と呼ぶ。大切な情報の損失は，企業にとっても個人にとっても大きなダメージをもたらす。企業の場合はその存続を脅かす場合もあり，情報資産を守るための方策は，企業経営にとって必要不可欠である。

情報資産やリスクおよびインシデントには，リスクの要因を明確な状態・状況で把握していなければならない。リスクをもたらす要因は何があるか。組織の外部からの加害，つまり脅威である。具体的には，ウイルスやシステムに侵入（不正アクセス）するのがクラッカーである。しかし，見逃してはならないのが，組織に内在している要因である。例えば，社内で使用しているシステムにソフトウェア的な弱点があればどう対策するだろうか。セキュリティホールとなって，セキュリティ事故（インシデント）を招く可能性がある。また，そもそも組織内になんらセキュリティについての概念がない，という状況も考えられる。例えば，社内データベースにどの社員でもアクセスできるとしたらどうなるか。顧客データの漏えいなど，大きな被害につながったとしても，文句のつけようもない。米国における不正アクセスの調査によると，外部より，内部の者による不正アクセスや内在する原因によるセキュリティ事故のほうがはるかに多いというデータもある。このように，内部と外部の 2 つの側面からのリスク要因を個別に検討することが，情報セキュリティを考慮する第一歩といえる（図表 4 参照のこと）[9]。

3.3 情報セキュリティとリスク事例

2008（平成 20）年前後から，情報セキュリティが劇的に変化している。IPA（Information-Technolgy Promtion Agency, Japan：独立行政法人　情報処理推進機構）は，企業や組織体のシ

ステム開発者や運用者を対象に，情報セキュリティインシデントや攻撃手口に関する報告やその対策の情報の提供を行っている。さらに，一般利用者向けとしてパソコンやスマートフォンを使用した情報セキュリティの認識と理解を促進している。特に，2014 年には，インターネットのいくつかの脆弱性が見つかり，それを利用した攻撃も確認されている。また，ネットバンキングの法人口座における不正送金被害の拡大，国・政府の機関やインフラ事業に従事している主力企業の機密情報をターゲットとした標的型攻撃も起きている。さらに，外部攻撃だけではなく内部の不正が表面化し社会的な問題になった。こうした様々な事柄が起き，未然に防げないところに問題があるが，少しでも外部，内部の問題に対応するために，2014 年 11 月にサイバーセキュリティ基本法が成立し，国・政府のセキュリティの強化へと変わった。今後，標的型攻撃に対抗する取り組みが今以上に強化されると思われる。現在では，手軽に情報収集ができる環境にセキュリティの重要さが見えてくる。特に，社会では様々な事例があり，その中から「リスク事例の個人情報の漏えい，常時接続状態，無線 LAN（Wi-Fi）など」に関して次に示す。

(a)　個人情報の漏えいのリスク

2004 年 2 月，ある大手インターネット接続事業者から約 460 万人分の顧客情報が流出するという事件が大きく報道された。原因は，ID（Identification：識別番号）とパスワード管理のずさんさである。かつて業務委託を受けていた大物の ID やパスワードが，その者の退職後も削除されず，1 年間も外部からアクセス可能な状態にあったということである。そのため，このパスワードを使って顧客情報が引き出された。この会社では，「ご迷惑をかけた」として，460 万人の顧客全員に 500 円相当の金券を送ることを発表した。金券を送るための費用総額は約 40 億円といわれている。また，翌 3 月には，大手通信販売会社から約 30 万人分の顧客情報が流出したことが明らかになった。この会社は，顧客情報流出を謝罪し通信販売活動を 1 ヶ月以上も自粛した。販売活動自粛による売上損失は，数十億円以上と試算された。このように，個人悄報の漏えいは，企業にとって大きな損害をもたらした[10)]。

(b)　常時接続状態のリスク

会社に勤務している A さんは，ADSL を利用してインターネットを楽しんでいた。接続時間にかかわらず料金が一定のため，24 時間接続したままの状態であった。ところが，気がつくとクラッカーに侵人され，ある有料サービスに登録していた ID とパスワードが盗まれてしまったのである。その後，同一ユーザ名によるアクセスが頻繁に行われ，そのことを不審に思ったサービス会社から A さんに問い合わせがあり，ID とパスワードの流出が発覚した。無防備な状態で常時インターネットに接続することは，不正アクセスされるリスクと常に隣あわせでいる[11)]。

(c)　無線 LAN（Wi-Fi）のリスク

無線 LAN（Local Area Network）は，ケーブルがなくてもインターネットにアクセスでき，とても便利である。しかし，無線 LAN の電波を検知するようにセットしたコンピューターを自動車に積み込み，無線 LAN のアクセスポイントを求めてオフィス街を走り回るウォードラ

イビング（War driving）という行為が横行している。無線 LAN の電波はビル外にも到達してしまうので，実際にウォードライビングを行ってみると，実に多くのアクセスポイントが検知できるようである。しかも，そのアクセスポイントを経由するデータには暗号がかけられておらず，ID やパスワードなしでアクセスポイントから侵入できる場合も多い，ということである。無線 LAN は，その便利さから普及が加速していますが，セキュリティ設定を怠ると，そこが弱点となって社内のネットワークに不正侵入されてしまい，大事なデータを盗まれたり，ネットワークを不正利用されたり，思わぬ被害を受けてしまうこともある。IT 環境が一般企業や個人まで幅広く浸透することにより，セキュリティを脅かす危険性も一段と身近になってきている[12)]。

(d)　その他（サーバ攻撃，サービス妨害　他）

企業では，社内の LAN によるメールサービスや Web サービスなどの様々なサービスが利用されている。このサービスを提供するコンピューターがサーバである。メールサーバは，メールの集配を行い，Web サーバはユーザのブラウザからのリクエストに応じてコンテンツを提供している。このようにサーバは，多くのユーザによって利用されているため，サーバへの攻撃は，より大きな被害をもたらす。特に，企業が取得した情報など，情報漏えいなどである。サーバにはユーザ情報などの貴重なデータも保管されている。この点からも攻撃のターゲットとされやすい。サーバに大量のデータを送って過大な負荷をかけ，サーバのパフォーマンスを極端に低下させたり，サーバを機能停止に追い込んだりする（Dos 攻撃）。災害などで電話が集中すると，電話回線がパンクしてしまうことがあるが，これと同じ状態をサーバに引き起こそうとする攻撃である。最近では，Dos 攻撃を行うコードをコンピューター内に仕込むウイルスも登場している[13)]。その他，米国ハッカー国際会議が米国ラスベガスで毎年 8 月に開催される（若江雅子（2015）「米国ハッカー国際会議」『読売新聞（朝刊）』8 月 26 日，p. 15）。今年も 8 月下旬である。国際会議は「ブラックハット」，「デフコン」である。今年は，IoT（Internet of Thing：モノネットワーク）の弱点を明らかにし，サイバーテロへの悪用を警告する発表が国際会議で行われた。IoT とは，モノのインターネットの総称である。様々なモノに通信ができる機能をつけて情報を収集し，分析し，製品の開発やサービスに活用する仕組みである。例えば，生活支援ロボットなどがそれである。「ブラックハット」は，最先端のセキュリティ状況が発表された。この会議は，1993 年，仲間とパーティーが始まり徐々に広まり，今では 18,000 人が参加している。世界の人々がインターネットを使い送金していた。またサービスを受けている。特に，年々増加の傾向にある電子送金システムや電子決済処理システムが社会環境の変化もあり利用者も増えほんとうに安心・安全に利用できなければならない。例えば，自動車の場合は「運転中，急にワイパーが動き，触ってもいないのにブレーキがかかり，ハンドルもクルクル回りはじめるなど」，PC で自在に操作が可能である。これは自動車のハッキングである（ネットワークに接続し，遠隔操作）が，他の製品でも可能であることを指摘している。つまり，このネットワークでは利便性のあまり，裏ではリスクが生じる可能性が高く，常にリスクとの背中合わせの状態であることを認識し，意識しなければならない。

日本では，一般社団法人重要生活機器連携セキュリティ協議会が IoT 製品の検証ツールや

基準作成に取り組む。はじめは，カーナビケーションやPOSの販売時点情報管理システムなどから取り組むようである。

3.4 IoTの情報セキュリティ

現在では，インターネットの利活用は社会環境を変化させた。社会環境の変化は正確な情報の把握と判断ができない状態を発生させている。いわゆる，企業事例でもある偽情報が飛び交うからである。情報の信頼性，信憑性等は事業を展開する上で重要である。よって，セキュリティは重要である。

インターネットの利活用は時間の経過とともに，日常生活の一部になっている。

ICTからIoTへとネットワークが進歩しているが，IoTの情報セキュリティにはあらゆるものが対象となる。例えば，米国の政府監介院（GAO）が2015年に航空機の不正アクセスに対する可能性を警告したが，未対応である。航空機システムは世界的に連携しているが，認証はされていないので不正アクセスのリスクが高いのである。各航空機は自分の位置を放送しそれを地上で受信管制している。外部からこれを簡単にコントロールできるのである。位置を変更して再発信させることができるので衝突が発生する可能性もある。スマートフォンを使ってBMWの白助車を操作したとか，技術領域は多岐にわたるのでセキュリティの担保が極めて難しい。IoTデバイスには，現状でいろいろな脆弱性がある。IoTデバイス1個当たり平均25件ぐらいの脆弱性がある。もちろん既存デバイスへの攻撃もある。各種のデバイスがマルウェアの温床になって多量の攻撃ができる現状では，コントロールが困難である。これは非常に難しい問題である。

企業における問題意識は，サイバーセキュリティは経営問題であり，社会問題化のリスクもある。特に，マルウェアによる攻撃の人半はクライアントPCからであり，既存の不正プログラム検知方法だけでは不十分である。不正送金では法人の口座が狙われやすい。そして，企業内に閉じて外部ネットワークには絶対につながらないシステムは今や難しい。外部からの利用，下請け企業や関連企業を含めて全従業員のセキュリティ意識にまできちんと責任を持てるか，というと必ずしもそうではない。情報がいったん漏えいしたら回収できないなど多くの課題がある。企業経営者には，組織目的の確認と改善，迅速な意思決定，社員意識改革・教育，セキュリティ監視・リスク認識である。企業経営者は情報セキュリティ対策に意識を持つことは当然であるがそれだけでは不足である。今どういう攻撃があり，その内のどの部分を防げているのかを認識しておく必要がある。自分はセキュリティ担当であるが，情報セキュリティ対策はその部下に任せているというようなことでは不十分である。そして，セキュリティ事故に備えた演習も行わなくてはならない。対策の中で考えなければならないのが法律である。情報法制に関して，サイバー空間では法律の限界がある。特に，国境を超えると匿名性が高くなり法律の施行ができなくなる。国内では以前から各種の法律が施行されている。その中で，電子署名法がそれに該当する法律である。サイバーセキュリティ基本法は，施行して1年が経過した。その後，監視対象の拡大を目的に改正案が提出されている。サイバーセキュリティに関しては，組織間の連携が必要であり，各種情報の共有化を図るための組織の再編も必要である。

4. おわりに

社会環境の変化はイノベーションと技術の進歩の結果に現れてくることは明らかである。また，社会的価値，意味が媒介となることも当然である。情報社会の形成に至ったとき，情報の本質的な側面が実感できると考える。

これらのことを踏まえながら，新たなノベーションと新技術が生活に浸透し社会，生活，文化，社会的性格，価値，意味が新しく形成される。その社会の形成には，重要かつ必要なことは，安全であることである。様々な人々が暮らす社会では，多次元認識とその認識が社会，生活，文化，経験に影響を及ぼす。筆者が以前から述べている課題テーマの中で，情報の文化的経験は影響を与えているのか，に対し現在の情報社会では答えは出ている。また，社会環境の変化は大きな意味を理解する必要がある。例えば，インターネットが単に利便性だけではないことをもっと知る必要があり，そこに情報セキュリティに対する認識が不足していることが分かる。インターネットの利活用が年々増えている傾向は，今後も続くと考える。さらに，小型の情報端末機が普及するにつれて情報に対する安全（保全）性がより一層重要であり，かつ必要になる。

今後はセキュリティ研究の開発強化が重要かつ，必要である。つまり，セキュリティに関する研究開発が極めて重要な役割を持っていることを理解しなければならない。しかし残念ながら，社会のセキュリティ技術は輸入依存である。情報セキュリティのコア技術やセキュリティ情報は社会にとって有益で必要アイテムであり，これは国際間でインテリジェンス情報をやり取りするための交換条件にもなる。このような情報はきちんと保持し監視する必要性がある。セキュリティシステムは今後より複雑化するので，これに対応できる情報セキュリティの基礎研究が必要である。さらに，セキュリティ解析のコア技術と設備が重要である。従来は専門家がチェックしているが，人間による対応では間に合わない。当然，コンピューターが対応することも考えなければならない。

最後に，AI によるセキュリティ対策や人材育成も必要である。さらに，組縦内では、担当責任者の存在も重要である。企業の経営者，セキュリティ責任者，セキュリティ担当者，企業グループなど，セキュリティ情報共有組織および横断・監視組織が必要である。

謝辞

最後に，本稿は令和 5（2023）度拓殖大学経営経理研究所個人研究助成による研究の成果の一部であること。そして，筆者は，日頃の研究活動に対し拓殖大学経営経理研究所に大変感謝するものである。ここに記して同研究所に謝意を表したい。

《注》

1） 総務省（2004）『平成 15 年版情報通信白書』ぎょうせい，pp. 1-26. 平成 15（2003）は，ブロードバンド，電子商取引，モバイルワークなど，情報通信の普及や高度化があらゆる場面において利便性をもたらすことが分かった時期である。しかし，その反面，情報セキュリティのリスクを増やすことにも気付く。当時は，情報通信に係わる全ての者があらゆるリスクを考え，情報セキュリティの必要性と対策を認識する「セキュリティ文化」の確立することが急務とされていた。

2） 総務省（2005）『平成 16 年版情報通信白書』ぎょうせい，pp. 28-30, pp. 59-60. 平成 15 年版情報通信白書の報告に関係し今後の「ネットワーク社会の構築」が示されている。ネットワークインフラの変化，企業のネットワークの活用や国民生活の変化など，「ユビキタスネットワーク社会の実現」を目指

している。情報セキュリティの重要性はもとより，デジタルデバイドに対する影響が課題として提示されている。この課題は，「平成 18（2006）年版情報通信白書」に情報通信やインターネット関係の立法化（個人情報保護，プライバシー，不正アクセスなど）と同時に対策が示されている。

3） 総務省（2016）『平成 27（2015）年版情報通信白書』ぎょうせい，pp. 64–69．情報セキュリティに関する事項は，平成 27 年から現在の令和 5（2023）年に至っても情報通信やインターネット関連の法律が改正され追加されている。しかし，現在でも 100％の安全性が確保されていない。さらに，2012 年以降「スマートフォン」の利用が増え，PC だけの対策が情報端末機器の種類が増えることでその対応が難しくなっている。

4） 総務省（2006）『平成 17（2005）年版情報通信白書』ぎょうせい，pp. 1–24．”U-Japan” とは，2010 年の日本の姿を示したものであり，当時少子高齢化社会の中でいろいろな課題が ICT によって解決されることを意味している言葉である。その理念は，4 つの ”U” である「ユビキタス，ユニバーサル，ユーザー中心，ユニーク」の言葉で「ユビキタス」が中心としている。

5） 総務省（2011）『平成 22（2010）年版情報通信白書』ぎょうせい，pp. 160–174．当時「ICT の利活用による持続的な成長の実現」を目指していた。中でも地球温暖化の問題，グリーン ICT の推進，地域活性化，イノベーション，グローバル展開を通じた国際競争力強化の検証などが課題であった。

6） 総務省（2006）『平成 17（2005）年版情報通信白書』ぎょうせい，pp. 1–24．当日は，4）と同様に「ユビキタスネットワーク社会の実現」を目指している。

7） 情報処理推進機構（2014）『情報セキュリティ読本』実教出版，pp. 10–11．ISO（国際標準化機構）の「情報の機密性，安全性および可用性の維持」であり，情報セキュリティの基本概念である。その他に関連する項目・内容としては「情報資産，リスクとインシデント」がある。

8） 情報処理推進機構（2014）『情報セキュリティ読本』実教出版，pp. 10–11．6）と同様に ISO（国際標準化機構）の「情報の機密性，安全性および可用性の維持」であり，情報セキュリティの基本概念は重要である。近年では，外部からの侵入行為（不正アクセス）が起きている。もちろんサービス妨害も対象となる。

9） 経済産業省（2009）『海外事業活動基本調査 ── 平成 20 年度実績 ──』．

10） 情報処理推進機構（2014）『情報セキュリティ読本』実教出版，pp. 2–3．個人情報の漏えいは，いわゆる IT の落とし穴であり，特に顧客情報を扱う事業者や業務として扱っている個人は，十分気注意しなければならない。企業にとっては企業倫理を疑われたり信用を失うケースも少なくない。他人のネット取引情報を不正に取得して悪用した事例もある。

11） 情報処理推進機構（2014）『同上書』実教出版，p. 4．日頃からインターネットを利用し仕事に従事している者や個人は，上記の 10）と同様に IT の落とし穴である。2015 年のインターネットバンキングにおける不正送金事件など，近年のサイバー犯罪が急激に増えている。また，外部からの攻撃やマルウェアには十分な対策が必要である。

12） 情報処理推進機構（2014）『同上書』実教出版，p. 4．屋外での無線は，有線よりリスクが高い。無線の電波は放射状に拡がり受信する場所を探す。その間，第三者が受信し情報を取得する可能性がある。なりすましがそうである。対策としては，情報の暗号化が進められているが不十分である。

13） 情報処理推進機構（2014）『同上書』実教出版，pp. 18–19．上記の 11）と同様にサイバー犯罪の急増は，PC よりスマートフォンの利用が増えていることからサイバー空間は暗闇の世界である。特に，米国の国防総省は，サイバー空間のことを「第 5 の戦場」と呼んでいる。米国では，外国政府からのサイバー攻撃は「戦争行為」と見なすほど深刻な問題であり，その対策は重要かつ必要である。

参考文献

Byars, L.（1987）: Strategic Management, 2nd ed Harper & Row, p. 6.

Hatten, k.. and M, Hatten（1987）: Strategic Management, Prentice-Hall, p. 1.

H. Miyamoto, H. fukumuro, I. Nakajima, and K. Aoki.: Information Technolgy To Support Information Exchangesamong Asia-Pacific Region Countries, *A Journal of Information and Communication Research*, Vol. 8, No. 4, pp. 102–120（1991）.

Jauch, L. R., and W. F. Glueck（1988）: Business Policy And Strategic Management, 5th ed., McGraw-Hill, pp. 5–6.

Jauch, L. R., and W. F. Glueck, Business（1988）Policy and Strategic Management, 5th ed., McGraw-Hill,

pp. 5–6.
Kasai, K.（1992）: Symphonic-space, No. 7, pp. 37–38.
Kasai, K., and S. Kanayama（1990）: Symphonic-space, No. 5, pp. 14–15.
Koontz, H. and H. Weihrich（1988）: Manaqgement, 9th ed., McGraw-Hill, p. 63.
Koontz, H. and H. Weihrich（1988）: Manaqgement, 9th ed., McGraw-Hill, p. 104.
Ministry of International Trade and Industry, Machinery and Information Industries Bureau, Information, Computer, and Communications Policy Planning Office: Management Systems, *A Journal of Japan Industrial Management Associatio*n, Vol. 7, No. 1, 1997, p. 37.
M. Nagai. : Information Interdependence and Interchanges in Asis, *A Journal of Information and Communication Research*, Vol. 8, No. 4, pp. 6–9（1991）.
Newman, W. H., Warren, E. K., and J. E. Schnee（1982）: The Process of Management, 5th ed., Prentice-Hall, pp. 21–23.
岡田・松田編著（2001）「ケータイ学入門」有斐閣）。
拙稿（2006）「情報通信と情報技術の史的展開，経営経理研究」『経営経理研究』拓殖大学経営経理研究所，第 79 号，pp. 85–112。
拙稿（2005）「知覚に関する情報処理環境の変化と意識」PCUA。
窪田健一，金山茂雄（2009）「情報化と教育環境の影響分析」『教育システム情報学会講演論文集』pp. 494–495. 他。
佐藤義信（1988）「トヨタグループ戦略と実証分析」白桃書房，pp. 207–261。
手島茂樹他（2010）「世界同時不況下での生き残りをかけて」リプロ，pp. 1–30。
野村総合研究所技術調査部（1988）：日本電気研究開発グループ，R & D Hotline，ノムラ・リサーチ，野村総合研究所情報開発部。
野中郁次郎（1995）「企業進化論」日本経済新聞社，pp. 217–231。
原真（2004）「巨大メディアの逆説」リベルタ出版。
松岡公二，金山茂雄（2007）「技術と IT ビジネスの戦略的利用」『経営経理研究』拓殖大学経営経理研究所，第 80 号，pp. 129–156。
森岡清志（2004）「改訂版　都市社会の人間関係」放送大学教育振興会。
キャス・サンスティーン（2003）「インターネットは民主主義の敵か」毎日新聞社。
NHK 放送文化研究所編（2001）「現代日本人の意識構造 第六版」NHK 出版協会。
NHK 放送文化研究所編（1988）「現代日本人の意識構造 第六版」NHK 出版協会。
総務省（2015）「平成 27 年度版情報通信白書」総務省。
総務省（2015）「平成 26 年度版情報通信白書」総務省。
総務省（2013）「平成 25 年度版情報通信白書」総務省。

（原稿受付　2023 年 6 月 21 日）