# ICT社会の明るい将来を見つめて サイバー・セキュリティーをどう考えるか

奈良先端科学技術大学院大学　情報科学研究科　准教授　工学博士

**門林 雄基 氏**

**【プロフィール】**

大阪大学大型計算機センターを経て、2000 年より現職。2004 年から独立行政法人情報通信研究機構（NICT）の短期専攻研究員を兼務し、NICT の研究成果を一部標準化する形で、2008 年 から ITU-T（International Telecommunication Union Telecommunication Standardization Sector:国際電気通信連合の電気通信標準化部門）においてサイバー・セキュリティーの標準化に従事。インターネット工学をバックボーンにして、インターネットの上で形成されるコミュニケーション空間のサイバー・セキュリティーをいかに高めていくかを研究テーマとして取り組み、サイバー・セキュリティー教育や人材育成にも尽力している。
産学官の研究コンソーシアム「WIDE プロジェクト」のボード・メンバーであり、2011 年からは、ニュージーランドの Unitec Institute of Technology の客員教授も務める。

**インターネット人口は、従来とは比較にならないスケールで今後も増加し続け、サイバー・スペースの拡大はもはや止められない流れとなっています。現在では想像もできない新しいサービスや仕組みの登場に期待が膨らむ一方で、サイバー・スペースの将来を考える時、負の側面としてセキュリティーへの不安が常に付きまとうことは否めません。**

**今回インタビューで話を伺った奈良先端科学技術大学院大学 情報科学研究科 准教授の門林 雄基氏は、サイバー・スペースにおける人とシステムとのかかわり、人と人とのコミュニケーションを含めたサイバー・セキュリティーの課題を解決するための取り組みを、さまざまな方面からけん引しておられます。そして、セキュリティー脅威を十分認識した上で、正しい知識や能力を高め、前向きな発想でセキュリティーをとらえるべきだと強調されています。**

**また、国内はもとよりグローバルな取り組みにも参加されている門林氏は、世界市場における今後の日本の競争力を考えた場合にも、セキュリティーをブランド化してアピールすることが日本の強みにつながると主張されます。**

**本記事では、門林氏のインタビューを通じて、将来を見詰めて、サイバー・セキュリティーの課題にどう取り組むべきか、またIBMはどのような貢献ができるかを考えます。**

## 世界中で多様化・深刻化する犯罪とセキュリティー・デバイド

―― まず、サイバー・テロなどを含め、世界のサイバー・セキュリティーの現状について教えてください。

**門林氏**：日本のメディアでの報道内容だけではグローバルの現状を認識するのは難しいのですが、サイバー犯罪は途上国を中心として非常に多様化しています。例えば、ロシアや東欧では、一部のテレコム会社がマフィア的な地下経済とつながっていて、東ヨーロッパの国にかけた長距離電話の数十万にも上る通話料金をだまし取るといった犯罪が発生しており、これは日本にも被害が及んでいます。

Windows の不正コピーが横行している中国では、OS やアプリケーションも含めた不正コピー製品が非常に安価で販売されています。不正コピーはもちろん Windows アップデートが利用できないので、セキュリティー・パッチが当てられず、マルウェアがはびこっている状況にあります。

ブラジルでは、プロバイダーの DNS（Domain Name System）サーバーが攻撃されて、偽の検索サイトに接続してしまった契約ユーザーが、案内に従ってマルウェアをインストールしてしまうという事件も起きています。

こうした状況を受けて、国際社会においてもサイバー・

セキュリティーの重要性が認識され、情報通信分野で初めての国連サミットであるWSIS（World Summit on the Information Society：世界情報社会サミット）で2005年に決議された行動方針の中では、「ICT（Information and Communication Technology：以下、ICT）の利用における信頼性とセキュリティの確立」（アクション・ラインC5）の推進が求められています。また、ITUの4年に1度の総会であるWTSA（World Telecommunication Standardization Assembly）でもサイバー・セキュリティーの重要性が再認識され、2008年に新しい標準化などに関する決議がなされています。さらに今年1月に開催された世界経済フォーラム（World Economic Forum）の年次総会でも、「Global Risks 2012」の上位にサイバー攻撃が挙げられています。

日本では近年、マルウェアの感染率は低くなっています。これは総務省と経済産業省が推進する、インターネットを悪用するボットなどを解析して駆除方法などの情報を提供するサイバークリーンセンター（CCC）をはじめとする取り組みが功を奏したものでしょう。しかしながら、サイバー・セキュリティーの取り組みは、それだけでは十分ではありません。日本社会においては、日本は安全という過信があり、サイバー・スペースに関するリスク意識が低いために、昨今の標的型攻撃に代表されるサイバー攻撃が大きな問題へと発展したという事情があると思います。また、企業などで本格的にITが導入されてから、かなりの時代が経過しているため、Windows XPや旧バージョンのInternet Explorerなどの古い技術をベースに業務システムなどが動いているケースが多くあります。こうしたレガシー資産が多いのも、日本を含めた先進国に多く見られる問題です。

さらに、先進国に限らず、人々のセキュリティー・デバイド（Security Divide：セキュリティー格差）が問題となっています。セキュリティーに関する体系的な知識を持つ人があまりに少なく、大半は「セキュリティーは専門家が守るもの」という意識が強く根付いているのです。例えば、わたしたちは医師レベルの専門知識を持っていなくても、1日に30品目の食品をバランスよく食べた方が良いとか、カルシウムやタンパク質が不可欠であるとか、運動や睡眠が大切であるとか、健康に関するさまざまな知識を持っており、自分自身でも健康を守ろうとします。これと同様に、サイバー・セキュリティーについても、自分の安全はある程度は自分自身で担保するべきなのですが、Windows 95が世に出てすでに15年も経過し、インターネットがこれほど使われるようになっているにもかかわらず、セキュリティーに関しては知識が乏しく、当事者意識や自己責任意識が欠如しているという状況です。言い換えれば、サイバー・スペースの公衆衛生がなっていない状況なのです。

そして、ソフトウェアが高機能化や複合化を繰り返すに伴い、ブラックボックス化（隠ぺい）する傾向にあります。例えば、ブラウザー上でリンクや画像をクリックしなくてもマウスのカーソルを合わせればプログラムが起動する仕組みがありますが、このような技術の知識がないと、「クリックさえしなければ安全」と確信しながらマウスのカーソルを合わせてしまい、結果として被害に遭うことになりかねません。

## 直感に訴えるユーザー・インターフェースとリスク・コミュニケーション

―― こうした現状において、日本の企業は、今後どのようなセキュリティー課題に取り組むべきでしょうか。

**門林氏**：企業の場合も同様で、企業の安全は自社の責任においてしかるべき投資をして守るべきものですが、自己責任原則が欠如していると感じることが非常に多いです。極端な場合、ファイアウオールとアンチウイルス・ソフトを導入していればセキュリティー対策をしていると勘違いしているなど、脅威に対する認識も欠如しているようです。また、自分のパソコンにどのソフトウェアが入っているのかということすら認識していない人もいます。会社としても、自社にパソコンが何台あり、どのアプリケーション・ソフトウェアが使われて、部署ごとにどのようにポリシーを分けているかを即答できないなどICT資産管理能力が欠如している場合が多いのではないでしょうか。セキュリティーに関する知識レベルがこのように低いケースを「サイバー無知（cyber ignorance）」と呼ぶことがありますが、正しい技術的知識や脅威認識がないと、具体的なアクションにも結び付きません。

その背景には、リスク・コミュニケーションの問題もあります。例えば、セキュリティー専門組織などが出しているアプリケーション・ソフトウェアの脆弱（ぜいじゃく）性に関する警戒情報を見ると、難解な長い文章が続いていることがよくあります。これでは専門家以外はほとんど読まないでしょう。こうしたことが、セキュリティーの専門家とそうではない人との間でのリスクに関するコミュニケーションを阻害

し、セキュリティー・デバイドに、より拍車を掛ける結果になっています。

米国の情報工学分野の学会であるACM（Association for Computing Machinery）の学会誌に「サイバー・セキュリティーをわれわれの直感に結び付けることができなければ、対策はうまくいかないだろう」という主旨のことが書かれていたことがあります。自分のシステムや振る舞いが安全なのか危険なのかを、システムからユーザーにいかにフィードバックして直感的に分からせるかという視点が必要なのです。

例えば、古いバージョンのOSでも、ユーザー・インターフェースに違和感はなく、変わらず使えてしまうので、セキュリティー上問題があることを実感できません。またブラウザーについても同様で、古いバージョンであってもセキュリティー上の問題に気付かないまま使えてしまう場合があります。こうした問題を見た目で分かるように直感的にフィードバックする方法を研究する必要があると思います。

最新のソフトウェアにも改善の余地はあります。例えば電子メール・クライアントで、メールの背景が白く本文が黒い文字で、リンク先のURLの色が薄い青で表示されていると、フィッシング詐欺メールでの「:」が「=」になっているというような微妙な異常には気付きにくいということがあります。つまり、ユーザー・インターフェースにおいてセキュリティーに関する配慮が開発者側にも欠けているのではないでしょうか。このような研究開発は、IBMが率先して取り組んでいただけるものと期待しています。

## 予防対策に偏らず、事後対策の重要さにも注目を

―― 脅威認識を高めるために、セキュリティー・リスクを計量化する方法はありますか。

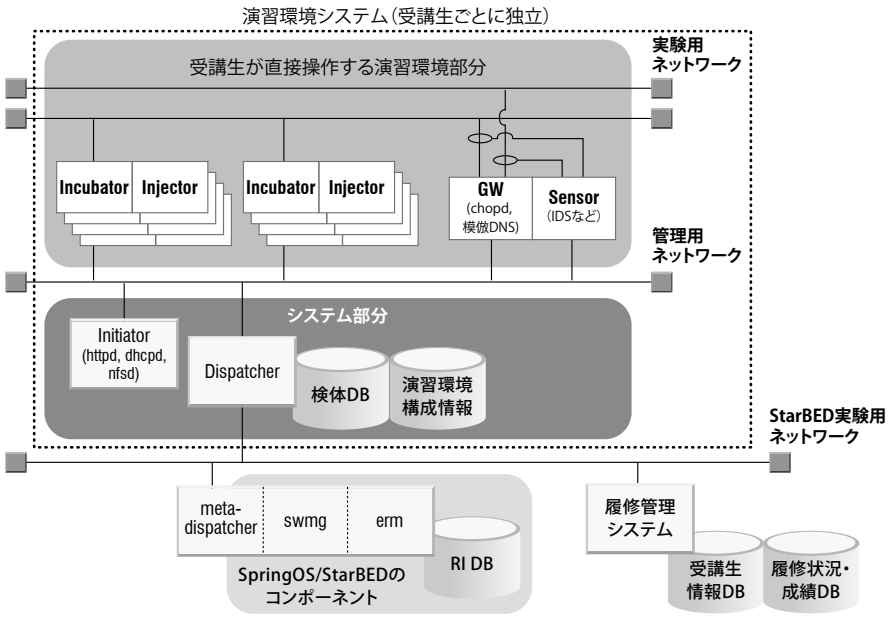
**門林氏**：脆弱性の深刻さや影響度などを数字で計量する標準として共通脆弱性評価システム（Common Vulnerability Scoring System：CVSS）という標準があり、わたしも国際標準化作業にかかわっています。1つ1つの脆弱性などのリスクを計量化できても、実際には、それらが複雑に組み合わされた犯罪や情報漏えいなどの問題が発生するので、まだ道半ばだと認識しています。これは今後、5年、10年と時間をかけて取り組むべき課題であり、リスクを計量化した結果が分かりやすく表示されるなど、前述の直感的な可視化の取り組みへとつながっていけばよいと考えています。

リスクが計量化されれば、企業にとってより適切なセキュリティー対策への投資が可能になると期待されます。しかし現時点では、ベンダー各社が提供する製品やソリューションは、予防対策に偏っていて、事後対策が少ないのではないでしょうか。既知のリスクや事象に対しては予防対策が有効ですが、未知の事象に関しては事後対策も必要になります。未知の事象が発生した時にどのような対策を施し、被るダメージをいかにコントロールするかというような視点でも、ソリューションを提供してほしいものです。

これまで挙げてきた課題を解決するための試みの1つとして、奈良先端科学技術大学院大学をはじめとする情報系の4大学院や企業・団体などの産官学が連携して開催している「IT Keys（IT specialist program to promote Key Engineers as securitY Specialists）」というプロジェクトがあります。IT Keysは、組織における情報セキュリティー問題に対して、主導的役割を果たすことのできる多面的・総合的能力とともに、経験に基づく知識と勘を兼ね備えた実践型人材の育成を目指しています。その教育コースの実験科目群でわたしが担当している「インシデント体験演習」では、マルウェア感染事案や情報漏えい事案などのインシデントを体験することにより、事前に何を準備し、事後に何をするべきかの両方を経験します。もし、事後対策の経験がなければ、実際のインシデント発生時にはパニックに陥り、何を調べればいいのかということすら分からない状態になりかねませんので、緊急時への備えとしてこのような演習が非常に重要だと考えています。

この演習は、完全隔離された200台近いコンピューターをプラットフォームとしたテストベッドに、3年分の検体から厳選した実際のマルウェアを使うという、スケールとリアリティーがある環境で行われます（**図1**）。1チーム10台で小規模なイントラネットを再現してさまざまな事案を演習します。90分の演習時間内に、インシデント発生から、インシデントへの対処・解析、Chief Information Officer（以下、CIO）やChief Security Officer（以下、CSO）などの経営者へのブリーフィング資料作成までを行います。ブリーフィングすることで、自分が理解していない点が明らかになり、影響範囲はどれだけでどれだけ深刻か、これを止めるにはどうすべきかなど、多様な視点が持てるようになります。

この演習は本物の火を使った大規模な防災訓練のようなもので、すでに5年続いており、毎年20数名の学




StarBED:独立行政法人 情報通信研究機構 北陸StarBED技術センターにある大規模なネットワーク実験環境の名称
SpringOS：StarBEDでのネットワーク実験をサポートするソフトウェア群
RI DB：Resource Information Database
swmg：switch manager
erm：experiment resource manager
IDS：Intrusion Detection System

**図1. IT Keys「インシデント体験演習」における演習用テストベッド構成**

生を育てています。受講生は卒業後、セキュリティー企業や団体の第一線で活躍しており、今後、この教育を受けた学生が、多様な一般企業に就職してCIOやCSOを補佐する立場で貢献してくれればと期待しています。また、このように事後対策も含めた教育が一般企業にも普及していくことが望ましいと考えます。

## サイバー・セキュリティーは複合科学 経営課題として投資コストを判断する

―― セキュリティー製品やソリューションを検討する際の評価軸にはどのようなものがありますか。また、セキュリティー・コストをどのように位置付けるべきでしょうか。

**門林氏**：セキュリティーに掛けるコストをいかに正当化するかが1つの課題ではあります。例えばデータセンターを価格だけで探すのであれば、いくらでも安いサービスがあるかもしれませんが、何千人、何万人といったユーザーを支えるインフラとして安心はできないかもしれません。

また、一言でセキュリティーといっても、情報漏えい防止、データ保護、システムの堅牢性（けんろう）などさまざまな複合要素から成っているので、セキュリティーを確保するためには、単体の製品やサービスで完結することはあり得ません。ですから、セキュリティーのそれぞれの要素をどの製品やサービスでカバーするかというバランス・チャートのようなものが必要かもしれません。栄養バランスを示すようなものです。それぞれの必要摂取量は、業種や業態によって異なります。BS（貸借対照表）やPL（損益計算書）の次に、ICTバランス・ポートフォリオの資料が続き、それが毎月役員会で提供されるようになれば、適切なマネジメントが期待できます。

従来は、セキュリティーはITの問題とされていましたが、サイバー・スペースは機械と人間の相互作用であり、サイバー・セキュリティー事件の実例をみると、システムのバグにとどまらず、政策ミス、判断ミス、認識ミスなど人間が起こすさまざまな要因が関係していることが分かります。従って、サイバー・スペースのセキュリティー課題は、コンピューター・サイエンスや情報科学の枠を超えて、認知科学や経営科学、パブリック・ポリシーなども巻き込んでいかなければ、総合的な問題解決にはつながらないのではないかと考えています。

パッチの適用率やウイルスの発生件数などはすでにダッシュボードなどで経営者に提供されていますが、今後は人的な要因も含めて複合的に解析されたセキュリティー対策状況を経営視点で見ることができる仕組みや機能が求められます。

また、セキュリティー・コストのとらえ方に関連して、わたしはセキュリティーを保険料率算定とリンクさせることを提唱しています。例えば、ファイアウオールなどのセキュリティー対策の有無や度合によって、情報漏えい保険の保険料率が変わるというもので、自動車保険であれば、自動車にエアバックを搭載しているかどうかで年間保険料が異なるのと同じイメージです。保険料率の算定はなかなか難しいとは思いますが、個人情報漏えい事故なども多発しており、情報セキュリティー資格保有者が何人いたか、認定審査を受けていたかどうかなど、プロセスや製品による対策の有無などについての調査も行われているので、そろそろ可能なのではないかと思います。また、

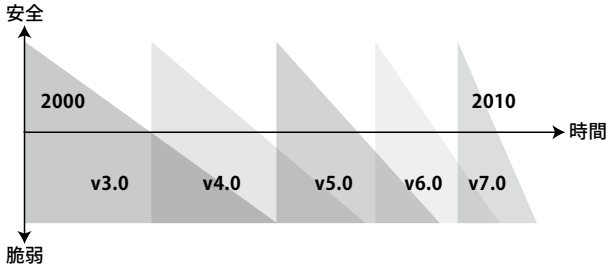
こうした事故調査がしっかり行われないと、社会的なリスクヘッジはなかなか進まないでしょう。

## ITのライフサイクル、開発形態などの変化を要因としたセキュリティー課題

―― ほかに、セキュリティーの課題がありましたらご提示ください。

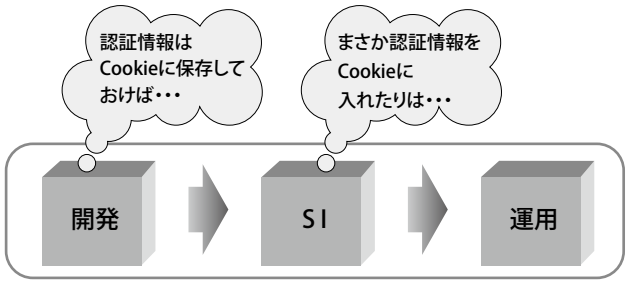
**門林氏**：ソフトウェアの脆弱性が見つけられるスピードが加速度的に上がっており、以前は、購入後1年間くらいは安全だったのが、今では1カ月くらいになり、プログラム修正が追いつかない状況になりつつあります（**図2**）。昨今は、サイバー・スペースの上に、さまざまな社会の仕組みや財産が載っている状態です。インターネット・バンキングのIDやパスワードを盗んだり、不正請求を仕掛けることで、莫大な金銭をだまし取ることができるので、犯罪者の真剣さとスピードもけた違いです。

ITの技術進化の速さがドッグイヤーなどといわれたことがあるように、サイバー・セキュリティーにおいても3カ月が1年に等しいくらいの感覚であり、従来は年に1回のセキュリティー監査で十分だったとしても、今ではまったく通用しません。これからは、リアルタイムに監視して




ソフトウェアの脆弱性が加速度的に増加し、プログラム修正で対処可能なスピードを超える危険性がある。

**図2. ゼロデイ攻撃リスクの増加**




SI: System Integration

コミュニケーション不足が脆弱性につながる。

**図3. 工程間のコミュニケーション・リスク**

いかないと、間に合わないのではないかという危惧すらあります。

また、ITシステムの開発、SI、運用が分業化される中、この工程間で的確かつ十分なコミュニケーションがないと、システムの脆弱性につながりかねません（**図3**）。特に、オフショアが盛んな昨今は、言葉の問題が意思疎通に少なからず支障を来す可能性があり、セキュリティー・リスクの確率も高まります。セキュリティー対策を設計・開発段階から盛り込んでくることを、これまで実施してこなかった企業が多いのが実情ですので、IBMにはグローバル企業の強みを生かしたソリューションを提供し、リードしてほしいと期待しています。

ちなみに、国際的な標準化の取り組みの1つとして、脆弱性やセキュリティーにかかわる事象を説明するための名前や用語を標準化し、各国語のディクショナリーを作成するCVE（Common Vulnerabilities and Exposures）というプロジェクトも進んでいます。これにより、脆弱性のデータベースやツールなどの共有が容易になり、一意の脆弱性認識番号をベースに、各国のディクショナリーやサイバー攻撃の詳細を調べることが可能になります。

ユーザー企業各社も、開発段階からしかるべきコストを掛けて、しかるべき対策を講じないと、取り返しのつかない重大なセキュリティー事故を引き起こすことになりかねないことを、経営者を含めて、十分理解していただきたいと考えます。運用してから問題が発覚すると、余計なコスト負担を強いられることにもなるので、できるだけ上流で押さえる方が結果的にコスト削減にもなるのです。

そして、コストと納期は企業にとって重要な要素ですので、セキュリティーも含めて3つのファクターをバランスよく考えるようにしたいものです。そして、IBMはじめベンダー各社には、バランスが良いソリューションを提供していただきたいと思います。

## ミッション・クリティカルな調達・構成・保守サービスの総合展開とサイバー・セキュリティー・コモンズの増進

―― セキュリティーの課題に関して、IBMに期待されることがありましたらお聞かせください。

**門林氏**：ミッション・クリティカル・サーバーと同様に、ミッション・クリティカルという概念は、アプリケーションやミドルウェア、ホスティング・サービスなどにも必要で、導入

時だけでなく、運用保守などの場面でも生きるはずです。例えば、SQL インジェクションで攻撃されてしまうことは、ミッション・クリティカルであるにもかかわらず必要なコストを掛けて十分に対策していないことが要因となっています。それぞれの企業にとって、何がミッション・クリティカルなのかを見極めた上で、総合的に信頼性の高い適切な提案をしていただきたいと期待しています。

また、セキュリティーに関しては、共有材、公共財が少ないのが現状です。IBM は、Linux、Eclipse や Java をはじめとするオープン・ソースのエコシステムにおいて中心的な役割を果たしており、セキュリティーに関しても、エコシステムの構築も含めて、同様の活躍を期待しています。IBM のセキュリティー研究開発機関である X-Force におけるナレッジ・ベースの公開や、セキュリティーに関する情報発信などに見られるような、ほかの企業の模範となるような取り組みをさらに増やしていただきたいと思います。

人材育成は次の世代につなげるという意味でも重要ですので、IBM の貢献にも期待しています。未来につながる取り組みとして、先にご紹介した IT Keys では、すでに 100 人以上を社会に送り出していますが、卒業生 1,000 人になるまで頑張りたいと思っています。

また、このほかに、世界の若者を対象とする技術コンペティション（CDMC：Cybersecurity Data Mining Competition）も実施しています。セキュリティーをはじめとする入り組んだ領域で能力を発揮できる優秀な若者を発掘することを目的としており、セキュリティーをテーマにしたものも継続的に実施しています。例えばスパムのデータ・セットをわれわれから提供し、これらを分析する優れたアルゴリズムを作った研究者を表彰しています。

コンペティションに参加するのは、データ・マイニングや画像認識などの分野で分析アルゴリズムを作ることができる優秀な若者たちです。コンペティションは、サイバー・セキュリティーという領域が社会にとって重要であり、今後活躍できる舞台がある、という若者に向けてのメッセージ発信でもあります。

サイバー・セキュリティーは、前述のように学問と学問が融合する総合科学で、生活の安全にも直結する重要な領域ですから、優秀な人にこそ取り組んでもらわなければならないのです。そのためにも、継続的な取り組みが必要であると認識しています。

## 前向きな発想でセキュリティーをとらえ世界に誇るセキュリティー立国を目指す

―― 最後にセキュリティーに関して、将来の展望をお願いします。

**門林氏**：インターネットは、人と人、人とシステムが相互作用するというサイバー・スペースとしてはまだ発展途上のインフラであるにもかかわらず、性能や機能の進化が早く、莫大な財産がインターネット上で扱われてしまっているというのが悩ましい現状です。

しかし、サイバー・スペースの拡大はもはや止められない流れです。中国、インドネシア、ブラジルなどにおいて、これまでの先進国とは比較にならないスケールで、億単位の人たちがインターネットを使い始めると予想されます。経済・サービスをはじめとする世の中の仕組みが、次々とサイバー・スペース上で展開され、想像を超えた新しい変化が起き、世の中が進歩するでしょう。そして、何ごとにも光と影があるもので、良いことばかりでなく、好ましくないことも起きるかもしれません。

しかし、過去を振り返ってみると、ICT の進歩は、膨大な利益を世の中にもたらし、もはや ICT がない世の中に戻ることはできないのです。ICT を生かして経済活動を展開しなければ、世界市場で生き残ることは不可能といっても過言ではなく、ICT 投資においてセキュリティー投資は必要不可欠なものです。

そして、几帳面であることが日本人のコア・コンピタンスであるので、セキュリティーの高さをブランドとして、世界市場に打って出ることもできるのではないかと思います。セキュリティー立国としての地位を確立し、日本人が運用しているからこそ、日本企業がやっているからこそ信頼できると、グローバルに認められれば、日本の製品やサービスは世界中でもっと使ってもらえる余地があると思います。

セキュリティーはとかく後ろ向きのイメージが付きまといますが、前向きな発想でとらえたいものです。企業や個人がセキュリティーの課題にしっかりと向き合っていくことが、ICT に支えられた明るい将来につながると思いますし、必ずそのような世の中が実現すると信じています。