サイバーセキュリティー強靭化へ 地政学リスクを見据えた政策と 企業経営者も徹底的な意識改革を

企業のDX推進委員会
委員長／伊藤 穣一・鈴木 国正

（インタビューは10月18日に実施）

サイバー攻撃は一段と巧妙化、高度化、複雑化、組織化が加速している。わが国は人手不足が顕在化する中で、企業がDXをさらに推進していく必要があり、そのためにもサイバーセキュリティーの強化が不可欠である。提言では、経営者が行動すべき八つのアクションと政府への六つの提言を示した。伊藤穣一・鈴木国正両委員長が語った。

サイバー攻撃というリスクの可視化 外部依存からの抜本的な意識改革

伊藤　日本のサイバーセキュリティーについては、サイバー攻撃を受けた際の報告義務や、サイバーセキュリティーを支える人材育成の体制、サイバーセキュリティーにかかわる企業数などさまざまな点で、欧米諸国と比較して明らかに後れを取っています。

また、日本社会全体でDXそのものが十分進展しているとは言えず、セキュリティーリスクが可視化しづらいという側面もあります。健康診断をしないと病気かどうか分からないのと同じように、まずはサイバー攻撃というリスクの可視化を行う必要があります。今それをようやく意識し始めたという段階かと思います。

鈴木　意識がまだ十分に高くないことは企業の体制にも表れています。例えばCISO（最高情報セキュリティー責任者）の設置割合は米国のトップ企業群「フォーチュン500」で約9割に達しているのに対し、日本の上場企業では4割程度です。

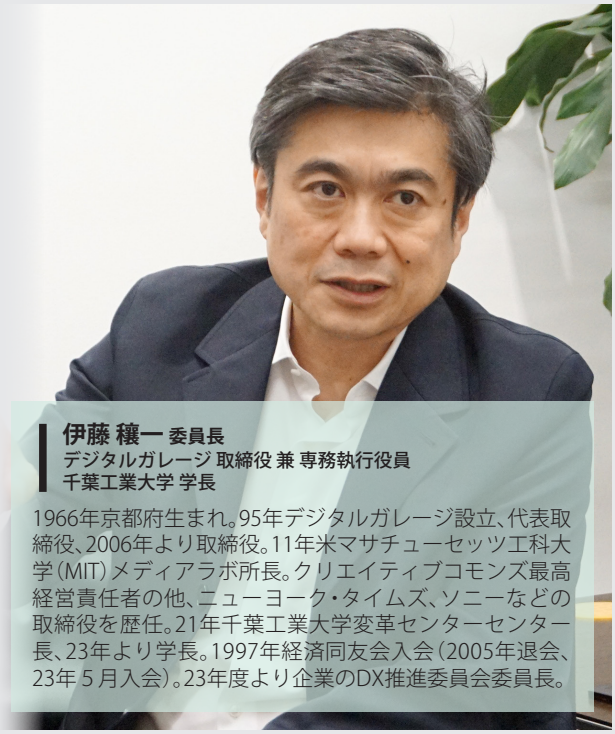
この背景にはIT化に対応した体制が多くの日本企業に備わっていなかったことが要因としてあります。経済産業省が2018年に発表した「DXレポート」では、DXが進展しない場合の経済損失「2025年の崖」が指摘されていました。そこではDXを阻む懸念として「企業が既存システムの保守・運用をベンダーに依存し過ぎていること」が挙げられており、この状態は現在も大きく変わっていません。自社人材やCIO（最高情報責任者）に情報システムのナレッジが蓄積されず、自社システムが抱えるリスクにも意識が及ばない中でサイバーセキュリティー、CISOを担う人材といった新たな課題にも取り組むためには、抜本的な意識改革が急務です。

サイバー攻撃の地政学リスクが すでに顕在化している

鈴木　DX推進と同時に、サイバー攻撃の対象となるアタックサーフェイス（攻撃対象領域）は確実に増加しています。それに比例するようにサイバー攻撃件数も年々増加傾向にあり、その中にデータを不正に暗号化して身代金を要求するランサムウェアも相当数含まれています。ランサムウェア攻撃に起因した情報漏えいによってサービス停止に追い込まれ、企業業績が悪化した企業もあります。ただし、こうした現状は表面化せず、非常に見えにくいという問題があります。

今回の提言に至った大きな背景の一つに、地政学リスクの高まりも挙げられます。ロシアによるウクライナ侵攻においては、武力攻撃に至る前からウクライナの重要な情報システムにサイバー攻撃が仕掛けられていたことが知られています。日本でも近隣諸国からのサイバー攻撃に見舞われており、日本企業にとっても看過できないリスクとなっています。

伊藤　こうしたサイバー攻撃を一つの組織ではなく分業化して行う「サイバー犯罪エコシステム」が成熟化しており、国家ぐるみでこうしたシステムを構築しているケースもあります。また、AIの進化もサイバー攻撃の複雑化を一層加速させているのです。さらに近年の生成AIの登場によりWormGPTなどサイバー攻撃における新たなツールも出現しています。攻撃の高度化に対処するため、セキュリティー側でもAIの活用を含めた高度化が図られていますが、日本では専門の技術者や企業がまったく足りていません。縦割り行政では、AI分野とセキュリティー分野がリンク



伊藤 穣一 委員長
デジタルガレージ 取締役 兼 専務執行役員
千葉工業大学 学長

1966年京都府生まれ。95年デジタルガレージ設立、代表取締役、2006年より取締役。11年米マサチューセッツ工科大学（MIT）メディアラボ所長。クリエイティブコモンズ最高経営責任者の他、ニューヨーク・タイムズ、ソニーなどの取締役を歴任。21年千葉工業大学変革センターセンター長、23年より学長。1997年経済同友会入会（2005年退会、23年５月入会）。23年度より企業のDX推進委員会委員長。

鈴木 国正 委員長
インテル 取締役会長

1960年神奈川県生まれ。84年横浜国立大学卒業後、同年ソニー入社。VAIO事業本部長、ソニー・コンピュータエンタテインメント副社長、ソニーモバイルコミュニケーションズ社長兼CEOなどを歴任。2018年インテル取締役社長、24年取締役会長。2018年12月経済同友会入会。22年度経済安全保障・科学技術委員会副委員長、23年度より企業のDX推進委員会委員長。

して高度化を図る体制が整備しにくいのも問題です。

企業の課題は「予算の孤立化」シナリオとコスト管理を同時に

鈴木　提言では、経営トップが取り組むべき三つの課題として、常時有事対応への体制づくり、ガバナンス強化、人材育成・獲得を挙げました。そしてこれらの課題を克服するために、経営者が取り組むべき八つのアクションを提示しました。

その中の一つの課題は「予算をどう組むか」「ROI（投資利益率）はどのくらいか」という点です。多くの経営課題には何かしらの数値化された指標が存在し、それを基にどの程度の投資でどれだけリターンを得られるかという経営判断を行います。ところが、サイバーセキュリティーに関してはリスクを想定するための数値化された材料が乏しいため、その判断が難しいのです。すると、最終的には経営者がいかにリスクを想定しながら意思決定を行うかが大きな鍵となります。そして次にCISOを含めた体制強化が重要となるのではないでしょうか。

伊藤　まず、シナリオプランニングが必要だと思います。自社のサービス停止はどのような攻撃を受けたときに起こり得るのか、コストはどれだけかかるのか、攻撃に対して誰がどのような決定をして対処するのか、これらを事前に想定することはできるでしょう。

サービスが全停止して企業の存続自体が危うくなるリスクについては役員会で事前に想定を行い、対応方針を固めておくべきです。過去のデータが少ない点で地震など自然災害への備えとは異なりますが、考え方は同じだと思います。例えば、経済同友会のような場でベストプラクティスを共有していくことが有用ではないでしょうか。

他方で、きめ細やかなサイバーセキュリティーをどこまで詰めるか、経営判断も求められます。例えば、記録を暗号化することでカード番号などの個人情報を保管せずにデータベース化するテクノロジーやアーキテクチャーが存在します。システムのアップデートにどれだけ投資するかはコスト管理の問題とも言うことができ、個々の経営判断に委ねられています。

破滅的な危機に備えるシナリオプランニングと、危機を未然に防ぐためのコスト管理を分けて、同時並行で進めていく姿勢が大切なのではないかと考えています。

他国と同様のスタンダード水準に人材は社会全体で醸成

鈴木　国のサイバーセキュリティー対策として政府が取り組むべきことについて、提言では６点掲げています。まずは未然に攻撃を防ぐ能動的サイバー防御が重要であり、早期導入をすべきです。また、省庁間の壁を越えた、あるいは官民連携による議論の場を設けることが重要だという点です。NISC（内閣サイバーセキュリティセンター）に官民連携組織を創設し、司令塔機能を強化するのもその一つです。その上で、重要インフラ事業者へのサイバー攻撃の報告義務化、サイバーセキュリティーに関する重要情報の有価証券報告書への記載など情報開示についても踏み込みました。

伊藤　提言に掲げている各項目は国際的にはスタンダードな水準です。日本も少なくともそこまでは引き上げていくべきです。他国では初等中等教育から大学まで、サイバーセキュリティー教育に手厚く投資しています。日本もキャッチアップしていかなくてはなり

ません。

その際、必ずしもトップ人材だけを育てるということではなく、各企業の現場でしっかり働く人材を育成し、数を増やしていくことが重要だと思います。例えば、米国にはサイバーセキュリティー人材を重点的に育成する地方大学があり、オーストラリアにはサイバーアカデミーという専門大学もあります。サイバーセキュリティーを学べば就職や収入増にもつながる、インセンティブを社会全体で醸成していくことも求められています。

まずはこの提言を読んでいただき意見や情報などフィードバックを

鈴木　経済同友会の経営者の皆さまには、まずはこの提言を読んで、ぜひ役員会や社内でディスカッションをしていただきたいと思います。インパクトのある内容だと自負していますし、サイバーセキュリティーに対する意識向上に寄与できるものと確信しています。今回の提言は主として大企業向けのメッセージとなりましたが、中小企業のセキュリティーという課題もあります。特に電力などのインフラ分野では、地方の中堅中小企業がセキュリティー上重要なデータを多く取り扱っていることが想定されます。意見交換を通じて解決すべき課題を検討し、連携して日本企業全体のセキュリティーを高めていければと思います。

伊藤　提言内容に対するフィードバックもぜひいただければと思います。特にサイバー攻撃の報告義務や有価証券報告書への記載義務などは、規制する側の政府と現場の企業側で見解も異なるでしょうし、より詳細を詰めていく必要がある部分だと感じています。セキュリティーリスクのような問題は社外で話すのが難しいクローズドな話題ですが、だからこそ経済同友会のような経営者のプラットフォームでの意見交換が有益です。「私たちの業界ではこういう問題が起きている」といった情報をぜひお寄せください。

提言概要（10月23日発表）

「Cyber Security Everywhere」時代
～経営者の８つのアクションと政府への６つの提言～

ウクライナ危機では、武力攻撃に先行してサイバー攻撃が行われ、その手口は一段と巧妙化、高度化しており、複雑かつ組織的になっている。一方で、国内では慢性的な人手不足・人材不足が顕在化し、グローバルな経済の中で企業がDXをさらに推進するため、サイバーセキュリティーの強化が不可欠である。

そこで今回は“Cyber Security Everywhere”の時代に突入したという認識の下、経営者が行動すべき八つのアクションと政府が進めるべき六つの提言を示した。

本会は業界や個々の企業が連携し、経営者が集団としてサイバーセキュリティーを強化することを支援していくことで“Cyber Security Everywhere”の時代を生き抜き、企業が持続的に成長できるよう、取り組みを一層加速させていく。

Ⅰ　経営者が行動すべき八つのアクション

【提言１】サイバーセキュリティーを成長ドライバーへ

サイバーセキュリティーを経営の重要課題とし、サイバーセキュリティーを成長ドライバーとして位置付け、守りの対策から攻めの戦略へ

【提言２】体制強化

CISO(最高情報セキュリティー責任者)を設置し、取締役や役員クラスに任命

【提言３】専門性のある取締役による議論とモニタリング

能動的に質問できる専門性のある取締役人材を配置。取締役会での議論、執行側に対してサイバーセキュリティー対応について定期的にモニタリング・改善する体制を

【提言４】リスクの見える化・数値化

自社のアセットを見える化、管理するとともに、被害リスクを数値化し、事業の影響度を把握

【提言５】リスク対応計画策定

あらかじめ有事に備えたリスク対応計画策定をすべき。優先順位やリスクの影響度を鑑みて、複数のプランを策定

【提言６】予算の独立化

IT予算とサイバーセキュリティー予算を独立させ、中長期的な投資を

【提言７】人材の定義化

サイバーセキュリティーの人材の役割、知識およびスキルなどの定義

【提言８】人材育成・獲得

「シン・日本型雇用システム」導入など制度や報酬体系を整えるとともに、人材の獲得や人材育成の実践を強化

Ⅱ　政府への六つの提言

【提言１】能動的サイバー防御・NISCの司令塔機能強化

安全保障や重大なサイバー攻撃の恐れのある場合、能動的サイバー防御を早期に導入、NISC(内閣サイバーセキュリティセンター)の司令塔機能強化

【提言２】重要インフラ事業者への報告義務化・新たな官民連携組織の創設

重要インフラ事業者への報告義務化を早期に導入。NISC内に新たな官民連携の組織体創設、定期的な会合、官民の人材交流など信頼関係の構築、一元化・統一化・効率化の徹底

【提言３】人材育成

人材定義の可視化、教育機関の質と量の拡充

【提言４】情報開示

サイバーセキュリティーに関する重要情報の有価証券報告書への記載義務を検討すべき

【提言５】サイバーセキュリティー産業の振興

高品質な国産セキュリティー製品およびサービス供給を強化、耐量子計算機暗号への対応

【提言６】サイバー保険

政府主導でデータ集約、分析、ルール作りをして、サイバー保険によるリスク評価の枠組みとしての選択肢を作る

詳しくはコチラ