Client Newsletter from
PwC Japan Group

Value Talk

三角 育生 氏

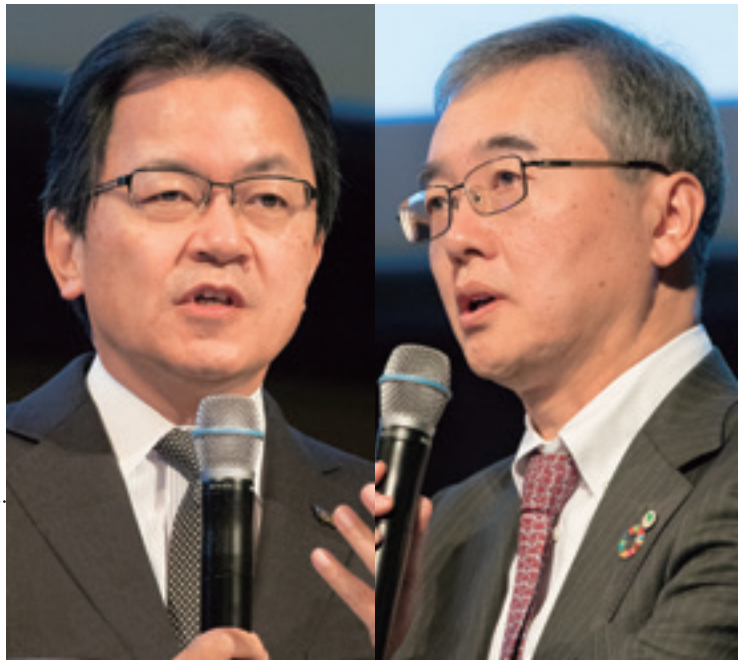
経済産業省サイバーセキュリティ・情報化審議官
内閣官房内閣サイバーセキュリティセンター
内閣官房情報通信技術（IT）
総合戦略室長代理（副政府 CIO）
内閣審議官

Value Navigator

2019 Winter

特集

経営戦略としての サイバーセキュリティ



Value Interview

宮部 義幸 氏
パナソニック株式会社
専務執行役員 CTO・CIO

小島 啓二 氏
株式会社日立製作所
代表執行役 執行役副社長 CISO

pwc

www.pwc.com/jp

Season's Report from Global

グローバルに広がるPwCの活動を現地オフィスからレポートします。

サイバーリスクには、取締役レベルの関与を ── 米国

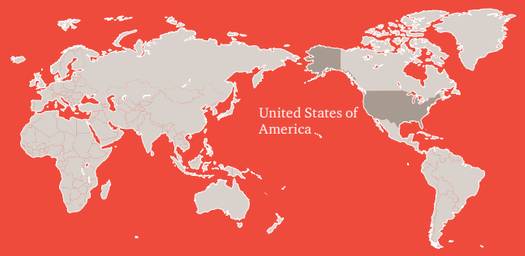
米国企業の取締役は、研修に限らず他の取締役との会話やサイバー事件に関するニュースから情報を得ることで「サイバーIQ」を上げています。これにより、組織における取締役のサイバーリスクに対する監督力を強化しているのです。また独立した社外取締役は、サイバーセキュリティなどの重要なリスクについての議論を、経営陣とも積極的に行っています。

多くの米国企業は、サイバーリスクに関する調査や、リスクを把握するための主なトレンドや指標を四半期ごとに更新するなど、最新の情報を取締役会へ定期的に報告しています。例えば、CISOやCIOなどのエグゼクティブが取締役会に報告し、次のような質問に回答しています。

・当社が直面している主なサイバーリスクは何か。
・そのリスクに対応するための施策は何か。
・その施策の有効性をどのように確認するのか。
・当社は、当社に適用されるサイバー法およびプライバシー法に準拠しているのか。

2018年には、JPX日経400の40％以上の企業において独立社外取締役が全取締役の3分の1を超えましたが、そうした企業の割合は2014年にはわずか6％でした※。日本企業では社外取締役の数が増えており、管理職はサイバーセキュリティに関する取締役会からの質問に対応する必要があります。日本企業でも、サイバーリスク対策に関する取締役会への教育を始めるのが望ましいと言えるでしょう。

※ 英語版：https://www.jpx.co.jp/english/listing/others/ind-executive/index.html
日本語版：https://www.jpx.co.jp/news/1020/20180731-02.html



特派員

ジョー・ダブス Joe Dubbs
PwC 米国シアトル事務所 サイバーセキュリティ ディレクター
（2016年7月から2018年6月まで日本へ赴任）

CONTENTS

Client Newsletter from PwC Japan Group
Value Navigator
2019 Winter

Value Navigator 2019年2月発行
企画・編集：PwC Japan グループ　発行人：北川 麻里
〒100-0004 東京都千代田区大手町 1-1-1 大手町パークビルディング
Tel. 03-6212-6810　www.pwc.com/jp
本誌についてのお問い合わせは、PwC Japan マーケット部までお願いします。
Email：pwcjppr@jp.pwc.com
制作：株式会社 ビーク・ワン

PwC Japan グループのご紹介
PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界158カ国に及ぶグローバルネットワークに250,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.com をご覧ください。

Value Navigator（バリューナビゲーター）
本誌では、PwCのグローバルに広がるプロフェッショナルネットワークを生かし、現場から得られる最新のビジネス情報やグローバルのナレッジ情報をご紹介します。 本誌がクライアント企業の皆様の価値創造を導く一助となることを願い、この誌名に表現しました。

特集

経営戦略としてのサイバーセキュリティ

あらゆる産業や経済活動、社会インフラにおいて、AIをはじめとするデジタル技術が世界規模で浸透していく動きが2020年代に向けてさらに加速していく。同時にサイバー攻撃に起因するリスクも増大しており、より踏み込んだサイバーセキュリティ対策が急務であるが、その対策に自信があると回答した企業の割合は世界では74%に上るのに対し、日本ではわずか38%にすぎないのが現実だ。データ利用のガバナンスに関しても、世界の多くの企業で十分な経験がない状況にある。取り組みが十分でなければ、ステークホルダーからの信頼（Trust）を失って企業価値を損ねかねないサイバーセキュリティは、いまや経営戦略としても大きな課題だ。サイバー空間と実世界の安全を確保し日本企業のさらなる成長を目指すには、どのような視点が必要となるのか――2年連続でグローバルでサイバーセキュリティ・コンサルティング・リーダーに選出※1されたPwCのエキスパートと、経済産業省 三角育夫氏との対談や、日本を代表する製造業であるパナソニック株式会社宮部義幸氏と株式会社日立製作所小島啓二氏が登壇したサイバーセキュリティの国際会議「サイバー・イニシアチブ東京 2018」での議論を通じて、探っていく。

PwCが協賛した「サイバー・イニシアチブ東京 2018」の様子
（2018年12月11日）

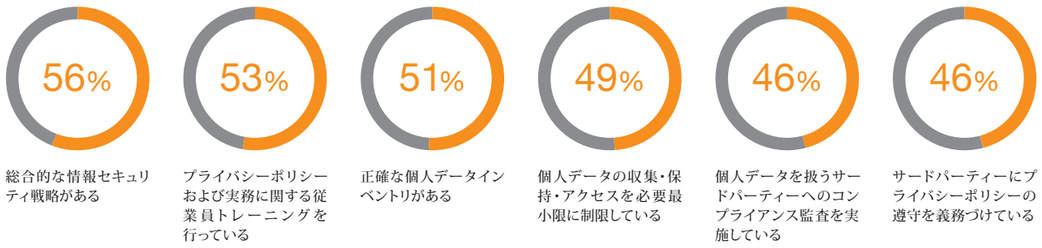
38%

サイバーセキュリティ対策に自信があると回答する日本の企業

出典：PwC「グローバル情報セキュリティ調査 2018」※2

多くの企業はまだデータ利用に対するガバナンスの経験が浅い

重要な対策を講じているとの回答者は約半数に留まる



出典：PwC「グローバル情報セキュリティ調査 2018」※3（回答者＝122カ国9,500人の経営幹部）

※1：https://www.pwc.com/jp/ja/press-room/leader-in-cybersecurity181023.html
Source: The *ALM Vanguard:* Cybersecurity Consulting, ALM Intelligence
※2：https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/strengthening-digital-society-against-cyber-shocks.pdf
※3：https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/privacy-and-trust.pdf

Value Talk

三角 育生 氏

Ikuo Misumi

経済産業省サイバーセキュリティ・情報化審議官
内閣官房内閣サイバーセキュリティセンター
内閣官房情報通信技術（IT）
総合戦略室長代理（副政府CIO）
内閣審議官

対談

鹿島 章

Akira Kashima

PwC Japan グループマネージングパートナー
PwCコンサルティング合同会社
代表執行役会長
JCIC（一般社団法人 日本サイバーセキュリティ・イノベーション委員会）理事

三角 育生

1987年通商産業省（現経済産業省）入省。2007年経済産業省 商務情報政策局 情報セキュリティ政策室長、2009年経済産業省 貿易経済協力局 貿易管理部安全保障貿易審査課長などを経て、2018年8月より現職。

鹿島 章

1985年大手監査法人に入所、さまざまな業種の監査業務に携わる。1995年会計事務所系コンサルティング部門に移籍。米国駐在を経て幅広いコンサルティング業務に従事。2016年にPwC Japan グループマネージングパートナー就任。

「Society 5.0」の本質と新たに生じてくる脅威とは

鹿島　近年の大きなキーワードとして、「Society 5.0」※が挙げられていますね。その実現に向けた過程に立ちはだかるサイバーセキュリティ上の脅威として、どのようなものが考えられるでしょうか。

三角　そもそもSociety 5.0というのは、狩猟社会、農耕社会、工業社会、情報社会に続く新しい社会の形――つまり情報社会から次のフェーズへと移行して“ポスト情報社会”となったときに大変革が起きるという未来予測が根底にあると考えています。コンピュータの歴史を振り返っても、単に単独で存在してプログラムを処理するだけの時代があり、その後にネットワーク化されて情報社会がつくり上げられたわけです。ではその次にどのような変化が起きるのかと言えば、最も影響が大きいのがIoT（Internet of Things）の進展であると見ています。IoTは既に指数関数的な勢いで広がっていますが、そうなると従来はバラバラに設置されたアナログな存

※内閣府が提唱している、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより経済発展と社会的課題の解決を両立する、人間中心の新たな社会の形。

在だったモノが、データ化・ネットワーク化されてつながり、IoTによってやがて自動化されていくのです。このように、全ての人とモノがネットワークされて多様な知識や情報が共有されることで、今までにない新たな価値が生み出されていくことでしょう。

鹿島　それこそが、サイバー空間とフィジカル空間が一体化してくるというSociety 5.0の本質であるわけですね。

三角　ええ。ただし、ここでサイバーセキュリティの話になるのですが、Society 5.0の時代になると人もモノも全てがつながるため、最も弱いところが攻撃者から狙われることになります。攻撃側からしても、テクノロジーの発展は攻撃の機会の増加を招くわけです。それともう一つ、データが本当に信用できるのかという点も大きな問題となるでしょう。既に多種多様なデータ形式がバラバラに存在していて玉石混交の状態なので、どこかで正規化する作業が必要です。しかし、その作業内容が信用できるのか、データを処理するAIが信用できるのかなどといった今まではあまり考慮しなかったような問題が生まれ、それが脅威となってくると考えられます。

もっとも、これは暗い側面だけの話ではありません。要はテクノロジーがとにかく進展して全く新しい社会となるわけなので、その飛躍をうまく活用すれば企業は大きな成長のチャンスをつかめるはずなのですから。ぜひ多くの日本企業にこの機を捉えてほしいと願っています。もちろん、激しい時代の変化には新たなリスクも伴いますので、そうした不確定な要素が良い方向にも悪い方向にもこれから大きくなっていくような時代に入るのだとまずは認識することが鍵ではないでしょうか。

信頼性の保証がセキュリティの新たなテーマに

鹿島　お話を伺って強く感じたのが、攻撃者のリスクはもちろんですが、データそのものであったり、データを加工・処理する人やプロセスなども含めて信頼を確保する仕組みが求められてくる――これは現状のサイバーセキュリティとはまた少し別の観点からのアプローチも必要になってくるのではないかということです。

三角　私も全く同じように考えていて、サイバーセキュリティの定義そのものが変わるのではないかと見ています。今はサイバーセキュリティの観点から、情報システムの機密性、完全性、可用性の議論がなされていますが、これはISOなどの認証制度の考え方とも合致しています。もしも信頼性が損なわれて社会的混乱が起きてしまったときに、セキュリティの問題として捉えるのか、信用失墜の問題として捉えるのか、入り組んでいて分からなくなってきていると言えるでしょう。この点については、今後の社会的な受容と認識によって変化してくる課題ではないでしょうか。

鹿島　PwCは財務諸表の監査も行っているので、ある意味で数字を作るプロセスに対して信用を提供しているのだと言えます。そのことについてグローバルでさまざまな議論を繰り広げていると、まさにいま言われたような点――例えばデータを扱うプロセスで間違いが起きないように保証する必要性などが重要課題として挙げられます。

三角　おっしゃるとおり、現実空間にある社会というのは、契約、法律、監査によって保証されています。一方でサイバー空間の場合はと言えば、従来は機密性、完全性、可用性で保証されることになるので、一般的なセキュリティ対策を行えばいいということでした。しかし、今後はそうした話とは少し様相が異なってきて、そもそも“それ”が正常な状態であるかという信用の話もサイバーセキュリティの範疇に入ってくるわけです。例えば電子商取引で認証が行われたとしたら、それが正しいプロセスによる認証であったかどうかもセキュリティマターとなるでしょう。つまり、信頼性、可用性、安全性、完全性が保たれているかどうかに関して、サイバーかフィジカルかではなく全体で見ていくことが必要となってくるわけです。

鹿島　いかに社会全体で信頼性を誰が保証するか、そこがポイントになってきそうですね。

三角　まさにそう思います。

セキュリティはコストではなく投資――経営層には意識改革を

鹿島　2018年7月に新たな「サイバーセキュリティ戦略」が閣議決定されましたが、その内容を踏まえて企業に期待するのはどのようなことでしょうか。

三角　端的に言うと、コーポレートミッションの中でセキュリティも考えるということです。自社のミッションがどこにあり、情報システムやICTは自社のコアコンピタンスにどのように関わってきて、それがステークホルダーにどういった影響をもたらすのか――まずはここからアプローチすべきでしょう。でなければ、セキュリティの確保そのものが目的となってしまいます。

鹿島　どの水準までセキュリティ対策をすればいいのか、日本の企業社会の間でレベルセットがきちんとできていないようにも感じます。

三角　そのとおりです。やはりまずは組織としてのコアコンピタンスであり、価値がどこにあるのかを決めておかないと答えは出ないでしょう。方法論としてはISMS（情報セキュリティマネジメントシステム）などがありますが、どこまでやるかは企業ごとに異なり横並びなどあり得ないはずです。リスクを100％払拭することなど不可能ですから、その時点で守るべきところと、予測可能な脅威とのバランスを取っていくことが重要です。

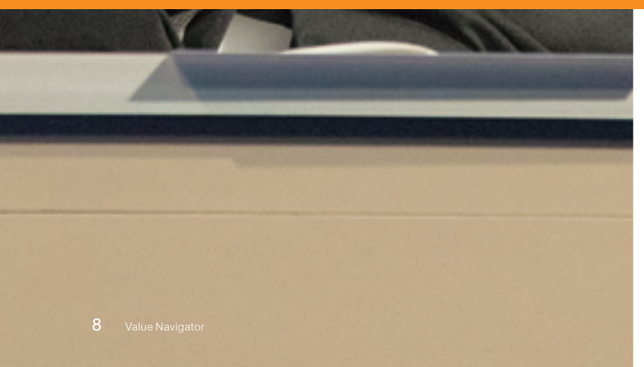
鹿島　ビジネス戦略とも密接に関係してくるように思えますね。

三角　本来はそうあるべきなのですが、そこまでになると少々時間を要してしまうので、まずは経営層の意識改革が求められてくると思います。そのため経済産業省が示している「サイバーセキュリティ経営ガイドライン」では、セキュリティ対策において経営層が責任を持ってリーダーシップを発揮すべきとしています。

さらに経営者の意識について言えば、サイバーセキュリティはどうしてもネガティブなベクトルで考えてコスト負担だとばかり捉えがちですが、本来はプラスとマイナスの両面から考えるものだと認識を改めるべきではないでしょうか。技術戦略があってICTを活用していくとなれば、ICTというのはまさに利益を生み出す道具です。例えば経営者が運転手だとすれば、車を速く安全に動かす――つまり利益を生み出すには、アクセルとブレーキを上手に使いこなす必要があるはずです。にもかかわらず、ブレーキもしくはセキュリティだけを切り出してコストを考えてしまったのでは、マイナスしか見えてこないでしょう。つまり、セキュリティもまたコストではなく投資だと捉えられるよう、経営層には意識変革が必要だと考えます。

鹿島　セキュリティも含めて、ICTを活用して企業に利益を生み出すことが大事であるという意識をまずは経営層が持ち、そうしたカルチャーが企業内で培われていくことが日本企業にも必要ですね。日本は、お客様の品質に対する要求が世界一厳しいと言われています。製品・サービスのセキュリティの品質を担保することも要求されており、それに対する答えを出していこうという意識も強いです。その点を、日本は強みとして生かしていくこともできるでしょう。ありがとうございました。

専門技術だけでなく、経営者としての目線を備えたセキュリティ人材の育成が不可欠



いまやサイバーセキュリティは組織が信頼を構築していくにあたって不可欠であり、経営者が先頭に立って取り組むべき重要課題となっている。サイバーセキュリティの国際会議「サイバー・イニシアチブ東京2018」では、日本を代表するメーカーである、パナソニック株式会社 専務執行役員 CTO・CIO 宮部義幸氏と株式会社日立製作所 代表執行役 執行役副社長 CISO 小島啓二氏が登壇。「Trust（信頼）の構築 ― 経営者アジェンダとしてのサイバーセキュリティ」をテーマに、PwCコンサルティング合同会社 パートナー サイバーセキュリティ・アンド・プライバシー・リーダー 山本直樹がモデレーターとして話を聞いた。

グローバル時代に求められるセキュリティガバナンス

山本　まず、日本を代表する企業であるパナソニック、日立製作所のお二人へ「グローバル企業におけるセキュリティガバナンス」についてお伺いしたいと思います。両社ともに国や地域を越えて複合的な事業を運営されていますが、グローバルを通じたセキュリティガバナンスの適用にはどのように取り組んでいるのでしょうか。

宮部　パナソニックでは、従来から三つのラインに基づいたセキュリティガバナンスを推進しています。一つが企業内の情報システムという軸でのガバナンスで、日常的に活用しているITに関するものです。二つ目が、モノづくりにおけるガバナンスです。当社は日本、中国、アジア、欧州、南米と世界各国に多くの工場を構えていますが、そうした生産拠点のネットワーク化が急激に進む中、工場のセキュリティにもしっかりと対応していかなければなりません。そして、三つ目が製品自体のガバナンスです。近年、多くの製品がネットワークに接続されて、そうした製品に対するセキュリティが重要な課題となっています。このラインについて、情報システムはCIO（Chief Information Officer）、モノづくりはCMO（Chief Manufacturing Officer）、製品はCQO（Chief Quality Officer）が責任を持っており、現在はこの三つの役職を私が兼務していますが、部門横断的な人材交流や情報共有レベルの向上といったメリットがあります。

小島　日立製作所では幅広くIT事業を手掛けていますが、2017年5月、ランサムウェアの「WannaCry」に感染するというセキュリティインシデントが発生しました。感染源は欧州にあるグループ会社の顕微鏡で、そうした検査機器から感染が一気に広がることは想定外だったわけです。私たちはM&Aも含めて企業規模を拡大し続けていますが、グローバルの規模でも、多様な種類の機器があるという意味でも、アタックサーフェス（攻撃領域）もどんどん拡大していることを、このインシデントを通じて改めて実感しました。そうしたことから、グローバルでのセキュリティガバナンスについて一から見直しを図っているのです。これも、CISO（Chief Information Security Officer）としての重要なミッションの一つと考えています。

山本　WannaCryの感染に対して、インシデントレスポンスという点ではどのような対応を行ったのですか。

小島　感染後、即座にレスポンスチームを設置したことで適切な対応ができ

宮部 義幸 氏
Yoshiyuki Miyabe
パナソニック株式会社
専務執行役員 CTO・CIO

小島 啓二 氏
Keiji Kojima
株式会社日立製作所
代表執行役 執行役副社長 CISO

宮部 義幸

1983年、松下電器産業（株）（現パナソニック（株））に入社。2008年に役員に就任。2011年常務取締役 技術担当、2013年AVCネットワークス社社長、2014年代表取締役専務。2015年4月より技術・知的財産・モノづくり総括・調達を担当。2016年4月より技術・モノづくり・調達・IT革新総括を担当。2017年6月より現職。

小島 啓二

1980年に京都大学大学院で数学を修めた後、コンピュータアーキテクチャーの研究者として中央研究所に入所。1996年からの4年間、米国にある「Hitachi Computer Products America」で勤務した。2014年からは日立グループのCTOと研究開発部門のCEOを務めた。2018年より現職。

ました。その後レビューを行ったところ、ネットワークの設計を含めてグローバルのセキュリティ機関から警告を受けていたことも分かったんですね。そうした事前防衛策を子会社まで行き渡らせることができなかった、つまり、全社を通じたガバナンスの適用がまだまだ不足していたわけです。今回の経験により、情報公開の重要性と、拡大し続けるアタックサーフェスを一社だけで防御するのは困難であると感じました。他の企業をはじめ、政府機関や現地の機関といかに協力体制を築いていくかが重要になると考えています。

山本　グローバルガバナンスの適用に苦労している企業は多く、日本の本社側セキュリティ部門を立ち上げて対策を講じても、海外では手付かずのケースが少なくありません。グローバルでのセキュリティガバナンスの適用は国際的に事業を展開する企業にとって欠かせないものであり、綿密に計画を立てて確実に実行していく必要がありますね。

セキュリティ品質も日本製品の強みに

山本　日本製品は品質の高さに定評がありますが、近年では品質を評価する項目の一つにセキュリティも挙げられています。製造業の立場から、製品やサービスの品質としてのサイバーセキュリティをどのように捉えられていますか。

小島　私どもの製品やサービスには重要な社会インフラに関わるようなものがありますが、品質を考えた場合、大きな評価軸の一つに「実績」があると考えています。とはいえ、実績だけでは評価が困難なこともあります。そこで、設計や品質保証のプロセスを投入するとともに、情報を広く公開していくことが重要だと考えています。これはなかなか勇気のいることなのですが、これをやっていかなければ信頼は実現できません。長い目で見れば、積極的な情報公開は信頼につながっていくと考えており、WannaCryに感染した時も広く情報を公開したことが奏功し、株価に対する影響も生じませんでした。

宮部　当社も製品のセキュリティを品質の一つとして捉えており、それを推進する組織として「製品セキュリティセンター」を設置し、出荷前のセキュリティ検査をはじめ、市場に投入された製品についてもアタックテストを行っています。自社製品のセキュリティを守ることに対して、製品セキュリティセンターのチームは高いモチベーションをもって取り組んでいるのです。また、あらゆる業界で同様のインシデントが発生していることから、当社を先行事例として異業種の企業の方々からも相談をいただくケースが増えています。

山本　従来、サイバーセキュリティ対策は情報システム部門を中心に行われていました。しかし、最近では生産拠点の品質管理部門がサイバーセキュリティを考え始めており、そうした背景には、単に製品を売るだけでなく販売後の顧客とのつながりを強化する「サービス事業へのシフト」も影響していると考えられるでしょう。

経営者の目線を持ったセキュリティ人材の育成が急務

山本　サイバーセキュリティに関する人材不足が問題となっていますが、この課題へはどう対処していますか。

小島　当社には大きなIT部門があり、サイバーセキュリティのテクノロジーという面については十分に育成できると考えていますが、経営目線でセキュリティを見ることができる人材は圧倒的に不足しています。経営者としての経験に加え、デジタルリテラシーとグローバルな感覚を有した人材の育成が急務であり、そうした観点に基づいてセキュリティ人材の育成に努めています。

宮部　私もセキュリティの専門技術を有した人材の育成に加え、そうした人材が経営目線を持って社内外に対して多様な取り組みを行っていくことが必要だと考えています。製品のセキュリティについては、業界に先駆けて取り組みを行ってきたことで当社の活動が世に知られたこともあり、新卒や中途採用の優秀な人材が集まるようになってきています。

山本　サイバーセキュリティの人材は、将来的に約193,000人も不足するともいわれています。数はもちろん質の向上も重要であり、経営的な視点を備えるように教育、育成を行っていくことが不可欠です。実際、金融業界などでは経営者や役員クラスの人材がCISOを担うケースが徐々に増えています。このようなキャリアパスが提示されることで、社内でセキュリティをリードしていく人材にも光が当てられるようになると期待を寄せています。

山本 直樹

コンサルティング業界で20年以上の業務経験を持ち、金融機関や大手製造業などへサイバーセキュリティをはじめ幅広い分野のサービスを提供。PwC入社以前には、米国系コンピュータメーカーの情報セキュリティ統括責任者として多様な実務経験も持つ。

サイバーセキュリティ面でも治安の良い国を目指す

山本　それでは最後に、重要な社会・生活インフラに携わっている立場から、安心で持続可能なデジタル社会を実現してくために、近未来社会のサイバーセキュリティについてどのような展望をお持ちなのかをお聞かせください。

宮部　サイバーセキュリティは、法律面でまだ整備できていない部分があることに加え、一般の方々の理解も十分ではなくコンセンサスができていないのが実情です。もちろんメーカーがやらなければならないことも山積みですが、国を挙げてサイバーセキュリティに取り組んでいく必要があると考えています。国家というレベルにおいてもサイバーセキュリティの“治安”を保つことができれば、多くの産業が発展していけるようになるでしょう。

小島　サイバーセキュリティの問題は非常に大きなチャレンジで、単独の企業だけで全て担うのは不可能であり、民間・政府を問わず皆が協力し合って次のレベルの信頼を創出していかなければなりません。そうした機運は出来上がりつつあり、インシデントに対する情報や対処のためのベストプラクティスの共有も進んでいます。そうした取り組みをグローバルにも広げ、次の社会を築いていくことが必要です。日本は未来社会のコンセプトとして「Society 5.0」を提唱していますが、その実現のためにも万全のセキュリティが不可欠となるでしょう。

宮部　セキュリティは、安定的な経済や生活などの多様なモノをつくるベースになることですよね。サイバーセキュリティに関係している皆さんは、「自分たちの取り組みがより良い社会をつくっていくんだ」という前向きな攻めのセキュリティ活動ができれば、理想とする安全な社会が実現されるのではないでしょうか。

小島　私も賛成です。明るく元気にセキュリティに取り組むためにも、情報の公開やシェアなど、デジタル社会の良さを生かしながら透明性を徹底的に上げていくべきだと思います。

山本　他国と比べて犯罪が少なく治安がいいと言われている日本の社会を、サイバーセキュリティの面でもさらに良くしていこうというのですから、より明るく自信を持って取り組んでいきたいですね。私もコンサルタントの立場から、皆さんと一緒になって未来社会のセキュリティを実現していきたいと考えています。本日はありがとうございました。

経営層と議論するための サイバーリスクの数値化モデル

デジタル化が進むほどサイバーリスクは高まり、セキュリティ事故の発生による経営インパクトも増大する。専門用語が多く、動向の変化も激しいサイバーセキュリティは、取締役や経営者には扱いづらい課題でリスクが見えにくい。そこで、経営層の共通言語である財務諸表を用いてリスクを金額に換算することにより、ITに詳しくなくてもリスクを把握できるようになる。

日本サイバーセキュリティ・イノベーション委員会（JCIC）主任研究員
（PwCコンサルティング合同会社から出向中）
上杉 謙二

サイバーセキュリティ専門の民間シンクタンクに出向中。現在の主な研究テーマは、海外のサイバーセキュリティ法規制、サイバーリスクの定量化、官民連携の動向、オリンピックにおけるセキュリティ体制等。PwCでは、官公庁や民間企業に対するサイバーセキュリティ戦略立案、サイバー演習、インシデント対応支援、M&A戦略策定に従事。また、サイバーセキュリティの国際会議やイベントの企画にも携わる。

コーポレートガバナンスの一環として取り組むべき経営課題

経済産業省の「デジタルトランスフォーメーション（DX）レポート」※1（2018年9月発表）によると、デジタル技術を活用したビジネスモデルの創出をスピーディに進めることで、2030年には実質GDPを130兆円超も押し上げる効果があるという。一方、デジタル化の加速によりサイバーリスクは高まり、セキュリティ事故が発生した場合の経営への影響も増大する。国内大手航空会社や仮想通貨取引所がサイバー攻撃に遭い、多額の被害を受けた事件は記憶に新しく、組織内部からの機密情報や個人情報の流出も後を絶たない。一回のサイバー攻撃により大規模な金銭的損害が発生し、経営者責任が問われる事例が増えていることから、サイバーセキュリティはIT部門だけの問題ではなく企業経営の持続的成長を揺るがす経営リスクだと言える。

PwCが実施した「企業取締役調査（2017年）」※2では、取締役会が時間を費やすべき重点領域にサイバーセキュリティを挙げた回答者が66％に上った。戦略立案や後継者の計画よりも上位で、特に米国企業ではコーポレートガバナンスの一環として、取締役が経営者へサイバーセキュリティ管理の強化を求める傾向が強いという。同じくPwCの「投資家意識調査 2018」※3によると、投資家の企業に対する懸念事項のトップはサイバー脅威である。サイバー攻撃で企業価値が損なわれる事例が増えているため、最低でも投資額は回収したいと考える投資家がサイバー脅威を最も懸念するのは当然だろう。

日本企業においても不祥事によるダメージを回避するため、株主などからコーポレートガバナンスの強化が求められており、その一環でサイバーリスクについても議論すべき段階にある。

セキュリティ事故による財務インパクト

セキュリティ事故の適時開示を行った18社の株価動向を調査したところ（下図）、50日後に株価が平均10％減少していることが分かった。また、東証一部以外の企業（東証二部、ジャスダック、マザーズ、札証）の平均下落率は15％であることから、セキュリティ事故は中小企業の株価へ大きく影響すると言える。中小企業のビジネスは特定事業に依存しがちであり、その事業へのサイバー攻撃の影響は大企業に比べて大きいからだと考えられる。

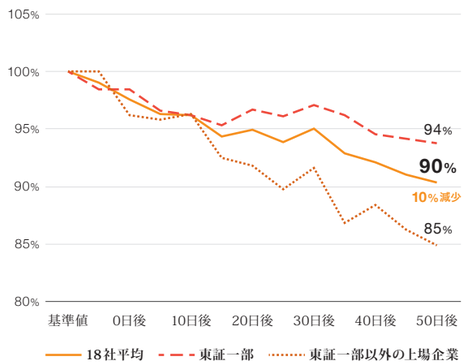
さらに適時開示を行った日本の16社の売上高と純利益を調べたところ、売上高は平均4％上昇したが純利益は平均21％減少していることが分かった。純利益の大幅な減少は、事故対応調査や再発防止のための特別損失に起因する。

サイバー攻撃が企業の株価の低下や純利益の減少を招き、経営者の責任が問われる事例もあり、サイバーセキュリティは経営リスクとして経営者が積極的に取り組むべき課題になっている。

セキュリティ事故の適時開示後の株価影響

サイバーインシデント適時開示後の株価傾向調査

調査手法
- 証券取引所へインシデントの「適時開示」を行った18社
- 2014年7月以降の適時開示企業を対象
- 開示日より10日前を100％（基準値）とした
- 日経平均株価の変動値は調整済み



出典：証券取引所の株価データをもとに筆者作成

サイバーリスクの数値化モデル（年商1000億円企業における社内報告資料の例）【潜在損失額】

		想定すべき損失額	算出根拠
直接被害	① 個人情報漏えいによる金銭被害	▲80億円	JNSA一人当たり損害賠償額より算出 （基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価×顧客数≒80億円）
直接被害	② ビジネス停止による機会損失	5営業日あたり ▲20億円	社内ヒアリングより算出 （1日あたりの生産量×商品単価≒2億円）（1日あたりのECサイト売上≒2億円）
直接被害	③ 法令違反による制裁金	▲40億円	EUデータ保護指令（GDPR）の制裁金 （全世界の売上高の4％≒40億円）
直接被害	④ 事故対応費用	▲0.6億円	過去事例や業者ヒアリングにより算出 （調査費用、データ復旧費用、応急処置費用等）
間接被害	⑤ 純利益への影響	▲10.5億円	JCIC調査実績より算出 （前期純利益50億円×21％≒10.5億円）
間接被害	⑥ 時価総額への影響	▲300億円	JCIC調査実績より算出 （時価総額3000億円×10％≒300億円）

出典：取締役会で議論するためのサイバーリスクの数値化モデル（https://www.j-cic.com/reports.html#org_ovrvw1）
「企業のCISOやCSIRTに関する実態調査2017」（https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html）

サイバーリスクの数値化モデル

企業内でのサイバーリスクの議論は技術的な話に終始しがちだが、企業経営者の立場では自社の経営に対する金銭的影響や経営責任が発生する可能性に関心を持つはずだ。経営視点で議論を行うには、経営者の共通言語である財務諸表によりリスクを金額に換算して見える化し、ITに詳しくなくてもリスクを把握できるようにする必要がある。

そこで、「サイバーリスクの数値化モデル」を策定した（上図）。これをもとに各企業でリスク値を算出し、取締役会や経営会議への報告などに活用することが可能である。このモデルで年商1,000億円企業のリスクを評価すると、直接被害が約141億円、間接被害が約312億円となる。サイバーリスクは歴史上新しい分野で過去データが比較的少なく、精緻なリスクモデルに比べると被害額は大きめに算出されるが、自社が被り得る最大損害額（PML：Probable Maximum Loss）を即座に把握できることは有意義だと考えている。

サイバー攻撃によるリスク自体は発生確率の算出が難しいが、情報処理推進機構（IPA）の調査※4によると、日本では一年間に26％の企業に被害が発生しているという。年間に、約4分の1の確率で被害に遭うと考えると分かりやすいだろう。サイバーリスクのコントロールには、数値化によるイメージが重要だ。サイバーリスクの数値化モデルなどを用いることで、投資額の妥当性判断がしやすくなるだけでなく、経営層がサイバーリスクを自分事として捉えられるようになるだろう。

※1：経済産業省「デジタルトランスフォーメーション（DX）レポート」（http://www.meti.go.jp/press/2018/09/20180907010/20180907010.html）
※2：PwC「企業取締役調査（2017年）」（https://www.pwc.es/es/publicaciones/consejos-y-buen-gobierno/pwc-2017-annual-corporate-directors-survey.pdf）
※3：PwC「投資家意識調査 2018」（https://www.pwc.com/jp/ja/knowledge/thoughtleadership/investor-survey.html）
※4：IPA「企業の CISO や CSIRT に関する実態調査 2017」（https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html）

サイバーセキュリティへの対応に不可欠である法的な視点

サイバーセキュリティは、現代のあらゆる企業が対処すべき極めて重要な課題である。企業においてサイバーセキュリティに関する検討を行う際には、技術的な側面がクローズアップされることが多いが、役員・従業員の法的な責任、法規制への対応、情報流出時の損害賠償責任といった法的な視点からの検討も欠かすことはできない。ここでは、サイバーセキュリティへの対応を検討するにあたって念頭に置くべき、基本的かつ重要である法的な視点を紹介する。

PwC弁護士法人
シニアマネージャー　弁護士、ニューヨーク州弁護士
山田 裕貴

2008年弁護士登録。一般的な企業法務をはじめとして、情報法制、コーポレートガバナンス、税務、M&Aおよび信託、危機管理を主な取扱分野としつつ、複数の法分野に関する経験を生かして、法分野にとらわれず、法的課題を総合的に解決することに注力している。

1.取締役の責務という視点（会社法上の規律）

取締役の善管注意義務と内部統制構築義務

会社の取締役は、法律上の義務として、善良な管理者の注意をもってその職務を執行する義務を負う（善管注意義務。会社法330条、民法644条）。また、取締役は、その職務の一環として、内部統制システムの基本方針を取締役会で決定し、当該基本方針に基づき、内部統制システムを構築する義務を負っている（内部統制システム構築義務。会社法362条4項6号・5項等参照）。サイバーセキュリティに関する対応は、企業にとって、競争力の源泉となり得る技術情報やノウハウ、顧客や取引先に係る情報などの安全を確保した上でこれらを有効に活用するという、経営上極めて重要な意義を有するものであることから、内部統制システムの構築にあたって検討すべき主要な要素の一つだと考えられる。個人情報の流出に係る損害に起因して株主代表訴訟が提起される事例も見られ、マネジメント層としては、自らの責任が問われ得ることを前提としてその責務と向き合うことが必要となる。

法的な義務違反の有無に関する判断

最低限の問題として、どの程度の対応を行えば法的には義務違反がなかったと評価されるのであろうか。この点については、事業の性質や保有する情報の質および量などの個別具体的な事情を踏まえつつ、問題となった行為が発生した時点において通常の企業の経営者であれば実施していたはずの対策が実施されていたかという、極めて当然の視点が重要となる。裁判所が判断する際の拠りどころとしては、まずは公的な機関から公表されているガイドライン等※1において推奨されている対策が参照されることになるであろう。

規制への対応と取締役の義務

近時においては、GDPRをはじめとする国内外のデータ保護規制への対応に関する費用や手間の負担に悩む企業も多いであろう。各企業が規制への対応方針を決定する際の出発点として、相当の費用や手間を要するとしても、会社法上、取締役には法令（外国の法令を含む）に違反する態様で事業を行う裁量は与えられていないことを改めて確認しなければならない。一般に、取締役の経営判断については取締役の裁量を尊重する「経営判断の原則」に基づき、損害賠償責任を負うのは限定的な場合とされている。しかし、取締役が国内外の法令に違反する態様で業務執行を行った場合、基本的には、任務懈怠があるとされ、これにより会社に生じた損害について損害賠償責任を負うものと考えられている※2。

2.インシデント発生時に企業に生じる第三者への損害賠償責任という視点

サイバーセキュリティへの具体的な対応や投資を検討する際には、費用対効果の観点からインシデントが発生した場合にどの程度の損害（業務への影響、レピュテーションへの影響、インシデントへの対応費用など）が発生し得るのかを考慮することが有用となるであろう。また、法的な視点からは、損害賠償責任・制裁金の負担が重要な論点となり得る。

個人情報の流出に関して生じ得る法的な責任（個人への民事賠償責任）

インシデント発生時に企業が負担し得る損害賠償責任の典型的な例として、個人情報が流出した場合における個人に対する損害賠償責任が挙げられる。これまでの日本の裁判例においては、個人情報の流出に関する不安感などを理由とした慰謝料の請求が認められた事例においても、その賠償額は一人あたり数千円から数万円前後である※3。しかし、最近では日本でも原告団を組成して訴訟を提起する事例が見られ、流出する個人情報の質および量によっては損害賠償の総額は高額になり得る。また、外国においては賠償額が日本におけるものよりも多額になる可能性があるという点も忘れてはならない。

当局が課し得る制裁金やペナルティ

このような個人に対する損害賠償に加えて、規制当局から課される制裁金についても留意する必要がある。日本の個人情報保護法は、その違反について直ちに罰金などが科される仕組みとなってはいない。もっとも、海外に目を向けると、EUのGDPRに違反した場合は最大で2,000万ユーロまたは企業の年間の全世界売上高の4%のうちいずれか高い方の制裁金が科され得る（GDPR83条）。また、米国においても個人情報の保護を直接の目的とする統一的な法令は存在しないものの、連邦取引委員会（FTC）が、個人情報の取扱いについて適切な開示をしていない企業などに対して、FTC法5条などに基づき不公正または欺瞞的な取引に該当することなどを理由として、行為の差止めや金銭的なペナルティの支払いなどを求めている※4。

その他の情報資産の流出や消滅などに伴う損害賠償責任

上記のような個人情報の流出事案に限らず、ある企業の故意または過失に基づくインシデントの発生によって他者に損害が発生した場合には、契約上または不法行為上の責任として損害賠償責任を負い得る。すでに述べた個人情報の流出事案においては、主として精神的な損害という算定しにくい損害が賠償の対象とされている。他方で、(i)顧客・取引先の預り資産が流出した場合、(ii)顧客・取引先の情報を消滅させた場合、(iii)提供するシステムの可用性を維持できなかった場合などは、数値化することに親和性があり、かつ多額に及び得る財産的な損害を賠償する責任を負い得る。日本法のもとでの損害賠償の額は一般論として、①過失に基づく行為がなかったと仮定した場合における財産の状況と②過失に基づく行為の後における財産の状況の差額として認識されることとなるため、例えば流出した資産の経済的価値そのものや失われた利益が、損害賠償の額として認識されることとなり得る。法的な視点からは、取引から見込まれる利益と自らが契約上負担するリスクが見合っているか、逆に契約の相手方に契約上適切な損害の負担を求めているかなど、契約上のリスクアロケーションが重要な論点となる。

3.人事・労務に関する視点

最後に、法的に重要なもう一つの視点として、従業員との法律関係を適切に整理しておくという点が挙げられる。「サイバーセキュリティ」というと、クラッカーなどの第三者による侵害行為をいかに防ぐかというイメージが強いが、現実に発生した情報流出事案の原因の多くは、従業員の不注意（誤操作など）といった、内部に原因が求められるものが多いといわれている※5。労働法規を踏まえつつ、就業規則等に秘密保持義務や懲戒の根拠規定などを適切に盛り込むこと、入社時・退職時に秘密保持に関する誓約書を徴求すること、データ保護に関する法令に関する教育を行うことなどの基礎的な対応は、サイバーセキュリティのみならず、有事における従業員との紛争に対処するという観点からも重要である。

※1：このようなものの一例として、経営層が参照することを想定して経済産業省・独立行政法人情報処理推進機構から公表された「サイバーセキュリティ経営ガイドライン Ver 2.0」（http://www.meti.go.jp/policy/netsecurity/mng_guide.html）が挙げられる。
※2：例えば、最判平成12年7月7日民集54巻6号1767頁参照。
※3：例えば、大阪高判平成13年12月25日判例地方自治265号11頁、東京高判平成19年8月28日判タ1264号299頁など参照。
※4：例えば、2017年におけるFTCによる法執行の状況について、FTC『Privacy & Data Security Update: 2017』（https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives）参照。
※5：具体的なデータについては、例えば、個人情報保護委員会『平成28年度個人情報の保護に関する法律施行状況の概要』19頁や、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『2017年情報セキュリティインシデントに関する調査報告書【速報版】』参照。

クラウドセキュリティ

―デジタルトランスフォーメーションの実現に必要な新たな手法―

あらゆる産業にデジタルトランスフォーメーション（DX）の波が押し寄せ、ビジネスモデルも従来の直線的なバリューチェーン型から、デジタルの活用によるクロスボーダー型へと変容している。価値創造は双方向かつ継続的にスケール拡大されるため、そのワークロードを支えるクラウドの利用が急速に拡大しつつある。こうした状況下でクラウドのリスク管理の取り組みにも変革が求められており、ここではビジネスモデルの変化にも対応したクラウドセキュリティの新たな手法について紹介していく。

PwCあらた有限責任監査法人
ディレクター
川本 大亮（監修者）

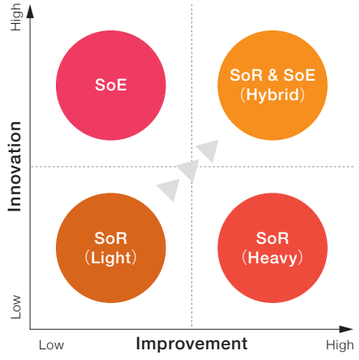
ITに関するアシュアランスおよびアドバイザリーサービスを日系・外資系企業に提供しており、内部監査、外部監査、US/J-SOXプロジェクト、セキュリティ評価、第三者に対する保証と意見表明サービスにおける、ITリスクの発見・評価の経験を豊富に有する。近年はクラウド利用者・事業者向けのクラウドセキュリティ監査、クラウドリスク評価アドバイザリ、サイバーセキュリティアセスメントなどを多数経験している。

PwCあらた有限責任監査法人
シニアマネージャー
饒村 吉晴（執筆者）

システム開発、コンサルティングファーム、起業、大手グローバルITベンダーを経て現職。金融／公共／製造／サービス業を中心に、経営管理、内部統制、サイバーセキュリティの分野でコンサルティングやプロジェクト管理の実績多数。事業戦略からビジネス開発の上流分野も得意領域。近年はクラウド、AI、FinTechなどにおける戦略立案や基準策定の業務に従事し、同領域における講演、寄稿、執筆の活動も多数。

クラウドの適用領域に応じた対応

そもそもシステムの目的にはSoR（System of Record）とSoE（System of Engagement）の二つがあり、「バイモーダルIT」とも呼ばれる。SoRは「記録のシステム」で内部プロセスのデジタル化によりインプルーブメントを追求することを目的とし、SoEは「つながりのシステム」で外部サービスの連携により新たなイノベーションを生み出すことを目的としている。



クラウドの適用領域が下図の右上（SoR & SoE）に広がる中、クラウドのリスク管理においては、一律にコントロールベースで評価するのではなく、システムの特性と複雑性を踏まえてリスクベースで必要な対応を効率的かつ効果的に検討し対応することが費用対効果の高い有効なアプローチである。

また、クラウドはビジネスの成長に応じてサービスや構成をアップデートしていくため、随時変化するサービスや構成に対してコントロールベースの標準的なアプローチでは不十分となる場合が多く、想定し得るリスクに迅速かつ柔軟に対応することが不可欠である。

1 **SoR（Light）**
Webサービスやファイル管理等におけるクラウド利用

2 **SoE**
外部サービスと連携したクラウド利用

3 **SoR（Heavy）**
基幹システム、ミッションクリティカルなシステムにおけるクラウド利用

4 **SoR & SoE（Hybrid）**
SoRとSoEを連携したクラウド利用

リスクベースアプローチに加えて、二つのトレンドを紹介する。一つ目は、情報セキュリティの三要素「CIA」に関することである。C（Confidentiality：機密性）、I（Integrity：完全性）、A（Availability：可用性）の順で重要性に基づき表記されるのが一般的だが、セキュリティに関連した国際的な団体などの文書では「AIC」と表現されるケースが増えており、可用性や完全性が重視される傾向が強い。これは、DXによるビジネスモデルがエコシステムによりつながる仕組みであるため継続性が求められ、さらにデジタルによるスマートライフやスマートヘルスケア、スマートカーにおいては可用性や完全性が人命と安全に関わるためだ。当然、クラウドセキュリティにおいてもこうした考えを検討する必要がある。二つ目は、このAICの検討対象である。従来のオンプレミスでは、「情報」と「情報システム」を対象としていた。一方クラウドは、「情報」を対象とすることは同じだが、抽象化された論理的なサービスでありハードウェアやネットワークといった物理的な情報システムではないため、クラウドが適用される「業務」を対象とすることが望ましい。

クラウドの適用領域となる「情報」や「業務」をAIC（可用性／完全性／機密性）の視点から重み付けを行い、その重要度とリスクに応じたリスクベースアプローチにより対応を行うことが有効だと言える。

責任共有モデルの領域に応じたユーザーの対応

リスクベースアプローチにおいて、責任共有モデルの領域に応じたユーザーの対応（上図）も重要なポイントとなる。

Ⅰのクラウド事業者が管理する領域では、クラウド事業者の内部統制を認証や外部監査で保証するが、ユーザーがその認証や外部監査の内容を理解した上で、リスクに対して足りないコントロールを必要に応じて追加で考えなければならない。

Ⅱのクラウドサービスで管理する領域では、クラウドサービスの特性に応じたセキュリティについて検討する必要がある。昨今、ストレージ型のマネージドサービスにおけるアクセス制御や通信の設定・対策漏れによるセキュリティインシデントが増加傾向にあり、特にクラウドで意識すべきポイントだ。

Ⅲのクラウドサービスに関係しない領域では、オンプレミスの技術で構築した領域を、オンプレミス環境と同様にセキュリティについて検討しなければならない。その検討に際して、ⅠとⅡとⅢのオーケストレーションも重要である。例えば、Ⅰのリージョン（クラウドサービスを配置する世界の各地域）やアベイラビリティゾーン（リージョン内のデータセンター）で災害などによりサービス停止が発生した場合、Ⅰ・Ⅱ・Ⅲをオーケストレーションさせて RPO（目標復旧時点）やRTO（目標復旧時間）についてどう実現するのか。もしくは、Ⅱのコンピューティングサービス上にⅢのオンプレミス環境と同様のOSやアプリケーションが配置されている場合、Ⅱのコンピューティングサービスのオートスケール（自動伸縮機能）によってスケールイン（縮小）した時に、通常であれば消滅してしまうOSやアプリケーションのログをどう保全するかなどということである。

最後に、クラウドでは容易にサービスを利用できることから、オンプレミスの静的な環境（一度構築、設定したら変更があまり発生しない）と比較して、動的（サービスの構成、設定共に変更可能）な環境であると言える。一度評価した構成と設定がユーザーによって変更されたり、クラウド事業者のサービスリリースによって構成や設定がアップデートされるため、設定変更に対する管理態勢や、クラウドの構成と設定への定期的な評価が重要である。

Eurasia Group GZERO SUMMIT JAPAN 2018

G7を構成する主要先進国が指導力を失い、G20も機能しなくなる“Gゼロ”の世界へと時代は突入しつつある。このようなリーダー不在の“Gゼロ”の世界では、地政学リスクを理解することが企業にとっても必要不可欠となる。さもなければ、国境問題に始まりテクノロジーの進歩に伴う未来の仕事への不安、遠隔地の選挙を標的にするハッカーの存在など、新世代の地政学的脅威には対処できないのだ。

このような情勢を背景に「社会に信頼を構築し、重要な課題を解決する」ことをPurpose（存在意義）とするPwC Japanグループは、八年にわたるユーラシア・グループとの協業を通して、地政学リスクを正しく捉えることの重要性を日本の経営者へと伝え続けてきた。そしてこのほど、ユーラシア・グループ社長であるイアン・ブレマー氏の「地政学リスクをテーマとした国際会議を日本で開催し、第二のダボス会議を目指す」という壮大な構想に共感し、2018年10月17日にパレスホテル東京で開催された「GZEROサミット」に協力することとなった。

本サミットの基調パネル・ディスカッションには、PwC Japan グループ代表の木村浩一郎がパネリストとして登壇。産業界からは経団連会長の中西宏明氏、政府の視点で経済産業省通商政策局長の田中繁広氏、モデレーターのブレマー氏とともに、「激変する国際競争環境～ジオポリティクスとジオテクノロジーのはざまで」というテーマのもとで活発な議論を繰り広げた。ここでは、ブレマー氏と木村の発言を中心にリポートする。

Opening

地政学的な景気後退期へ陥る世界

まず、ブレマー氏が現在の地政学リスクの概要を説明するとともに、今回のサミットの意義を示した。国際情勢にまつわる最新のニュースの数々を紹介すると「これらの出来事は、偶然起きているわけではない。世界が地政学的なリセッション（景気後退期）に突入してしまったのが原因だ」と強調した。

振り返れば第二次世界大戦以来、およそ七年間に一度の割合で世界的な経

> “「Gゼロ」の世界では理想的なモデルとして日本が注目を集めている”

済不況が生じてきた。前回は、言わずと知れたリーマンショックだ。この時は主要国の政府が立ち上がり、足並みをそろえて全力で世界恐慌を防いだ。「そして今、地政学的な景気後退期に差し掛かっている。この不況が大恐慌へ移行すれば、戦争のリスクが極めて高くなる。本サミットの目的はそうした事態を防ぐことでもあり、日本で開催した理由は、日本が“例外的な国”だからである」（ブレマー氏）

日本のリーダーシップに世界が注目する理由

世界ではリベラルな民主主義が侵食されており、中産階級の労働者の多くがグローバル経済の恩恵を受けているとは考えられず社会制度への不満を募らせている。さらにはテクノロジーの進展により情報の消費量が増え、意見の固定化が生じ社会が二分化されつつある。

ブレマー氏は言う。「このような状況があまり見られない、例外的な国が日本なのだ。中産階級は経済状況や社会制度へ大きな不満を募らせるほどではなく、また他国ほどには社会が分断されていない」

このような日本ならではの特性によって、“Gゼロ”の世界において、日本は世界が学ぶべきモデルとしての価値を高めることになったのだという。「『リベラルな民主主義が機能するということを、日本は体現している。もっと日本から学ぶことがある』という意識が芽生えつつあるのだ。今こそ日本そして日本企業にはリーダーシップを発揮していただきたい」とブレマー氏は力説し、日本企業が競争力を再構築するためのアクションについて議論を促した。

こうした情勢のもと、世界の政治リスクを見ていく上で、地政学に加えて、民間主導の米国と国家主導の中国の異なるシステム間で展開されるテクノロジー分野の覇権争いの行方に注目する「ジオテクノロジー」という視点が不可欠となっている。

Panel Discussion

激変する国際競争環境
～ジオポリティクスと ジオテクノロジーのはざまで

ジオテクノロジーがもたらす 新たな競争環境下での企業の在り方

続いて、経団連会長の中西氏、経済産業省通商政策局長の田中氏とともにPwCの木村が登壇したセッションでは、ジオテクノロジー下の新しい競争環境に日本企業がどう向き合うべきかについて議論がなされた。

PwCが各国のCEOを対象に毎年実施している「世界CEO意識調査」の第21回の結果では、CEOにとっての脅威として「過剰な規制」「テロの脅威」「地政学上の不確実性／サイバー脅威」がトップ3となり、いずれも40％台の高い割合を占めている。一方、アジア太平洋地域に限れば「人材の獲得」「技術進歩のスピード」「テロの脅威」という順で、日本のCEOもほぼ同様の結果である。

これについて、木村は次のように総括した。「世界的に、CEOは企業側で十分にコントロールができず対応が受け身にならざるを得ない地政学リスクをより強く意識する傾向にあることが分かる。対して日本も含めたアジア太平洋に限れば、企業側でコントロール可能な脅威が目立つ。ただし、数年前までは世界のCEOも自社でコントロールできるリスクを上位に挙げており、今回の変化は地政学上の多様なリスクが高まってきたからに他ならない。日本企業にも、地政学に関するリスクを十分に理解し、それらが顕在化した際にいかにレジリエンスをもって対応できるかが求められてくるのだ」

世界の三極構造化と保護主義2.0

ブレマー氏によると、市場規模や貿易だけでなくAIとサイバー世界においても「米国と中国の二つの大国によるダブルスタンダード」の世界秩序が進行しているという。そして雇用創出を目的とした伝統的な産業保護だけでなく、デジタルネットワーク経済における覇権争いを狙い、「古い」経済と「新しい」経済の双方に障壁を有する「保護主義2.0」が生み出されているのである。こうした状況について、木村は「政治リスクにとどまらずテクノロジーの要素も加わり、企業の競争環境が大きな転換点を迎えている」と指摘した。

また、米国と中国の二大国が自由競争主義と国家主導の経済産業政策において、それぞれが自国主導のスタンダード確立を目指す中、欧州ではGDPRなどの規制を強化しながら「社会民主主義」的な自国産業の保護・育成を目論むといったように、世界には三極構造が見て取れる。「米国と中国、欧州のアプローチはそれぞれ異なっている。しかし幸か不幸か日本のマーケットというのは既にグローバル化されており、三極のうちのどこか一つのマーケットに特化しているわけではない。従来の貿易戦争にテクノロジーの要素が加わった保護主義2.0の時代に入ったと言える」（木村）

> 「ビジネス」「技術」「法律」の三つのリテラシーに精通した人材の育成が不可欠だ

デジタルネットワーク経済のもとで 価値を創出するには

保護主義が強まるほど、デジタルネットワーク経済下での覇権争いが熾烈になっている。木村は、デジタルネットワーク経済における三つのフレームワークを示していった（図①～③）。

一つ目のフレームワークとして、デジタルネットワーク経済の流れを振り返り、これまでを「1回戦」、これからを「2回戦」というラウンドに切り分けた。過去二十年間には、「情報」の交換技術であるインターネットの台頭とともに、デジタルネットワーク技術で複製可能なテキスト、音楽、映像といったコンテンツを巡る戦いが展開された。その典型的な勝者が、FANG（フェイスブック、アマゾン、ネットフリックス、グーグル）に代表されるプラットフォーマーである。これらの米国系のプレイヤーが参入できない中国では、BAT（バイドゥ、アリババ、テンセント）といった新興企業が成長を遂げており、両者によるプラットフォームの寡占状況がデジタルネットワーク時代の1回戦であった。

「来る2回戦では、金融資産や自動運転、遠隔医療などの人命に関わるデータをデジタルネットワークで扱うため、情報の安全性、『信頼』が鍵となる。1回戦で米国・中国企業にプラットフォームを寡占されてしまった日本企業にとって、巻き返す絶好のタイミングだ。勝利の最大のポイントは、1回戦におけるプラットフォーマーの戦い方を理解することにある」（木村）

デジタルネットワーク時代において重要となるのが、二つ目のフレームワークである「ビジネス」「技術」「法律」という三つのリテラシーだ。1回戦において米国と中国はそれぞれ法律を巧みに活用してプラットフォーマーを誕生させたが、日本ではそうはいかなかった。しかし、2回戦ではユーザーからの信頼を確保するための「法律」の重要性が、1回戦と比べて格段に増すことになる。

「ジオテクノロジーという視点での戦いでは、法律に対する国としての取り組みも大きなアジェンダとして問われてくる」と言う木村に対して、中西氏と田中氏からも賛同の意見が発せられた。

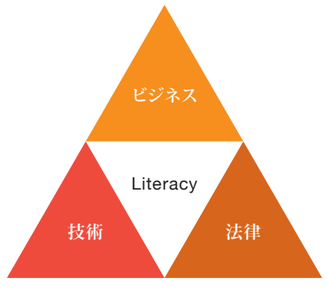
最後に木村は、三つ目のフレームワークとして日本企業におけるデジタル推進の段階を「調査・研究」「実証実験」「ビジネスモデル再構築」の三段階に分類。「第三段階のビジネスモデルの再構築から新しい価値創造につなげていくところのプレゼンスが、日本企業は海外企業と比較すると相対的に弱いと言える」とし、その理由として先述の三つのリテラシーのうち「技術」にフォーカスし過ぎている点を挙げた。

「三つのリテラシーに精通した人材育成に、産業界さらには国家として取り組むことが課題である」と木村が締めくくると、ブレマー氏、中西氏、田中氏も同意して議論は幕を閉じた。

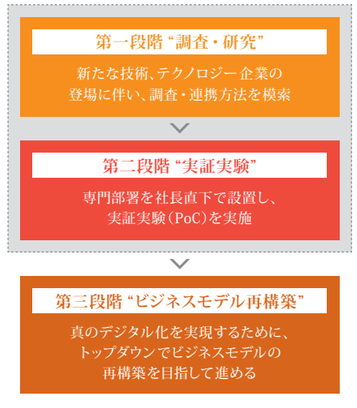
デジタルネットワーク経済における3つのフレームワーク

①デジタルネットワーク経済における1回戦と2回戦

②保護主義2.0時代に求められるリテラシー



③日本企業におけるデジタル推進の三段階



PwCあらたの監査品質を支える取り組みを紹介する「監査品質に関する報告書2018」開示

ステークホルダーの皆様へ、PwCあらた有限責任監査法人のミッションを遂行するために構築しているガバナンスおよび品質管理の体制に関する説明責任を果たすため、「監査品質に関する報告書」を開示しました。ウェブページには、当法人の監査品質を支えるパートナー・職員の声を紹介した動画を掲載しています。ぜひご覧ください。

https://www.pwc.com/jp/ja/about-us/member/assurance/transparency-report.html

M&Aを成功に導く『ビジネスデューデリジェンスの実務』刊行

PwCアドバイザリー合同会社は『ビジネスデューデリジェンスの実務（第4版）』を刊行しました。昨今のM&A環境を踏まえて第3版を見直し、「派生型デューデリジェンス」や「業種別デューデリジェンス」といった項目を追加しています。また、近年活況を呈しているベンチャー投資に加えて、企業経営に強く求められるサステナビリティの視点からもM&Aにおける留意点を記載しています。ビジネスデューデリジェンスに関する基礎的な説明から、デューデリジェンスの重要な視点や進め方などを具体的な解説をまとめた手引書です。
（中央経済社／5,000円・税抜き）

「地方創生SDGs官民連携プラットフォーム」分科会を開催 ―地方創生をテーマにディスカッション

内閣府が事務局となり設立された「地方創生SDGs官民連携プラットフォーム」にPwCコンサルティング合同会社が参画し、先導的デジタル技術・まちづくり開発手法による地域創生分科会の第一回を主催しました。本プラットフォームは、SDGsを共通言語として、課題解決に取り組む産学官のパートナーシップの推進を目的としています。PwCのコンサルタントによるファシリテーションのもとに行ったグループディスカッションでは、自治体・企業など多様な視点から現場の課題感が共有され、地方創生の実現に向けた活発な議論が行われました。

経理・財務の実務家に向けた定番書の最新版『投資ストラクチャーの税務［九訂版］』刊行

PwC税理士法人は、投資ストラクチャーに関する税務上の取扱いを網羅的に解説した最新版『投資ストラクチャーの税務［九訂版］』を刊行しました。2004年の初版以来、大変好評を得て九訂版まで版を重ねています。クロスボーダーの投資ストラクチャーに関する税務は、慎重な検討を要するとともに専門的な知識を必要とする分野です。本書は、当法人の豊富な知識と経験に基づき、企業の経理・財務・税務ご担当者の投資ストラクチャー検討時の一助となることを目指した、実務家必読の一冊です。
（税務経理協会／4,800円・税抜き）

"Build trust in society and solve important problems
（社会における信頼を築き、重要な課題を解決する）"というPwCの存在意義（Purpose）に基づいた多様な活動や取り組みをご紹介します。

インクルーシブなカルチャー醸成に向けたLGBT活動で「work with Pride Gold」受賞

PwC Japanグループでは、LGBTメンバーが本来の力を最大限発揮できるインクルーシブなカルチャーを醸成するため、グループ代表の木村浩一郎と共に、各法人のリーダー、ダイバーシティ推進リーダーを中心にさまざまな取り組みを行っています。LGBT当事者のグループや支援者であるアライネットワークを組織し、外部講師を招いた研修やe-learning、より自分らしく各個人が幸せを追求できる社会を目指す「東京レインボープライド」への参加やフォトコンテストなどを実施しました。

2018年10月、東京ミッドタウン日比谷で開催されたLGBTカンファレンス「work with Pride 2018」のPRIDE指標の表彰式では、これら一年間の取り組みを評価されて、最高位のGoldを受賞しました。

work with Pride Gold 2018

PRIDE指標 2018 Gold

“全てのメンバーにとって働きやすい職場づくりを推進していきます”

PwC Japanグループでは、LGBT支援のための取り組みを始めました。これらの新たな活動が、多様性を尊重し異なる視点を取り入れる私たちのインクルーシブな企業文化をより強固にし、ひいては、PwC Japanグループメンバー全員、クライアント、社会への価値提供を最大化できると信じています。LGBTメンバーはもちろん、全てのメンバーにとってインクルーシブで働きやすい職場づくりに積極的に参加してもらえるように働き掛けていきます。

木村 浩一郎
PwC Japanグループ代表

体験から
新たな視点と発想を

PwC Japanグループは、2017年に東京大手町にエクスペリエンスセンターをオープンしました。「体験」することで生み出される新たな視点と発想が、イノベーションを創造します。私たちは、変化の時代に、皆さんが次々とイノベーションを生み出すことを総力を挙げて支援します。「体験」から新たな視点と発想を。新しいPwCはすでに動き出しています。

PwC Japan グループ

PwCあらた有限責任監査法人　PwC京都監査法人　PwCコンサルティング合同会社
PwCアドバイザリー合同会社　PwC税理士法人　PwC弁護士法人

お問い合わせ：03-6212-6810　pwcjppr@jp.pwc.com

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。