今、経営者はサイバーセキュリティとどう向き合うべきか

IoT、AI時代のリスクと価値創造

デロイト トーマツ リスクサービス 代表取締役社長

丸山 満彦

Maruyama Mitsuhiko

1992年、監査法人トーマツ入社。1998年からアメリカ合衆国のDeloitte デトロイト事務所に勤務し、製造業グループなどの米国企業のシステム監査を実施。2000年に帰国後、リスクマネジメント、情報セキュリティ、個人情報保護関連の監査・コンサルティングに従事。経済産業省の情報セキュリティ監査研究会、情報セキュリティ総合戦略策定委員会、個人情報保護法ガイドライン策定委員会の委員などを歴任。2012年3月まで、内閣官房情報セキュリティセンター情報セキュリティ指導官を兼務。

２０００年に日本政府のウェブページが改ざんされ、ページを開くと中国の国旗が表示されるという事件があった。それまでも政府はサイバーセキュリティ対策を行っていたが、これを機に本格的な対応が取られるようになった。その後２００３年に情報セキュリティ総合戦略が公表され、２００４年には内閣官房に政府の情報セキュリティの司令塔として情報セキュリティセンター（現在のサイバーセキュリティセンター）がつくられた。以降、国家としての情報セキュリティの総合的な方針、政府自身や重要インフラ等の情報セキュリティ対策については、この情報セキュリティセンターが司令塔として動くようになった。２０１４年にはサイバーセキュリティ基本法が制定されて法律の裏づけも定められ、日本としてのサイバーセキュリティのリスクに対応する体制が確立されてきている。

２０００年当時はサイバーセキュリティ攻撃等について報道されることはほとんどなかったが、今ではニュース番組で取り上げられることも多くなり、場合によっては特集を組まれることもある。また、映画のストーリーのなかにもサイバーセキュリティが取り上げられることも増えてきた。

経営者のみなさんも、もちろんサイバーセキュリティについてのリスク認識はしていると考えている。上場企業の役員でサイバーセキュリティのリスクを認識していないという人はいないと思っている。私も多くの企業の役員と話す機会があるが、サイバーセキュリティについて何も知らないという人と出会ったことはない（もちろん、サイバーセキュリティの課題に取り組んでいる役員と会うことが多いせいもあるが）。一方で、企業のネットワークを預かっている現場の人と話をすると、「経営者はサイバーセキュリティのリスクについて理解がない」という話を聞くこともある。

こうしたギャップが解消されないまま、リスクマネジメントの重要性はさらに高まっている。ＩｏＴ時代と言われるように、工場やプラントの機器が構内ネットワークを通じてインターネットにつながったり、自動車自体が情報システムとしてインターネットにつながるようになってきているからだ。今後は従来の基幹システム等の情報システム以外のシステムに対するサイバーセキュリティ対策にも力を入れなければならない。

こうした状況を踏まえて、「経営者はサイバーセキュリティにどう向き合えばよいのか」というのが本稿のテーマである。紙面も限られているので、できる限りストレートに５つのポイント

に絞って私の意見を述べていきたいと思う。

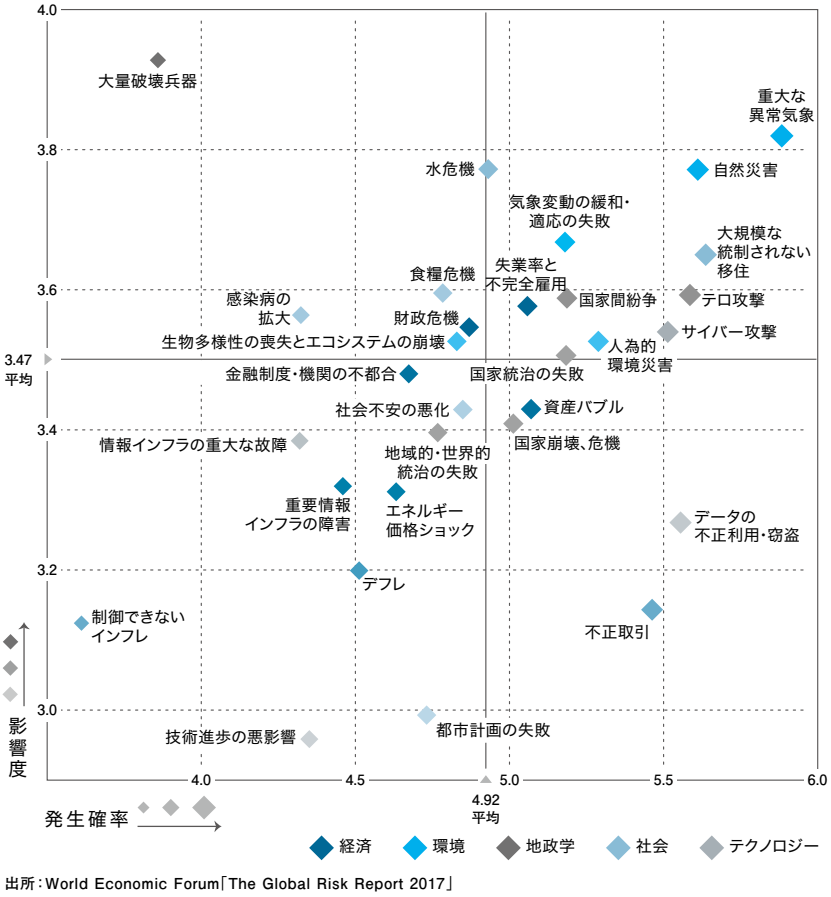
Ⅰ：役員間で、サイバーセキュリティリスクについての共通認識を持つ

Ⅱ：サイバーセキュリティ対策の司令塔をつくり、論理的に対応戦略を考える

Ⅲ：サイバーセキュリティ管理においてもPDCA、とりわけ監査が重要である

Ⅳ：予防・発見・対応の3つを意識して対策を実施する

Ⅴ：マネジメント・オペレーション・技術の3つで対策を実施する



出所：World Economic Forum「The Global Risk Report 2017」

企業の重要な業務執行については取締役会で決議をとることになる。年度予算の承認もその1つである。その予算には当然にサイバーセキュリティ対策の予算も含まれる。適切な予算が配分されなければ適切な対策を行うことはできない。従って、企業の予算を承認する役員のなかでサイバーセキュリティリスクについて共通認識を持つことが重要である。

Ⅰ 役員間でサイバーセキュリティリスクについての共通認識を持つ

例えば、自社がサイバー攻撃により工場システムを停止せざるを得ない状況に陥る可能性はどのくらいあるのか、その場合の被害はどのくらいなのか、企業価値にどの程度の影響を及ぼすのか。個人情報の漏えいの場合はどうか。技術情報の漏えいの場合はどうか……。このような質問を役員全員にたずねて、果たして全員から同じ答えが返ってくるだろうか。

自分が担当をしている領域により多く予算を配分してもらいたいと考えるのが通常であり、自分の職務とは関係ないリスクについては甘めに見てしまっていないか。企業が直面するリスクはサイバーセキュリティリスク以外にも多くあるため、こういう状況ではいわゆる声の大きな役員が重要視するリスクの対策に重きが置かれることが多くなる。これでは適切なリスク対策が取られているとは、とても言えない。

上の図を見てもらいたい。ダボス会議で有名な世界経済フォーラム（World Economic Forum）が発表している「グローバル・リスク報告書2017」の「グローバル・リスク・ランドスケープ2017」である。経営者が考えるリスクを、発生可能性を横軸に、影響度を縦軸にしてプロットした図である。さまざまなリスクが1つの図の上にプロットされている。

これを各企業においても作成することを、私はすすめたい。役員が集まってつくるのである。サイバー攻撃のリスクが高いか低いかは、ここでは重要ではない。正しいリスクを求めるのが目的でもない。1枚のシートに他のリスクとサイバーセキュリティリスクの相対関係を明示して、役員全員で共通認識をつくることが重要なのである。いろいろな意思決定の局面で役員間で意見が分かれる場合もあるだろうが、その時の立ち戻る点となる。役員それぞれの背景があるため、実際には共通認識を醸成するのは簡単ではない。しかし、こういう図をつくり、毎年毎年それを繰り返していると共通認識が醸成されていく。

Ⅱ サイバーセキュリティ対策の司令塔をつくり、論理的に対応戦略を考える

サイバーセキュリティ対策は総合的な対策である。マネジメントとして考

えるべきこと、オペレーションのなかに組み込むもの、ＩＴなどの技術を使って行うもの、物理的な対策など、企業のあらゆる活動に空気のように対策が浸透していかなければならない。従って、部門横断的な調整が非常に重要となる。そのような権限を持った司令塔が必要となる。これがいわゆるＣＩＳＯ（Chief Information Security Officer）というものである。

ＣＩＳＯの権限をどのように持たせるのかは、重要かつ難しい問題である。しかし、最大のポイントは部門横断的な調整を行うことができる権限を与えることである（従来はプラントやインフラの制御に用いるシステムについてはＣＩＳＯの所管の範囲外とされることが多かったが、最近は加える組織も出てきた）。

政府のサイバーセキュリティ対策の組織を考えてみると、その重要さがよくわかる。私は内閣官房に情報セキュリティセンターを設立する際にかかわった。内閣官房にセキュリティセンターを設置したのはなぜか。それは内閣官房が内閣の事務局であり、各省庁の調整機関であるからである。各省庁に命令を直接出すことはできないが、各省庁の調整を行う権限がある。

政府のサイバーセキュリティセンターのような組織を各企業につくるのは難しいかもしれないが、組織デザインを行う際の参考にはなるはずだ。ちなみに政府のサイバーセキュリティの責任者にあたるサイバーセキュリティ戦略本部長は、サイバーセキュリティ基本法で内閣官房長官と定められている。

次に、司令塔であるＣＩＳＯが、企業内でどのようにサイバーセキュリティ対策を整備していくかである。まずは戦略が重要である。適切な戦略に基づいて適切な戦術を組み立てていくのは、あらゆる組織において当然の話である。

ただ、リスクとしての歴史が浅く、また変化が激しいサイバーセキュリティのリスクは、全体像が見えにくいという特徴がある。状況変化が激しいので戦術を柔軟に変えていく必要もある。そのためには骨となる戦略をしっかり策定しなければならない。熟考を重ねたうえで論理的に立て、さらに少なくとも3年おきぐらいには見直す。サイバーセキュリティセンターでも、さまざまな有識者を交えながら約1年かけて練りあげた政府の戦略を、3年ごとに見直していた。

Ⅲ サイバーセキュリティ管理においてもPDCA、とりわけ監査が重要である

いわゆるＰＤＣＡは組織マネジメントの基本であり、サイバーセキュリティ管理においても同様である。このＰＤＣＡを継続して回していく際のポイントはＣ、とりわけ「監査」である。もう少し正確に言えば、適切な監査を行い、そこで発見された課題を次のＡやＰに適切につないでいくことである。

チェック（Check）は第一義的にはその部門で行うことが重要である。いわゆる自己点検だ。しかし、自己点検による発見には限界がある。例えば、専門性が不足している、第三者ではないためどうしても見逃しやすくなるといった理由からである。その際に「監査」が重要となる。特にサイバーセキュリティについては専門的な知識が必要となる場面も多いので、監査が大きな役割を担う。

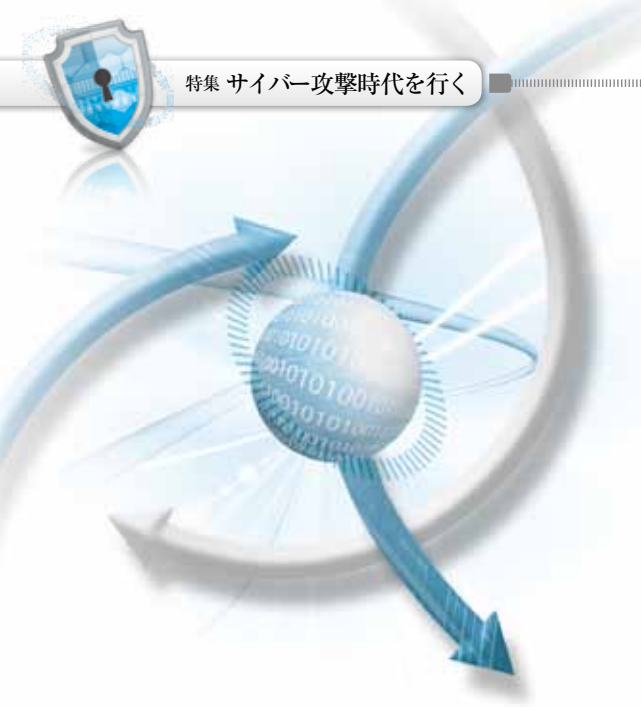
そしてこの監査で発見した課題を次の計画に反映し、対策を実施していくことが重要である。もちろん、その場で修正できるようなオペレーション上のミスや設定の誤り等は直ちに対応をすればよい。ただ、対策には時間がかかることも多い。組織をまたいでの対応が必要となるものや、予算措置が必要となるようなものについては次のＰに適切に反映し、マネジメントサイクルを回していく。

私が見る限り、多くの組織で十分な監査ができていないため次の計画に適切な対応策が組み込まれず、その結果、当初策定したサイバーセキュリティ対策がどんどん陳腐化していき、有効性を失っているケースが非常に多い。

ちなみにサイバーセキュリティセンターでも設立当時から内閣官房に監査組織を設置し、年を追うごとにそれを強化していった。サイバーセキュリティ基本法でもＰＤＣＡの重要性が明記され、サイバーセキュリティセンターに監査を推進していくことを戦略に含むように記載されている。

Ⅳ 予防・発見・対応の3つを意識して対策を実施する

これまでのサイバーセキュリティ対策は予防に重きが置かれすぎて、発見・対応についての対策が遅れていたというのが私の持つ印象である。リスクについては予防、発見、対応の3つで考えるのがセオリーであり、経済産



業省が２００３年の段階で策定した情報セキュリティ総合戦略で「事故前提」という言葉を用い、予防はしきれないことを強調したにもかかわらず、そうした状況に変化は見られない。

もっとも、予防がまずは重要であるということには変わりない。しかし、サイバー攻撃は攻撃者側が圧倒的に有利な状況に置かれている。それは長い国境を守る国とそこに侵入しようとするテロリストの戦いにも似ている。攻撃する側は1点突破に集中できるのに対して、守る側は全体を守らなければならない。圧倒的に攻撃者が有利なのだ。

従って予防、特に意図的な攻撃者に対する予防は完全にはできないという想定に立ち、侵入されたことを早く発見し早く対応する、早期発見、早期対応が重要となる。火事を１００パーセント予防することはできないが、早期発見、早期消火で被害を最小限に食い止めるのと同じである。

サイバーセキュリティにおける問題は、侵入をどのように発見するかである。これは透明人間をどのように見つけるかに似ている。透明人間であっても足跡は残すので、たくさんの足跡のなかから侵入者の足跡を見つけ出すことができる。幸いコンピュータではログを残すことができる。そのログを丹念に分析し、発見し、早期に対応する。これが重要である。

不幸にも発見が遅れた場合は大規模な消火活動が必要となり、関係者に迷惑をかけることになるが、そうした場合でも影響度を減らすために適切に対応する必要がある。最近はＣＳＩＲＴ（Computer Security Incident Response Team）を組成し、組織的な対応ができる企業も増えてきた（一方、制御システムも含めたＣＩＳＲＴとはまだまだなっていないという問題もある）。このインシデントレスポンスは危機管理の一部なので、言うまでもなく経営者もかかわる。特に重要な利害関係者への説明は当然に経営者が行う必要がある。何が起き、どのように対応をしていくのかを適時、適切に説明できなければならない。ＣＩＳＯが重要な役割を演じることになる。

Ⅴ マネジメント・オペレーション・技術の３つで対策を実施する

他のリスクマネジメント同じく、サイバーセキュリティについてもマネジメント、オペレーション、技術の３つの分野で考えればよい。どうしても技術的な対策の割合が他のリスクに比べると高くなるが、サイバーセキュリティの戦略に基づき規定等を整備する、オペレーションにセキュリティ対策を組み込む重要性は何ら変わるところがない。

経営者に意識していただきたい点が２つある。

①マネジメントが適切にできなければ、オペレーションや技術の対策は有効に機能しない

②技術的な対策でカバーできないことを、オペレーションで補うという考え方で対策を設計する

①はⅢで説明したとおりなのでここでは省略する。②はどういうことか。

人間はエラーをすることがあるが、機械のエラーは人に比べて圧倒的に発生可能性が低い。つまり、機械はほぼ間違いなく機能するということである。従って、サイバーセキュリティ対策はまずは技術的に対応できるものは技術的に対応すべきである。同じ効果を得るのであれば、人にオペレーションさせるよりも機械で自動的にさせるほうがはるかに効果的だ。言い換えれば、オペレーションコストをかけるよりもセキュリティ製品を使うほうが一般的には効果的ということである。

ただ、人工知能が発展しつつあるとしても、設定を誤っていないか、バグがある製品を使い続けていないかなど、人間のオペレーションに頼らなければならないことも多い。この３つをバランスよく設計することが非常に重要となる。

人工知能、ＩｏＴが普及していく社会になるだろう、しかし、経営者が意識すべきところは、そのような変化の中身ではない。変化に応じてどのようにマネジメントを変えていくかである。情報システムというのは五感で感じにくいだけに、マネジメントが難しい面もある。しかし、最新技術を活用したイノベーション以外に、企業発展の源泉を求めることはできない。これらをうまく活用していくということは、リスクをうまく制御していくということでもある。サイバーセキュリティ対策が、今後ますます経営の重要課題となっていくことは間違いない。この課題と正面から向き合うことが、経営者には求められている。