第 250 回　監査実務研究会報告

[日　時]　　2021 年 7 月 19 日（月）午後 2 時～午後 5 時
[問題提起者]　J-POWER テレコミュニケーションサービス㈱ 監査役 小川 重光
[ｺｰﾃﾞｨﾈｰﾀｰ]　サイバートラスト㈱ 常勤監査役 小林 正一氏
[形　式]　　Zoom のみ

[テーマ]

DX、サイバーセキュリティへの監査役の対応

○はじめに

昨今、DX という言葉を聞かない日はないと言ってもいいと思います。DX がデジタルトランスフォーメーションの略語（transformation なら”T”なのでは？と最初思いますが、trans-が右と左が交差する across のイメージで”X”を使うようです）だということを最近知った人もいるでしょうし、もう会社で推進プロジェクトを立ち上げているという人もいるでしょう。

サイバーセキュリティ（Cyber Security:コンピュータやインターネットが作る空間に関する安全保障）も言葉としてはよく聞きますし、企業や行政府等からの情報漏洩があったというニュースもよく報道されています。

DX とは何か、サイバーセキュリティ（以後 CS と略します）とは何か、その概要を各種資料よりの引用などからお示しし、監査役としてそれらにどう対応し、どう振る舞っていったらいいのか考える材料が提供できればと思います。

なお、引用した文献は本報告末尾の別表に番号付きで載せているものとなっています。引用の中には問題提起者が勝手に注意書きを付加しているところもありますので、すべて原文通りではないことをお断りしておきます。また、ウェブサイトからの引用については多種多様であり記事名やサイト名の表示は省略させていただきました。

○ＤＸとＣＳの共通点と相違点

どちらも IT、ICT、IoT、AI、デジタル化、といった先端的なテクノロジーの概念や技術を使うことでは共通です。DX は将来に向かって企業のビジネスモデルや事業を変革しようとする攻めの概念として、CS はどちらかというと（DX を進めるために）情報漏洩や経済的被害の発生リスクを減らすための守りの概念として使われることが多いです。

○ＤＸとＣＳの国内における源流

21 世紀の始めである 2001 年 1 月に通称 IT 基本法（正式名称：高度情報通信ネットワーク社会形成基本法）が施行され、IT 社会構築のための基本理念・体制についての基本的な枠組みを作り、政府としての重点計画を策定することとされました。同じ月に政府としての情報通信戦略「e-Japan 戦略」（公表文書 1）が策定されています。この時点では DX はもちろん CS も、セキュリティの言葉さえもありませんでしたが、セキュリティについては 2005 年 4 月に内閣官房情報セキュリティセンター（NISC）が設立され体制整備が始められました。

第１章　ＤＸ（デジタルトランスフォーメーション）

１．ＤＸの定義

DX の言葉を世界で初めて使ったのは 2004 年、スウェーデンのエリック・ストルターマン教授らだと言われています。このときは「IT の浸透が人々の生活をあらゆる面でより良い方向に変化させる」という単純なものでした。日本では 2018 年 9 月に経産省が発表した「DX レポート」（公表文書 5）により経済界に DX の言葉が広まったと言われています。ここでの定義は次に引用するように、詳しいながら少々わかりにくいものになっています。

「企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第３のプラットフォーム（クラウド、モビリティ、ビッグデータ/アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネスモデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること」

経産省はその後 2019 年 7 月に公表した「DX 推進指標とそのガイダンス（公表文書 7)」の中では定義を次のようにもう少しわかりやすくしました。

「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位を確立すること」

ある書籍（参考図書①）ではかなり簡略化し、「デジタルを使って自らを変革し、圧倒的な競争力を身につけること」と定義しており、ほかにも独自の定義や説明はあふれていますが、直上に挙げた経産省の定義が必要十分なように思われます。

２．ＤＸの現状

⑴著名な世界の DX の成功例

世界で最も DX が進んだ企業としてよく言及されるのは GAFA（Google, Apple, Facebook, Amazon）。巨大 IT 企業あるいはプラットフォーマーと呼ばれますが、platform（原義の「台」から転じて生活やビジネスに不可欠なインフラ的な製品・サービス）を提供する者、という意味でのプラットフォーマーは和製英語です。他にも DX の成功企業として規模はそこまで大きくないですがウーバー（配車）やエアビーアンドビー（民泊）も有名です。

⑵日本企業のＤＸは遅れている

日本企業でもウーバーイーツや LINE、メルカリなど DX 先進企業が出てきていますが、日本全体としてはどうなのでしょうか。

2020 年 12 月に経産省は先に触れた 2018 年の DX レポート後の報告として、「DX レポート 2（中間報告書)」（公表文書 9）を公表しました。その中で書かれていますが、先

に経産省が取りまとめた「DX 推進指標」（公表文書 7）の企業による自己診断結果を2020 年 10 月までに提出した約 500 社分を分析した結果、うち約 95%が DX 未着手か散発的に実施にとどまっており、残り 5%だけが部門横断的に推進したり持続的に実施している企業となりました。自己診断するくらいの企業ですから DX に対する意識は一般より高いと考えれば、日本企業全体でみれば状況はもっと悪いかもしれません。

ここで私的な疑問を差し挟みます。日本企業の DX は遅れている、という命題を真とするためには、他国の DX はもっと進んでいるという事実をもって比較して欲しいところです。その答えの一端として米国の例は「DX レポート」内で説明されています。全米取締役協会（NACD: National Association of Corporate Directors）が発行しているガイドラインを CEO は守る必要があり、その中に IT システムやサーバーセキュリティの項目があるので、CEO は自らその現状を把握して将来ビジョンを示さないといけないという非常に厳しい仕組みがあるので納得できます。では他の国はどうなのか、何かランキングのようなものはないのかと思って探してみました。すると JETRO（日本貿易振興機構）のウェブサイトにスイスの国際経営開発研究所（IMD: International Institute for Management Development）という、MBA プログラムで世界でも高い評価を受けている機関が毎年発表している「世界デジタル競争力ランキング 2020」の記事が載っていました。

このランキングは、デジタル技術を政府や企業がどれだけ積極的に活用しているかを示しており、1)知識・ノウハウ、2)技術開発の環境、3)将来への準備、の 3 項目で 63 の国と地域を対象に評価しています。首位から 5 位までは、米国、シンガポール、デンマーク、スウェーデン、香港となっており、東アジアでは韓国が 8 位、台湾 11 位、中国 16 位ですが、日本は 27 位となるほど確かに低くなっています。

３．ＤＸの推進政策

⑴ Society 5.0 と未来投資戦略

唐突に Society 5.0 が出てきたように思うかもしれません。この言葉は元々「科学技術基本法（1995 年 11 月施行、2021 年 4 月「科学技術・イノベーション基本法」として改正施行）」に基づき 5 年ごとに改定される「科学技術基本計画」の第 5 期（2016～2020 年度）（2016 年 1 月 22 日閣議決定）(公表文書 2)に登場しました。これまでの社会が 1 狩猟、2 農耕、3 工業、4 情報と進んできて今度は 5 デジタル化、簡単に言うと、サイバー（仮想）空間とフィジカル（現実）空間を高度に融合させた社会へ向かおうとすることです。広い意味ではこのデジタル化の中に国内では DX や既に CS の概念が含まれていたと言えます。サイバー空間はビッグデータと AI が占め現実空間に価値を提供するイメージです。所管は文部科学省（MEXT）になりますが、関連して Society 5.0 の実現に向けた改革のために「未来投資戦略 2017」が 2017 年 6 月に閣議決定され（公表文書 3)、経産省や産業技術総合研究所、経団連もそれぞれがレポートを公表しています。

未来投資戦略の中には Society5.0 と同様にまだ DX の言葉は出てきていませんが、サイバーセキュリティの言葉は登場しています。Society5.0 の実現のために次の 5 つの戦略分野が掲げられていますが、いずれも手段として、IoT、ビッグデータ、AI などを取り入れようという方向性を示しています。①健康寿命の延伸　②移動革命（自動運転、

無人飛行機・船など）の実現　③サプライチェーンの次世代化（革新的で無駄のない供給体制）　④快適なインフラ・まちづくり　⑤フィンテック（情報技術を駆使した金融サービス）

⑵ DX レポート

先に DX の定義のところで触れた 2018 年 9 月の「DX レポート」（公表文書 5）の中身を簡単にご紹介します。このレポートには「～IT システム「2025 年の崖」の克服と DX の本格的な展開～」という副題がついています。

ここでは、企業が DX によりビジネスをどう変えるかという経営戦略の方向性を定めていく課題を取り上げるとともに、既存の IT システムを巡る問題を解消しない限りは、新規ビジネスを生み出しかつ俊敏にビジネスモデルを変革すること、すなわち DX を本格的に進めることは困難であると指摘しています。それが副題に言う「2025 年の崖」であり、日本企業が複雑化・老朽化・ブラックボックス化した既存システム（＝レガシーシステム）が 2025 年まで残存した場合、経済損失が年間 12 兆円（現在の約 3 倍）にのぼる可能性があると試算しています。この試算は独立行政法人 情報処理推進機構（IPA: Information-technology Promotion Agency, Japan）が 2016 年 2 月に公開したまとめと一般社団法人日本情報システム・ユーザー協会（JUAS: Japan Users Association of Information Systems）が 2016 年 5 月に公表した「企業 IT 動向調査報告書 2016」を元にされています。

この DX レポートは副題に「2025 年の崖」という象徴的な言葉を用いて既存のシステムの問題を強調しましたが、もちろんそれだけはなく今後の DX の本格的な展開のために現状の課題や対応策への議論の結果も示しています。企業をユーザ企業とベンダー企業に分け、ユーザ企業の中の経営層・事業部門・IT 部門の関係と問題、人材の課題を挙げるとともに、ベンダー企業にある人員逼迫と顧客への提供価値高度化の課題、そしてユーザ企業とベンダー企業の丸投げ的な関係を排した契約手法や価値提供と価値評価の関係構築を提言しています。特にユーザ企業側の経営層が DX を実現するために押さえるべき事項や方法論については「ガイドライン」を策定することを提言しました。

⑶ DX 推進ガイドライン

「DX レポート」の提言にしたがって 2018 年 12 月に公表されたガイドラインです(公表文書 6)。レポートではなくガイドラインとして、企業に具体的な施策の指針を与えている関係で、より政策的なものになっています。

ガイドラインの「1 はじめに」では次のような認識を述べています。

「DX レポートにおける提言を受け、DX の実現やその基盤となる IT システムの構築を行っていく上で経営者が押さえるべき事項を明確にすること、取締役会や株主が DX の取組をチェックする上で活用できるものとすることを目的として、本ガイドラインを策定した。」

また、本ガイドラインは企業と投資家の建設的な対話を促すために経産省が 2017 年 5 月に策定した「価値協創のための統合的開示・対話ガイダンス」（価値協創ガイダンス）（公表文書 4）における基本的な考え方にも沿っており、DX 推進に当たっての視点を整

理したものとして、「価値協創ガイダンス」と併せて参照することが期待される、とあります。
「価値協創ガイダンス」は企業と投資家を繋ぐ「共通言語」であり、企業にとって投資家に伝えるべき情報（経営理念、ビジネスモデル、戦略、ガバナンス等）を体系的・統合的に整理し情報開示や投資家との対話の質を高めるための手引きです。IT・ソフトウエア投資がその戦略の項目の一つとなっていて、DX 実行の一助となることが期待される、とあります。

ガイドラインの中身は、次のような構成になっています。
（1）DX 推進のための経営のあり方、仕組み
　1．経営戦略・ビジョンの提示
　2．経営トップのコミットメント
　3．DX 推進のための体制整備
　4．投資等の意思決定のあり方
　5．DX により実現すべきもの：スピーディな変化への対応力
（2）DX を実現する上で基盤となる IT システムの構築
（2)－1 体制・仕組み
　6．全社的な IT システムの構築のための体制
　7．全社的な IT システムの構築に向けたガバナンス（システムの全社最適化他）
　8．全社的な IT システムの構築に向けたガバナンス（ベンダーに丸投げしない）
　9．事業部門のオーナーシップと要件定義能力
（2)－2 実行プロセス
　10. IT 資産の分析・評価
　11. IT 資産の仕分けとプランニング
　12. 刷新後の IT システム：変化への追従力

⑷「DX 推進指標」とそのガイダンス

2019 年 7 月、経産省は先の「DX レポート」の提言を踏まえ、「DX 推進指標」を策定しました（公表文書 7)。上記「DX 推進ガイドライン」の２つの柱、「（1）DX 推進のための経営のあり方、仕組み、（2）DX を実現する上で基盤となる IT システムの構築」について、DX の推進に向けたアクションをとっていくための気付きの機会を提供するものとして、この指標は策定されました。（1）（2）のそれぞれに定性指標と定量指標の項目を設定し、経営者が自ら回答すべきキークエスチョンと経営者が経営幹部、事業部門、DX 部門、IT 部門等と議論をしながら回答するサブクエスチョンから構成されています。[別添図表１]

定性指標については成熟度レベルをレベル０からレベル５の間で判定し、定量指標については会社が自ら設定した目標に対する進捗度を算出するものとして、５ページにわたる詳細な「DX 推進指標（本体)」を用意しています。
経産省は現状の課題として次の３つが指摘されていると言い、その課題を経営幹部、事業部門、DX 部門、IT 部門など関係者が共有し、アクションにつなげていくことが不可欠であるため、「DX 推進指標」により自己診断を基本としながら DX を実現していく

ことを想定しています。この自己診断を経産省に提出したものが２．⑵の日本企業の DX 進展度を見る統計の元になりました。

課題 (1)「顧客視点でどのような価値を創出するかビジョンが明確でない」
課題(2)「号令だけでは経営トップがコミットメントを示したことにならない」－具体的な仕組みとして、組織を整備し権限を委譲しているか、適切な人材・人員をアサインしているか、予算を十分に配分しているか、プロジェクトや人事の評価の仕方を見直しているか、必要な人材の育成・確保を行っているかといったことが必要になる。
課題(3)「DX による価値創出に向けてその基礎となる IT システムがどうあるべきか、認識が十分とは言えない」－DX を進める基盤として IT システムに求められる主要な要素である３点、ⅰ)データをリアルタイム等使いたい形で使えるか、ⅱ)変化に迅速に対応できるデリバリースピードを実現できるか、ⅲ)データを部門を超えて全社最適で活用できるか、を満足するかが求められています。IT システムの話になると経営者は IT 部門任せにしてしまうケースが多く、経営者がリアルな認識と必要な打ち手を講じていくことが不可欠である。

このガイダンスで監査役が注目すべき項目と思えるのは、末尾近くに「DX 推進における取締役会の実効性評価項目」が付属していることです。これは、コーポレートガバナンス・コードの原則 4-11 補充原則③において「取締役会は、毎年、各取締役の自己評価なども参考にしつつ、取締役会全体の実効性について分析・評価を行い、その結果を開示すべきである。」とされているところに関連して、経産省はこの「取締役会の実効性評価」に活用できるものとして策定したと述べています。

DX 以外の項目の取締役会の実効性評価とのバランスはどう取るのかという問題はありますが、また DX に触れた開示例があるのか寡聞にして知りませんが、監査役が関心を持つ理由が十分にあると考えられます。

⑸ DX 認定制度/DX 銘柄と DX 投資促進税制

①DX 認定制度

2020 年 5 月に DX に向けた準備状況を経産省が企業の申請に基づき評価して認定したら公表する「DX 認定制度」が作られました。DX 認定制度は経営者がデジタル技術を用いたデータ活用によって自社をどのように変革させるかを明確にし、実現に向けた戦略を作るとともに企業全体として必要となる組織や人材を明らかにしたうえで IT システムの整備に向けた方策を示し、さらには戦略推進状況を管理できる準備ができている状態（DX-Ready）の事業者に対して経産省が認定を付与するという制度です。したがって DX の成果や実績が出ていることが必要なわけではなく、また業種や企業規模の制限もありません。DX 認定制度は「情報処理促進法（正式名：情報処理の促進に関する法律)」に基づいて付与される公的な認定制度です。具体的には国が策定した「情報処理システムの運用管理に関する指針」を踏まえて、DX に向けた優良な取り組みを行う事業者を申請に基づいて認定します。認定の基準は経産省令に定められており、実際の認定審査事務は IPA が行っています。DX 認定制度と次の⑹で紹介するデジタルガバナンス・コードとは対応する関係にあります。

②DX 銘柄

2020 年 8 月に経産省と東証が共同で「デジタルトランスフォーメーション銘柄(DX 銘柄)2020」を発表しました。これは 2015 年から毎年「攻めの IT 経営銘柄」として選定してきたものを衣替えしたものです。東証に上場している企業の中から DX を推進するための仕組みを社内に構築し優れたデジタル活用の実績が表れている企業を「DX 銘柄」として業種区分ごとに選定したものです。DX 銘柄の選定は 6 つの項目（ⅰビジョン・ビジネスモデル、ⅱ戦略、ⅲ組織・制度等、ⅳデジタル技術の活用・情報システム、ⅴ成果と重要な成果指標の共有、ⅵガバナンス）と財務指標についてスコアリングした後に評価委員会の最終選考を経て決定されます。選ばれた会社は日本の先進企業とのお墨付きを得たことになります。

2021 年 6 月 7 日には DX 銘柄 2021 などの発表があり、「DX 銘柄 2021」28 社と、DX 銘柄に選ばれなかった企業中総合的評価が高かった企業、注目されるべき取り組みを実施している企業である「DX 注目企業 2021」20 社が示されました。さらに今年は新型コロナウイルス感染症（COVID-19）の影響に対する優れたデジタル対応の取り組みを実施した企業として「デジタル×コロナ対策企業」11 社が選定されました。
なお、DX 銘柄の中で特に優れた取り組みを行った企業に選定される「DX グランプリ 2021」には日立製作所と SRE ホールディングス（ソニー傘下の不動産会社）の 2 社が選ばれています。

③DX 投資促進税制、DX 認定ポータル

認定を基盤に関連投資額に対する法人税等の減税を可能とする「DX 投資促進税制」が 2021 年度から設けられています。こちらのほうが直接的な税金優遇というメリットが得られます。これは「産業競争力強化法」の改正により法的根拠を与えられています。

2021 年 4 月には認定事業者数が急増しており多くの大企業が含まれていることから本税制の利用を視野に入れた大企業もありそうです。認定事業者は IPA のウェブサイト上の「DX 認定ポータル」のページで毎月公表され、企業名を検索することもできるようになっています。

⑹ デジタルガバナンス・コード

直接的には 2018 年 9 月の DX レポートを受けて、DX を本格的に展開していくには、経営トップのコミットメントの下で、顧客、投資家、従業員、取引先、地域社会等のステークホルダーへの説明責任を果たし評価されることが必要という認識に基づき、企業の DX の取組みにおける行動原則となるデジタルガバナンス・コードを経産省らが主体となって 2020 年 11 月に策定しました（公表文書 8)。したがって同じく「コード(code)」ー直訳すれば「規則」もう少し意訳すれば行動原則と外部への責任ーであるスチュワードシップ・コードやコーポレートガバナンス・コードとは策定主体が異なりますが、ステークホルダーを意識しているという意味では類似のものと言えるでしょう。

内容としては情報処理促進法に対応して以下の「柱立て」それぞれについて、「基本的事項（柱となる考え方と認定基準)」「望ましい方向性」「取組例」を記述したものなって

います。「DX 認定制度」はこの「基本的事項」と連動して認定する仕組みになっており、「望ましい方向性」と「取組例」は「DX 銘柄」に連動するものとなっています。
[別添図表 2（下段）]

（デジタルガバナンス・コードの柱立て）
1. ビジョン・ビジネスモデル
2. 戦略
  2-1. 組織づくり・人材・企業文化に関する方策
  2-2. IT システム・デジタル技術活用環境の整備に関する方策
3. 成果と重要な成果指標
4. ガバナンスシステム
（この中でサイバーガバナンスシステムには柱となる考え方の中に「経営者は、事業実施の前提となるサイバーセキュリティリスク等に対しても適切に対応を行うべきである。」とあり、認定基準の中に、「サイバーセキュリティ経営ガイドライン」（公表文書 20,21）等に基づき対策を行い、セキュリティ監査（内部監査を含む）を行っていることの説明文書等が提出されること、中小企業においては、SECURITY ACTION に基づ
き自己宣言（二つ星）を行っていることを確認する方法でも可とする、とあります。

⑺ DX レポート 2

経産省が公表した 2020 年 12 月の DX レポート 2（公表文書 9）では、2018 年 9 月の DX レポート後の進展状況とコロナ禍により高まった DX の緊急性を示し、民間企業の事業変革のために取るべきアクションと、それをサポートする政府の政策について提言をしています。エグゼクティブサマリから抜粋して（一部加工）紹介します。

『2018 年の「DX レポート」から 2 年が経過した現在でも⑵で述べたように日本企業の DX への取り組みは「始めている企業」と「何もしていない企業」に 2 極化しつつあり、後者が圧倒的に多い状況である。当該レポートのメッセージは正しく伝わらず「DX とはレガシーシステムの刷新」あるいは現時点で競争優位性が確保できていればこれ以上の DX は不要である、等の本質ではない解釈が是となっていたのではないか。新型コロナウイルスが猛威を振るった影響に柔軟に対応できた企業とできなかった企業の差が拡大していいて、デジタル競争における勝者と敗者の明暗がさらに明確になっていくことになろう。企業がレガシー文化から脱却し変化に迅速に適応し続けるためには、DX 推進という変革に向けて関係者間での共通理解の形成や社内推進体制の確立といった変革への環境整備に今すぐ取り組む必要がある。その認識のもと、企業が取り組むべきアクションを具体的に示すことにより変革の加速を目指す。』

そのアクションを「直ちに、短期、中長期」の 3 つの時間軸に分けて挙げています。
ⅰ)直ちに
・業務環境のオンライン化
・業務プロセスのデジタル化
・従業員の安全・健康管理のデジタル化

・顧客接点のデジタル化
・DX の認知・理解

ⅱ)短期

（DX 推進体制の整備）
・経営層、事業部門、IT 部門の共通理解の形成
・CIO/CDXO の役割・権限等の明確化
・遠隔でのコラボレーションを可能とするインフラ整備

（DX 戦略の策定）
・DX 推進状況の把握

ⅲ)中長期
・デジタルプラットフォームの形成

（産業変革のさらなる加速）
・変化対応力の高い IT システムを構築
・ベンダー企業の事業変革
・ユーザー企業とベンダー企業との新たな関係

（DX 人材の確保）
・ジョブ型人事制度の拡大
・DX 人材の確保

ここまでの「DX レポート」「DX 推進ガイドライン」「DX 推進指標」「DX 認定制度」「DX 銘柄」「デジタルガバナンスコード」の各施策の関係と展開を図示したものが載っていますので引用します。

［別添図表２（上段）］

⑻ デジタル社会形成基本法

2021 年 5 月 12 日に国会でいわゆるデジタル改革関連 6 法案が可決成立し施行日が 9 月 1 日とされました。中心となるのはデジタル社会形成基本法とデジタル庁設置法であり、個人情報保護法の改正やマイナンバー法（正式名：行政手続きにおける特定の個人を識別するための番号の利用等に関する法律）の改正、押印を求める各種手続きについて押印を不要とし電磁的方法による書面交付を可能とする内容が含まれています。押印の不要化は新型コロナウイルス感染症の蔓延によるテレワークの推進から生まれた改革とも言え、また内閣府へのデジタル庁の設置は遅まきながら 2016 年 1 月に打ち出された Society5.0 の実現に向けた中央指令組織の実現を具体化したと言えるものなのかと思います。なお、2001 年 1 月に施行されたいわゆる IT 基本法（正式名称：高度情報通信ネットワーク社会形成基本法）は廃止されデジタル社会形成基本法に置き換えられることになります。格調高い日本語の法律が失われることを問題提起者は残念に思います。

４．ＤＸへの疑問

ここまでで出そうな少し極端なものも含めて懐疑的な反応を想像してみます。答えることは難しそうですが、現実的には DX の入口前で止まるのでなく DX 推進を一度考えた上で、あるいは考えながら取り組むことかもしれません。

・本当に必要なのか。政府に脅され踊らされるだけではないのか。
・どんな業種にもどんな規模の企業にも必要なのか。たとえば接客業や建設業で従業員 20

人以下の企業にも必要なのか。もともとIT基盤のない企業には不要なのではないか。
・ソフトウエアのベンダーに対する提言もあるが、経産省のその業界担当部署が当該産業育成のために全体推進政策を作り上げたのではないか。
・DXに成功した企業がDXに積極的でなかった企業より確実に競争に勝つと言えるのか。企業競争力の一要素でしかないのではないか。
・よく検討した後に我が社にはDXは不要である、という結論を出すことは認められないのか。その会社は競争力を失うと判断できるのか。また投資家もそう判断するのか。

５．経営者がなすべきこと（私見入り）

これまでDXに対する基礎的な知識や資料を紹介してきましたが、監査役のDXへのあるべき対応を考える前に、経営者がまずなすべきことを挙げてみたいと思います。参考文献に書いてあることの抜粋であったり、私の考えであったりが混在しています。

・DXに対する認識を深めること
・自社の現状を把握すること
・デジタルガバナンス・コードへの対応を具体化
・業務フローの無駄と非効率の洗い出し
・現在のITシステムの維持にかかっている費用と今後の開発費用の算出
・企業内検索エンジン作成など手軽で便利な開発の可能性検討
・将来の自社のビジネスモデル想定とそのためのDX推進方針の立案
・ITシステムの部分最適から全体最適への開発方針作成
・親会社がある場合、親会社のDX方針の理解とどこまで協力し傘下に入るかの検討
・親会社があっても自社独自のDXの必要性の有無を確認

６．監査役に望まれる態度と実行行為（私見）

上で挙げた経営者のなすべきことに対応して監査役がどうするべきかを考えてみます。監査役の直接の監査対象である経営者や取締役個々に対しての態度という意味で書きますが、上で挙げた項目を直接経営者に実行の提案をすることのほかに、経営者のなすべきことのうち執行行為に当たらない、知識や意義の深掘りを監査役も行うということもありかもしれません。

・経営者に対するDXに関する理解の促進
・取締役がDXの理解を進めず実現を目指さなくても善管注意義務違反は問えない
・従業員とDXに関連する会話の機会作りとアイデア収集
・親会社や一般他社の監査役等からのDXに関する情報収集
・デジタルガバナンス・コードへの対応を提言
・DX認定制度適用の申請を提言
・外部セミナーや外部相談窓口、外部ベンダーなどからの情報収集を提言、などなど

第２章　ＣＳ（サイバーセキュリティ）

１．ＣＳの定義

サイバーセキュリティはデジタル大辞泉（小学館）では次のように説明されています。

「サイバー攻撃に対する防御行為。コンピューターへの不正侵入、データの改竄（かいざん）や破壊、情報漏洩、コンピューターウイルスの感染などがなされないよう、コンピューターやコンピューターネットワークの安全を確保すること。」

ではサイバー攻撃とは何でしょう。日本大百科全書（小学館）には、次のように書かれています。

「インターネットを通じ、企業などのシステムを攻撃する行為。標的とする団体や個人の持つサーバーや個別のパソコンに不正ログインし、そのシステム内のデータを改竄、破壊、盗むなどするのが一般的である。攻撃対象を社会基本インフラや政府機関としたものは特にサイバーテロとも呼ばれる。」

公的なものでは、2015 年 1 月に施行されたサイバーセキュリティ基本法の第 2 条に次の定義規定があります。

「この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。」

もう少し簡略化された公式文書での定義には経産省の「サイバーセキュリティ経営ガイドライン」（公表文書 20, 21）の用語集において、「サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。」というのがあり、こちらのほうが先のデジタル大辞泉の説明とともにわかりやすい部類かもしれません。

２．ＣＳに関する現状と事件

⑴サイバー攻撃は増えている

普通に考えて今の世の中でサイバー攻撃が増えないわけはないと思いますが、ではどのくらいの勢いで増えているのか、しかも被害が大きくなりそうな攻撃方法が増えているのか、良さそうな統計はすぐには見当たりません。ベンダー企業の宣伝ではないかと言えるようなものもネット空間には多く見られます。

信頼できそうな政府系の統計として「NICTER 観測レポート 2020」を挙げてみます。調査・公表の主体は、国立研究開発法人 情報通信研究機構（NICT: National Institute of Information and Communications Technology）、2004 年に通信総合研究所と通信・放送機構が統合して設立された総務省所管の研究所です。サイバー攻撃関連通信の観測を NICTER(Network Incident analysis Center for Tactical Emergency Response)と呼ばれる観測・分析システムにより 2005 年から続けてきており、毎年レポートを発表しています。

2021 年 2 月に発表された最新版によると、2011 年から 2020 年の 10 年で「ダークネット観測網」という、インターネット上に研究所が構築した大規模サイバー攻撃観測網

の範囲に届いた年間パケット数は、1 IP アドレスあたりで約 45 倍（約 4 万→約 180 万）になっています。この IP アドレスは機構が管理する未使用のものなので、無差別に送られてきたパケットはスキャン（探索）や攻撃が目的とみなせるという仕組みです。
[別添図表 3]

⑵日本年金機構からの個人情報大量流出事件

サイバーセキュリティが大きく破られた事件として国内で始めに有名になったのは、サイバーセキュリティ基本法が施行された年 2015 年の 5 月に起きた、サイバー攻撃による日本年金機構からの大量（125 万件）の個人情報流出です。これについては内閣サイバーセキュリティセンター（2015 年 1 月に従来の内閣官房情報セキュリティセンターを権限強化して改組設立。略称は同じ NISC: National center of Incident readiness and Strategy for Cybersecurity）が 3 ヶ月後の 8 月 20 日に公表した原因究明調査結果（公表文書 10）において、「標的型攻撃（メール）からの有効な遮断機能を有すると考えられるインターネットに接続していない業務系から、インターネットに接続している情報系に個人情報を移して取り扱っていたため、標的型攻撃を受けるリスクに当該個人情報をさらす結果となった」と記載しています。

この報告とほぼ同時の 2015 年 8 月 21 日には有識者を集め厚生労働省によって組織された「日本年金機構における不正アクセスによる情報流出事案検証委員会」による検証報告書が公表されました。内容については次の新聞記事（2015 年 8 月）を参照してください。とにかくこの事件はさまざまな問題を投げかけており、その後今度は総務省に設計・調整・調達に問題があったと指摘されたという新聞記事（2019 年 12 月）も参考になると思うので続けて載せます。

<日本経済新聞電子版　2015 年 8 月 21 日>

サイバー攻撃を受けて日本年金機構の個人情報が流出した問題で、有識者で構成する検証委員会（委員長・甲斐中辰夫元最高裁判事）は 21 日、機構を監督する厚生労働省も「サイバー攻撃への対応や意識が不十分だった」とする報告書をまとめた。機構への攻撃が始まる前の 4 月に、厚労省が手口の似たサイバー攻撃を受けていたことも新たにわかった。
検証委は、20 日に調査報告書を公表した機構とは別に、第三者の立場から流出問題の原因や再発防止策をまとめた。厚労省と機構は報告書の内容を踏まえて、関係者の処分を検討する。

報告書によると、4 月 22 日に厚労省年金局などが標的型メールを受信。端末がウイルス感染し、約 2 時間後にネットワーク環境から遮断した。これについて内閣サイバーセキュリティセンター（NISC）から「同種のウイルスに感染した場合、被害が大きくなる可能性がある」との注意を受けていた。
だが、厚労省は 5 月 8 日に機構が似た攻撃を受けた際にも、機構に情報提供しなかった。この段階で情報提供しても一連の情報流出がすべて防げたかは不透明だが、検証委は「（危機感を）意識することはできたはず」と分析している。

報告書では、厚労省の情報セキュリティーを担当する専任の職員が実質 1 人しかいなかったことも指摘、「到底十分な体制とは言いがたい」と批判した。サイバー攻撃を受けた機構の LAN システムの担当部署が、厚労省内で不明確になっている点も問題視し「監督官庁としてあり得ない」と断じた。

<日本経済新聞電子版　2019 年 12 月 5 日>　（問題提起者が内容を編集）

サイバー攻撃から機密情報を守るにはインターネットとの完全隔離が必要だ。こうした方針の下、総務省は政府の IT（情報技術）基盤「政府共通プラットフォーム（PF）」上で、高セキュリティーを確保した「セキュアゾーン」と呼ぶ専用区画を 2017 年に構築した。ところが利用実績が全くなく、わずか 2 年で廃止した。対策があまりに強固すぎて利用する側の要件に合わなかった。拠出した予算 18 億 8709 万円は無駄遣いに終わった。［別添図表４］

総務省がセキュアゾーンをひっそりと廃止した事実は会計検査院の検査で明らかになった。会計検査院は 19 年 10 月 28 日、一連の経緯と問題点を指摘した報告を公表した。報告では「計画を作る前に実需を把握し費用対効果を検討するべき」などと指摘し、再発を防ぐための是正改善を要求した。

どの省庁も利用しないセキュアゾーンが、なぜ作られてしまったのか。セキュアゾーンを構築したきっかけは、15 年 5 月に発生した日本年金機構へのサイバー攻撃に遡る。職員を狙った標的型メール攻撃によって機構内のパソコンがマルウエア（悪意のあるプログラム）に感染。外部からの遠隔操作により、機構が運用する社会保険オンラインシステムから最大 125 万件の個人情報が流出した。

事件を受け、政府高官や有識者からなる内閣官房の「サイバーセキュリティ対策推進会議」が動いた。同年夏の会合で議長を務めた杉田和博官房副長官（当時）が「行政システムで機微な情報を扱う部分とインターネットなどを分離する」などの対策を指示した。

この方針を受けて、政府は新たなセキュリティー対策の導入を具体化した。15 年末にまとめた補正予算案で、国や自治体、独立行政法人が実施する様々なセキュリティー強化策として 520 億円の拠出を盛り込んだ。

省庁横断で多数の行政システムが稼働していた政府共通 PF のセキュリティー対策費用もこの中に含めた。職員が利用する端末も含めてインターネットとの分離を徹底した区画を設ければ、議長指示通りの高度なセキュリティー強化策が実現できる。総務省はこう考え、政府共通 PF の中に特に機微な情報を扱う専用区画を設ける方針を固めた。16 年 1 月の補正予算成立から、この方針に従う「セキュアゾーン」の要求仕様作りに着手した。

並行して各省庁に利用意向を聞いた。厚生労働省が感染症の情報を扱うシステムなど 3 つと、農林水産省が企業情報を扱うシステムについて利用希望があると分かった。総務省は「実需はありそうだ」と判断した。

セキュアゾーンは利用端末をゾーン内の仮想パソコンに限定し、外部からは画面転送方式で仮想パソコンを遠隔操作する仕様にした。利用端末を踏み台にした攻撃による情報漏洩を封じるためだ。仮想パソコンと外部のデータ交換は禁止とした。さらに他の侵入経路を塞ぐため、原則として他の行政システムとは連携させない仕様にした。

事業者が決まり、16 年 10 月からシステム構築が本格化した。しかし 17 年 4 月の運用開始を前に、早くも暗雲が垂れ込める。

「機能に関する情報が不十分だ。利用するかどうかは回答できない」。16 年 12 月に総務省が厚労省に確認したところ、担当者からこう返答された。だがその後も総務省は厚労省へ詳しい説明をせず、総務省は最終的に厚労省という「大口顧客」を逃した。

そもそも総務省と厚労省には最初からボタンの掛け違いがあった。厚労省は利用意向の調査時に、セキュアゾーン利用の条件として「日常業務で職員のパソコンにデータをダウンロードできる必要がある」と明言していた。総務省の担当者はこの機能を実現しない方針だったにもかかわらず、その説明をせず、議論や調整の機会も持たなかった。会計検査院は総務省の説明や各省庁との調整が不十分だったと断じた。

セキュアゾーンを担当した総務省行政情報システム企画課は、政府共通 PF など省庁横断の行政システムを担う。本来は IT 調達の手本となるべき立場にもかかわらず、会計検査院から「ダメ出し」を受けた格好だ。

結局、セキュアゾーンは制約が強すぎて、その後も利用を希望する省庁は現れなかった。

政府が取り組む IT 調達のガバナンスにも問題があった。政府の IT 予算は内閣情報通信政策監（政府 CIO）の下で無駄な IT 投資を減らすために、様々な点検や助言を受ける体制に移行したはずだった。

しかし総務省は今回のプロジェクトについて「政府共通 PF の追加機能である」として、新規にプロジェクト計画書を作成しなかった。このため内閣官房などによる点検を受けずに予算が執行されてしまった。短期に執行する必要のある補正予算だったこともあり、事前の調査なども不十分なまま調達手続きが進んでしまった。

この調達を進めた当時の総務省の担当者らは現在、他部署に異動したという。現任の担当者は日経コンピュータの取材に「当時の作業状況は分からないが、システムへの需要や費用対効果を踏まえたシステム調達ができていなかった。大変反省している」と話した。

IT 予算を効率化する政府の調達改革は現在も進行中だ。20 年度からは内閣官房による IT 予算の一元化も始まる。だが、ずさんな IT 調達はまだ撲滅できていない実態が分かった。

一義的な責任は発注者の総務省にあるが、一方で受注したIT大手は途中で意見を述べたり軌道修正を提案したりできなかったのだろうか。今回の反省をどう生かすか。IT調達改革の真価が試される。

（日経コンピュータ　玄忠雄）［日経コンピュータ 2019年11月14日号の記事を再構成］

⑶その他のサイバー攻撃による被害の事例

年金機構の事件後の国内での主なサイバー攻撃の事例を列挙します。

・2015年11月　東京五輪組織委員会のウェブサイトにサイバー攻撃があり約12時間閲覧が不能になった(DDoS 攻撃)　→読みはディードス攻撃（Distributed Denial of Service attack)、複数のコンピュータから大量に、対象のウェブサイトやサーバーに対して過剰なアクセスやデータ送付を行うサイバー攻撃。
・2016年6月　i.JTB（JTBの子会社、2018年4月に親会社に吸収合併）の職員が利用する端末がマルウエアに感染しパスポート番号を含む個人情報が流出した可能性（標的型攻撃)
・2017年5月　国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）→ransom(身代金)を要求するもの。メールやウェブサイトからサーバーなどに侵入して勝手に暗号化して鍵をかけてしまい、解除するために金銭などを要求する。
・2018年1月　コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
・2020年　三菱電機やNEC等において防衛関連情報を含む情報が外部に流出した可能性が判明（不正アクセス）
・2020年　ドコモ口座経由で、不正に入手された口座番号・暗証番号等を使用した不正出金が判明（不正アクセス）
・2020年　カプコンがランサムウェアによる標的型攻撃を受け、個人情報等が外部へ流出した可能性が判明（ランサムウェア）

海外の同様の事例紹介は省略しますが、最近大きく耳目を集めたものとして、2021年5月に米国東海岸の燃料輸送を担うコロニアル・パイプライン社がランサムウェアによる攻撃を受け、東海岸の約半分の石油供給が5月7日から5日間にわたって停止に追い込まれた事件がありました。参考に次のnet newsを紹介します。

<BBC NEWS JAPAN 2021年6月8日>

アメリカ司法省は7日、サイバー攻撃を受けて先月5日間にわたり操業停止となった同国最大の石油パイプライン「コロニアル・パイプライン」がハッカーに支払った440万ドル（約4億8000万円）の身代金について、大半を取り戻したと発表した。

リサ・モナコ司法副長官は、連邦捜査局（FBI）がこのうち230万ドルに相当する63.7ビットコインを「発見・回収」したと説明した。

コロニアル・パイプラインのジョゼフ・ブラウント社長は、FBI の「迅速な仕事とプロ意識」が身代金の奪還に寄与したと感謝を述べた

「サイバー犯罪者を罪に問い、その活動を可能にしているシステムを阻害することが、将来の攻撃を防ぐ最善の方法だ」

同社のパイプラインは、東海岸で消費されるディーゼル、ガソリン、ジェット燃料の45%を供給している。サイバー攻撃により、供給は数日間阻害され、燃料不足が懸念された。

米当局は、犯行に及んだサイバー犯罪集団「ダークサイド」は東欧やロシアから運営されているとみている。

コロニアル・パイプラインは 5 月、「ダークサイド」によるランサムウェア（身代金ウイルス）を使った攻撃を受け、7 日から操業を停止。その後、操業再開の見込みが不透明だったことから、11 日に身代金を仮想通貨ビットコインで支払った。

ウォール・ストリート・ジャーナルによると、同社は仮想通貨ビットコインによる身代金支払いの見返りに、ハッカーに侵入されたシステムを解除するための復号ツールを受け取った。しかし、すぐにシステムを再起動するには至らなかったという。

ブラウント社長は「私は軽々しく（この決断を）下したわけではない。正直、このような人物にお金が渡るのを見るのは不愉快だった」と述べ、「ただ、この国にとって正しいことをした」と語った。

また、身代金を支払わなかった場合、システムの回復に数カ月かかる可能性もあり、攻撃による損害が数千万ドル単位になると予測したと話した。

米政府は過去に、企業がランサムウェア攻撃を受けた場合、さらなる攻撃につながる可能性があるため、犯罪者に金銭を支払わないよう勧告。セキュリティー対策の強化を呼びかけている。

ジーナ・ライモンド商務長官は 6 日、ジョー・バイデン大統領がこの問題について、今月予定されている米ロ首脳会談でウラジーミル・プーチン大統領と話をする予定だと述べた。

ダークサイドは 10 日、関与を認める声明を発表。「私たちの目的は金銭であり、社会で問題を起こすことではない」とし、「地政学には関わらないし、私たちの動機は（中略）どこの国の政府とも関係ない」と付け加えている。

BBC のジョー・タイディー・サイバー記者は、アメリカのランサムウエア攻撃との戦いにおいて、今回の件は大きな勝利だと解説。

ロシアなどから何のとがめもなくサイバー攻撃を仕掛けてくる犯罪者に向けての力強いメッセージになったと述べた。
（英語記事　US recovers most of Colonial Pipeline ransom）

３．ＣＳに関する政策

この報告書の冒頭部分「DX と CS の国内における源流」のところで述べた 2005 年 4 月の内閣官房情報セキュリティセンター(NISC)発足後、政府機関や重要インフラの防御体制の整備、人材育成、研究開発、国際連携などが進められました。この間経産省は 2009 年 6 月には「情報セキュリティガバナンス導入ガイダンス」（公表文書 19）を定めて企業経営者に情報流出やシステムダウン等の事故が発生することに備えるリスク管理の必要を唱えましたが、サイバー攻撃を想定したものではありませんでした。

⑴サイバーセキュリティ基本法

2015 年 1 月にはサイバーセキュリティ基本法が施行され、内閣官房長官を本部長とするサイバーセキュリティ戦略本部が事務局を NISC として組織され、NISC の大幅な権限強化とともに、サイバーセキュリティ戦略の策定・推進・政府機関の防御能力の強化、関連組織との連携強化などが行われることとなりました。そのほかに基本的施策として法に定められたものに、民間事業者及び教育研究機関等の自発的な取組の促進、我が国の安全に重大な影響を及ぼすおそれのある事象への対応、産業の振興及び国際競争力の強化、研究開発の推進、人材の確保、教育及び学習の振興・普及啓発、国際協力の推進等があります。

この法律の施行直後に先に挙げた日本年金機構における個人情報流出事案が発生するわけですが、標的型メールによる攻撃に対しての脆弱性が明らかになっただけでなく多くの教訓を残したものとなり、法改正して、特殊法人や独立行政法人も NISC の直接の監視・調査の対象に加えること、IPA への委託を拡大、情報処理安全確保支援士の国家資格新設、サイバーセキュリティ協議会の創設などが行われています。

⑵サイバーセキュリティ経営ガイドライン

2015 年 9 月にサイバーセキュリティ戦略本部が策定した「サイバーセキュリティ戦略」（公表文書 11）を踏まえて 2016 年 12 月に経産省（発行者は IPA）は「サイバーセキュリティ経営ガイドライン ver1.1」（公表文書 20）をまとめました。翌 2017 年 11 月には改定版の ver2.0（公表文書 21）を公表しています。本ガイドラインは、大企業及び中小企業（小規模事業者を除く）のうち、IT に関 する製品やシステム、サービス等を供給する企業及び経営戦略上 IT の利活用が 不可欠である企業の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3 原則」、及び責任者となる担当幹部（最高情報セキュリティ責任者(CISO）等)に指示すべき「重要 10 項目」をまとめたものです。

ver1.1 では対象企業を IT 関連企業に絞っていましたが ver2.0 ではその限定を取り去りました。経営者が認識すべき 3 原則と担当幹部(CISO 等)に指示すべき 10 項目について

も小幅な改訂を加えています。3 原則だけ紹介します。

1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

⑶企業経営のためのサイバーセキュリティの考え方

2016 年 8 月には NISC は企業の経営層を対象にサイバーセキュリティをより積極的な経営への投資と位置づけた自発的な取組みを促進するために「企業経営のためのサイバーセキュリティの考え方」（公表文書 13）を策定して普及に向けた取組みを開始しています。ここでは⑵で述べたサイバーセキュリティ戦略とそれを踏まえたサイバーセキュリティ経営ガイドラインと併せて経営層への認識期待と経営戦略を企画する人材に対しての実装のためのツールを示すことを目的にしていると述べられています。そして持つべき次の二つの基本認識をあげています。

1. サイバーセキュリティは利益を生み出しビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。
2. 全てがつながる社会においてサイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

また、次の三つの留意事項もあげています。

①情報発信による社会的評価の向上
②リスクの一項目としてのサイバーセキュリティ
③サプライチェーン全体でのサイバーセキュリティの確保

CS 実装に向けたツールとしてはまず企業を、CS に対応するレベル別に三つに分けた上でそれぞれに具体案を示しています。

まず、1)積極的な競争力の強化にセキュリティを活用する企業に対しては、セキュリティ品質の向上によるブランド価値の向上などを認識すべきとし、取組みを積極的に情報発信することや「IoT セキュリティガイドライン」（公表文書 12）の活用を挙げました。

次に、2)事業戦略へ CS を積極的に取り入れていない企業には、社会的な責任のもとにセキュリティ対策へ取り組むよう求め、既述⑵の「サイバーセキュリティ経営ガイドライン」を活用するよう促しています。

最後に、3)中小企業等でセキュリティの専門組織を保持することが困難な企業に対しては、消費者や取引先との信頼関係構築においてセキュリティ対策に取り組む必要があるとする一方、十分なリソースを確保できないケースもあることから、解決策としてセキュリティ対策を実施しているクラウドサービスの利用やリスクを転嫁する保険の活用などをツールとして挙げたほか、CS 相談窓口やセミナーの活用を提案するなど、具体的な方向性を提示もしています。

⑷中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドラインの初版は 2009 年に発行されました。同じ IPA が発行した上記⑵の 2017 年のサイバーセキュリティ経営ガイドライン第 2 版の改訂内容を反映して 2019 年 3 月に中小企業の情報セキュリティ対策ガイドラインの第 3 版（公表文書 22）が発行されました。対象はサイバーセキュリティ経営ガイドラインでは大企業及び中小企業（小規模事業者を除く）としていましたが、中小企業の情報セキュリティ対策ガイドラインは対象を中小企業及び小規模事業者に絞ったものです。さらに企業の中でも対象者を経営者向けと情報セキュリティを実践する層向けとの 2 部構成にして詳細な解説を記したものとなっています。

⑸最近のサイバー攻撃の状況を踏まえた経営者への注意喚起

経産省は 2020 年になって 4 月 17 日に「産業界へのメッセージ」（公表文書 23）、6 月 12 日にやたら長い表題ですが「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバーセキュリティお助け隊」）の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（公表文書 24）（以後「昨今の状況認識」と略します）、12 月 18 日には「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」（公表文書 25）と立て続けに文書を発表しました。

これらは、「2020 年に入ってから新型コロナウイルスの感染拡大に伴いテレワークの利用の急拡大など、サイバー空間を巡る環境が大きく変化していること。また、サイバー攻撃の手法の高度化・巧妙化が進むとともに、中小企業等のサプライチェーン上の弱点を起点とする攻撃の拡大が見られる。」（公表文書 25 から引用）という認識の下、企業やその関係機関等に対して注意点を伝え、サイバーセキュリティの取組の一層の強化を促しています。

経営者への注意喚起をする状況の認識については以下の 3 点を挙げます。

①中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり
②大企業・中小企業を問わないランサムウェアによる被害の急増
③機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃の深刻化

次にランサムウェアの事例などのサイバー攻撃の事例を紹介してから、次の認識による対応を経営者に呼びかけています。

①サイバー攻撃による被害が深刻化し、被害内容も複雑になっており、経営者の一層の関与が必要になっている
②ランサムウェア攻撃によって発生した被害への対応は企業の信頼に直接関わる重要な問題であり、その事前対策から事後対応まで、経営者のリーダーシップが求められる
③サイバーセキュリティを踏まえた事業のグルーバル・ガバナンスを構築する必要がある：海外拠点をシステム統合する際の留意点
④改めて（6 月 12 日に公表した「昨今の状況認識」に記した）「基本行動指針（共有・報告・公表）」に基づいた活動の徹底を（原文のママ）

ここで言う「基本行動指針」は次の３つです。

1)サプライチェーンを共有する企業間におけるサイバー事案に関する高密度な情報共有の実施

2)機微技術情報の流出懸念がある場合の経済産業省への報告

3)情報漏えい等の被害が取引先等不特定多数の関係者に影響するおそれがある場合における関係者の規制緩和の取組促進のための公表の実施

以上はいずれも経産省からの公表文書に基づくものですが、内閣官房の NISC も 2020 年 11 月 26 日に「ランサムウエアによるサイバー攻撃について【注意喚起】」という文書を発信し、特別な警戒感を示しています。

⑹情報セキュリティ監査制度

少し時間は遡りサイバーセキュリティの言葉もまだない時期に始まった制度を、サイバーセキュリティは情報セキュリティに包含されるものという認識に基づいて紹介します。2003 年 4 月から経産省は「情報セキュリティ管理基準」（公表文書 17）と姉妹版である「情報セキュリティ監査基準」（公表文書 18）の制度運用を開始しました。目的は企業などの組織体が効果的な情報セキュリティマネジメント体制を構築し適切なコントロール（管理策）を整備・運用するための実践的な規範の提示です。管理基準は国際標準規格（ISO）を基にしていますので ISO の追加・変更に合わせ、2008 年と 2016 年に改正が行われています。監査基準はそのままです。

監査基準は、情報セキュリティ監査業務の品質を確保し有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。ただ通常「監査人」といえば公認会計士を連想しますが、ここでは情報セキュリティ分野に知識と経験を持ち、JASA（Japan Information Security Audit Association：特定非営利活動法人（NPO）日本セキュリティ監査協会）の資格認定を得た「公認情報セキュリティ監査人：CAIS-Auditor)」のことを指します。

JASA が自らのウェブサイトでも述べています。古いですが 2002 年の総務省調査「情報セキュリティ対策の状況調査」によれば、情報セキュリティ監査を実施している割合は大企業で 20%、大学で 9%、中小企業で 7%などと低い状況でした。その理由としては監査を行う主体としては、監査の正当性を信じてもらえないという点、被監査主体としては、どのような効果があるか分からない、または誰に頼めば良いかわからないという点が最上位としてあげられています。

問題提起者がこの制度について不思議に思うのは、経産省の担当課が経営者への注意喚起などを次々と出している同じサイバーセキュリティ課であるのにこの制度を本気で普及・推進させようとしているのか疑問になるほど、ウェブサイト上でも情報が得にくいところです。また、総務省の上記 2002 年の調査以降は同じ質問を投げた調査がされているのかも探せませんでした。外部認証制度の性格として、ISO9001 の認証も産業界で一定の宣伝効果は持つものの、同等以上の内容の品質管理を自社で構築・運用しているところは外部認証は必ずしも必要ないということもあるかもしれません。そういう意味

では企業の内部で公式の情報セキュリティ監査と同等の監査を自ら実施するという方法も考えられると思います。

４．経営者の責務―CS の必要性の認識から―（私見入り）

CS の場合は、DX のようにそもそも一体それは何だろう、なぜ必要なのだろうという懐疑的なところから始まるのではなく、政府がいろいろ警鐘を鳴らし対応の指針を打ち出しているけれども、情報漏洩することやサイバー攻撃がどのくらい危険なことかという理解と問題意識から始まるものと考えられます。言い換えれば、上記３．⑵「サイバーセキュリティガイドライン」の 3 原則の始めに掲げられていた「サイバーセキュリティリスクの認識」から始まるものと考えられます。

次の段階として 3 原則の他の 2 つ、「サプライチェーン全体の対策」「サイバーセキュリティリスクについての関係者との適切なコミュニケーション」が必要になります。ただ、経営者が具体的な方策を含めてすべてを自身で実施することは現実的でないため、CISO 等の幹部(14 参照）への指示について行き届いたものとすることが求められることになります。

私見で小さくまとめると、結局のところ経営者はこうした政府や報道機関、ベンダー企業等の発するメッセージや情報に常に耳を傾け最新のサイバーセキュリティリスク対策を取ることを CISO に指示する必要があると思います。会社全体のリスクマネジメントの一部として、欠けることは許されないという意識が必要でしょう。

リスクマネジメントあるいは危機管理に話を広げると大変ですが、会社がマネジメントすべきリスクの一覧表を作るなら、サイバーセキュリティリスクは、自然災害、設備故障、労災事故などと同様にハザードリスクとして分類されると考えられます。したがってサイバー攻撃インシデントの発生確率の大小、損害（額）の大小を考慮した、あるいはそれらにかかわらず、事前の想定に基づいた予防策の実施（その中には初動対応、事後処理などを含めた「防災訓練」も有効と思われます）が必要になるということだと思います。

５．監査役に望まれる態度と実行行為（私見）

上で挙げた経営者のなすべきことに対応して監査役がどうするべきかは、基本的に第１章の DX のところで述べたのと同様と考えます。監査役の直接の監査対象である経営者や取締役個々に対しての態度という意味で、直接経営者にサイバーセキュリティ対策の実行の提案をすることのほかに、知識や意義の深掘りを監査役も自ら行うということもあると思われます。取締役の施策執行プロセスとして基本である経営判断の原則が守られているかはもちろんですが、その前段階の検討や基盤作りを確認したり促したりすることもしていいのではないかと思います。具体的な監査役の行動として考えられることを、DX で挙げたことと類似のことを含めて列記します。

・経営者に対する CS に関する理解の促進
・取締役が CS 対策をしない場合の善管注意義務違反は問えるか
・内部統制システムのうち「会社の損失の危険の管理に関する規程その他の体制」が CS を含めて構築・運用されているか、子会社についても同様にされているかの確認
・全社的リスクマネジメント（ERM）は整備運用されているか、その中に CS の項目は含

まれているかの確認
・従業員と CS に関連する会話の機会作りとアイデア収集
・親会社や一般他社の監査役等からの CS に関する情報収集
・サイバーセキュリティ経営ガイドラインの遵守を提言
・外部セミナーや外部相談窓口、外部ベンダーなどからの情報収集を提言
・中小企業であれば「中小企業の情報セキュリティ対策ガイドライン」による検討を提言、
などなど

○参考文献　（別添）政府の DX、CS に関連する公表文書一覧
○参考図書
①「今すぐ知りたい DX の基礎」日経 BP 社 2021 年 4 月発行
②「サイバーセキュリティ」谷脇康彦 著　岩波新書　2018 年 10 月発行

以　上