デジタルトラストを支える保証・第三者評価

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**加藤 俊直**

はじめに

「社会のデジタル化が加速している」。この文章が陳腐化してしまうくらいに、日々の社会生活は急速にデジタルに置き換わり、デジタル社会との情報のやりとりを行うことが当たり前の世界が到来しています。その一方で情報のセキュリティや情報を取り扱う組織の信頼性に対しては、社会全体として漠然とした不安や懐疑的な見方が払拭されていない状況にあります。

本稿では、デジタル社会において、リスクを測り、取捨選択し、対応し、確認し、発信するというのはどういうことなのかを考えます。昨今、注目を集めている委託先・サプライチェーンにおけるデジタルトラストに対する新たな評価の方法や制度が注目を集めていますが、企業や情報利用者はこうした制度をどのように活用していくべきなのか、その一部を紹介し、解説します。なお、本稿の意見にわたる部分は著者の私見でありPwCあらた有限責任監査法人の公式な見解ではないことを申し添えさせていただきます。

1 いま、何が問題なのか？

これまで日本の社会においては、「自社のリスク管理の取り組みやその状況を社会に向けて発信する」こと自体が、各種のインシデントを引き起こしてしまう要因であり、そのこと自体逆にリスクを高めてしまうことと考えられる風潮がありました。その背景には、政府や企業に対して無謬性を求め、ゼロリスクを志向する文化があると考えられます。情報提供者も、情報利用者も「見えていないことは起きていないこと」と片目をつぶりあうことで、リスクが顕在化するまでは見たくない、見せたくないという暗黙の了解が成り立っていた面もありました。

それを象徴する例として、行政手続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（以下、マイナンバー法）、改正個人情報保護法の施行など、ここ数年で進んできた、プライバシーの保護と社会の効率化に向けた動きについての報道の状況が挙げられます。報道ではこうした動きの全体像や取り組みを体系的に伝えることよりも、起きてしまった事件・事故についてその影響範囲や事前・事後の対応に焦点を当てることなくセンセーショナルに報じる場合が多くあります。企業側が「少しでもネガティブに捉えられる情報を発信するのは良くないこと」との意識から脱却できない要因の1つになっていたと言えます。また、情報利用者側の知識不足や、どうせ何を言っても改善されないだろうとの諦めがそうした傾向を助長していた面もあります。

しかしながら新型コロナウイルスが世界中に蔓延していく中で、「活動を抑制することで感染リスクを低減する」「ワクチン接種を受けることで副反応のリスクと感染・重篤化リスクを比較する」といった発想が一般的・日常的になってきたこともあり、リスクの把握、管理、比較を正面から捉えはじめるという副次的な効果が生まれてきています。

では、デジタル社会において、リスクを測り、取捨選択し、

対応し、確認し、発信するというのはどういうことなのでしょうか。さまざまなリスク評価の方法や制度がある中で、企業や情報利用者はデジタル化を進めていく際に、それらをどのように活用していくべきなのでしょう。

2 事業者が発信することが市場に評価されるポイント

2020年6月3日より「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program、通称ISMAP）」の運用が開始され、本稿執筆時の2022年1月1日時点において34サービスがリストに掲載されています。これは、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ策定された制度です。政府全体としてクラウド化を推進する上で適切なセキュリティ水準が確保された信頼できるサービスの利用を促進することを目指し、その評価・審査制度などが定められました。

それではこの制度に則って登録されたサービスを利用していれば、利用者は絶対的な安全と安心を得られるのでしょうか。また、このリストに掲載されていない企業のサービスでは安全・安心は得られないのでしょうか。

答えはいずれも「No」です。登録されているサービスを眺めてみると、本誌読者の方も利用されている著名なサービスも多いのですが、そのサービスにおいて、必ずしも絶対的な障害やサービス停止が起きていないわけではないことは皆さんもご存じのとおりです。

では、ISMAPに登録されているとはどのようなことを意味するのでしょうか。一言で言えば「政府が必要と考える最低限のリスク管理体制の構築と管理の実施が行われている」ということです。各省庁や法人が求める高水準のサービスレベルと、それを支える統制活動の全てが評価検証されているわけではありません。

ならば、これらのサービスを提供する企業はなぜこの制度を利用し登録するのでしょうか。もちろん、直接的には公的機関に利用してもらうために必要だからという理由があります。しかしそれだけではなく、自社のリスクマネジメントやステークホルダーへの情報発信の取り組みに対して、外部の第三者が評価・審査していることを発信するために、日本政府の公的機関が行っていることでアピール効果が高いからという大きな副次的効果があることも否めません。「政府御用達」というブランド効果にもつながるためです。

では、官公庁（公共機関）以外の業界、例えば高いセキュリティが求められることが容易に想像される金融業界や医療製薬業界、自動車産業などでは、事業者は何をもとに評価を行い、どのような内容を発信していけばよいのでしょうか。

金融機関向けのものとしては、金融情報システムセンター（FISC）の安全対策基準があり、医薬業界には3省2ガイドライン（厚生労働省、経済産業省、総務省の3省が発行する医療情報を取り扱う事業者が準拠すべき医療情報の保護に関するガイドライン）が存在しています。自動車産業においては、今後普及する自動運転の枠組みに対して、自動車基準調和世界フォーラム（WP29）で制定された国連規則が存在します。

次節では、これらの各種ガイドラインなどを評価・保証する枠組みについて見ていきましょう。

3 内部統制に対するさまざまな評価方法

評価を行うにあたっては、当然ながら評価対象を定めなくてはいけません。陸上競技をするのか、野球がしたいのか、サッカーなのかボードゲームなのかによって定められるルールはまったく異なります。比較的シンプルな競技である陸上競技のトラック競技で考えても、スタートの位置やオープンレーンか否かなど、詳細なルールが必要なことは誰にも異論はないでしょう。このような取り組みを定めるためのルールブックがセキュリティの管理にも必要になります。これには、上述した業界のガイドラインなどが該当します。

次に対象をどう評価するかを定める必要があります。この評価の仕方は被評価者と評価を利用する者によって決められます。サッカーの例で言えば、練習試合と公式戦、小学生とプロリーグとで異なるレベルのレフェリングが、大会の運営者などに決められて行われているようなものです。実際の評価で言えば、書面で評価するのか、評価者が直接証跡を確認するのか、内部監査などの利用結果をどこまで利用するのか、特定の一時点を評価とするのか、それとも一定期間を対象とするのか、などが決まっていないと評価目的を達成することはできません。

経理や会計監査の世界にいる人であれば「会計監査における会計基準と監査基準のことか」とすぐイメージが湧いたかもしれません。システムやセキュリティの監査評価においても基本的な考え方は同じです。

これらのルールは技術的な進化を反映し、変わってきています。サッカーの例に戻れば、VAR（Video Assistant

Referee）に代表される映像技術や、ボールがゴールラインを通過したかを判定する自動のゴールライン判定技術（Goal line technology）などのテクノロジーを使うかどうかによってレフェリングが変わっていくように、セキュリティ評価においてもクラウドの活用における技術的な要素が取り込まれたり、サイバーセキュリティに関わるガバナンスやマネジメントの考え方が整理されたりしています。

何を評価対象にするのか、誰が、何を、誰に対して、何の目的で、どの水準まで業務を実施していくかのルールと、どこまでの水準の評価を求めるかによっても使われる物差しや求める評価方法は異なってきます。

評価業務に求める水準を決める際に、一般的に考えられているのは主に以下のパターンではないでしょうか。

① 知識経験のある者に評価してもらいたい
② 単に知識経験のある者ではなく、（組織内でもよいから）一定の客観性を有する第三者に評価してもらいたい
③ 組織外の客観的な第三者に評価してもらいたい
④ 知識経験のある第三者に評価してもらうだけではなく、お墨付きを得たい

後者になればなるほど求められる評価水準の高さと客観性の水準も増えていることが分かります。それぞれの水準に必要な「知見」「客観性」「お墨付き」に加え、「コスト」を加えた4要素で上記の4パターンを比較してみましょう（**図表1**）。

1. ピアレビュー・上長のチェック

上記の①に該当します。客観性よりも適時性や職務分掌上の役職などが重視されます。対象の業務や分野の専門性をある程度有しているものの、評価の専門家ではない人が行う場合も多く見られます。チェックリストなどに沿って行われることもあれば、特に基準が設定されていないケースもあり、レベル感はさまざまです。

2. 内部監査

評価者は同一の組織内（企業・グループ等）に所属している者ではあるものの、評価対象業務に直接携わっているわけではなく、一定の客観性を持つと外部の利害関係者からもみなされます。内部統制監査における経営者評価やISO 27001におけるマネジメントテストなどもこれに該当します。監査計画、監査手続などを定め実施することが大半です。

3. 第三者評価（助言型監査）

評価者は組織の外部から調達されるため、客観性は基本的には確保されます。一方で、評価者に求める知見やアプローチ、コストなどには明確な基準がないため、たとえ評価実施者が著名な企業であったとしても、評価の広さや深さが明確に定まっていない限り、必ずしもこの方法のみで評価の水準を担保できるものではありません。このような場合、知見を確保するために資格や経験を求めることがよくあります。

金融庁が企業統合や大型プロジェクトの際に各金融機関に求める評価も基本的にはこの形式になります。

4. 保証業務（保証型監査）

企業外部の独立した知見のある評価実施者が、非財務情報に対して意見（一般的に「お墨付き」と呼ばれる）を与える評価実施方法であり、評価の対象や規準には明確な定義が存在します。

少し長いですが、公認会計士協会の定義する保証業務と日本セキュリティ監査協会の定義する保証型監査を引用します。

> 「保証業務」とは、適合する規準によって主題を測定又は評価した結果である主題情報に信頼性を付与することを目的として、業務実施者が、十分かつ適切な証拠を入手し、想定利用者（主題に責任を負う者を除く。）に対して、主題情報に関する結論を報告する業務
> 引用：監査・保証実務委員会研究報告第31号「監査及びレビュー業務以外の保証業務に係る概念的枠組み」（平

図表1：主な評価者属性と期待される評価水準

評価要素	評価者に求められる知見	得られる客観性	お墨付き	コスト
1. ピアレビュー・上長のチェック	低〜中	低（無）	低	低
2. 内部監査	中	中	中	低
3. 第三者評価（助言型監査）	低〜高	中〜高	低〜中	低〜中
4. 保証業務（保証型監査）	中〜高	高	高	中〜高

成29年 日本公認会計士協会）※1

監査の対象となる組織体の情報セキュリティに関するマネジメントやマネジメントにおけるコントロールが監査手続きを実施した限りにおいて適切である旨を伝達する監査の形態を、「保証型監査」と呼ぶ。
引用：日本セキュリティ監査協会ホームページ※2

いずれの場合も、被評価組織から独立した評価者であること（独立性）と高い知識・経験が求められ、合理的な保証であることは共通です。

財務諸表監査や内部統制監査に利用されるSOC（System and Organization Controls）1（あるいはISAE3402、保証業務実務指針3402）、SOC 2などが有名なところですが、それだけに留まらず、サステナビリティに関する業務やVFM（Value for Money：バリュー・フォー・マネー）に関する業務、法規制関連業務で実施されることもあります。セキュリティの領域でも関連する法規制関連で行われているケースが見られます。

これらの枠組みの中で、委託先やサプライチェーンまで含めた、世の中の流れに沿ったものはあるのでしょうか。それこそが、デジタルトラストの構築に寄与するはずです。次節にて、その潮流を説明します。

4 委託先・サプライチェーンに対する保証業務の新たな流れ（SOC For Supply chain）

現在のセキュリティを考えていく上で大きな課題の1つが、企業間のセキュリティの管理方法と説明責任をどのように伝えていくかです。これまで企業間のセキュリティ管理と言えばガバナンスが効きにくく、実際にリスクが顕在化することが多い委託先管理に主眼が置かれていました。

セキュリティの保証業務で最も一般的なのはSOC 2です。SOC 2とは、米国公認会計士協会（AICPA）のTrustサービス規準を用いて行うセキュリティの保証業務であり、外資系のクラウド事業者を中心に、日本国内においても徐々に普及が進んできています。なお、日本公認会計士協会IT委員会実務指針3850の保証制度もほぼ同等のつくりであると考えてよいでしょう。金融情報システムセンター（FISC）の『金融機関等コンピュータシステムの安全対策基準・解説書』においても委託先の管理状況を確認する際に利用が推奨されるなど、受託企業だけでなく委託企業の認知度も高くなってきています。

監1　外部委託先の監査方法の例示

5. 金融機関等が外部委託を行う場合には、委託する業務の遂行状況及び、外部委託先の要員によるルールの遵守状況等について、評価・検証することが必要である。

（中略）

外部委託先の監査の方法としては、以下の例がある。

（3）第三者保証による報告書（注2）または第三者認証に関する情報（注3）について確認を行う。

（注2）SOC 1、SOC 2、監査・保証実務委員会実務指針第86号、IT委員会実務指針7号等に基づく第三者保証による報告書。
（注3）情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS（ISO27001、ISO27017）やPCIDSSlevel1、プライバシーマーク等に関する情報。

引用：金融情報システムセンター『金融機関等コンピュータシステムの安全対策基準・解説書　第9版改訂』平成31年3月

SOC 2は以前Service Organization Control reportと記されていたこともあり、また今でもAICPAにおいてSOC1、3とあわせて「SOC for Service Organization」と記載された枠組みに入っているように、受委託関係にある企業間で発行されます。その枠組みにおいて再委託先に関しては、Curve out方式（再委託先に対する保証を取り込まない）もしくはInclusive方式（取り込んで一体報告を行う）の2方式がとられていますが、どちらの場合であったとしても委託先管理という目的を達成するために一定の役割を果たしていると言えるでしょう。

ところで、昨今のビジネス環境においてはIoTや自動化などの急速な技術進歩により、製品の生産と流通はより複雑になり、またこれらの技術のおかげでモノを製造・生産する事業体（ユーザー・企業）と、そのサプライヤー、流通業者およびビジネスパートナー（サプライヤー）との関係は、以前よりも相互に結び付いています。さらに、これらの情報を、異

※1 保証業務実務指針 3000「監査及びレビュー業務以外の保証業務に関する実務指針」、日本公認会計士協会、2017年12月19日／改正2019年8月1日
https://jicpa.or.jp/specialized_field/publication/files/2-8-30-2a-20171225.pdf
※2 「ニーズに応じた監査方式」日本セキュリティ監査協会
https://www.jasa.jp/audit/about/about02/

図表2：従来のSOC2とSOC for Supply Chainの比較

項目	SOC for Supply Chain	従来のSOC 2
対象となる組織	製品を生産、製造、または流通させる事業者	受託企業にサービスを提供する組織、または組織のセグメント
責任者	事業体の経営者	サービス提供組織の経営者
評価の対象は組織全体かシステムか	一般的には製品を生産、製造、または販売する企業の全体。関連のシステムに対して行われる場合もある	一般的にはサービスを提供するシステム
想定される利用者	企業のマネジメントおよび全体の枠組みと体制について十分な知識と理解を有する特定の者	受託企業管理者および受託企業およびその体制について十分な知識と理解を有する特定の者
利用目的	特定ユーザー（上記想定利用者）に対し、セキュリティ、可用性、処理の完全性、機密性、またはプライバシーに関連する企業のシステム内の統制に関する情報を提供し、そのサプライヤーと物流ネットワークとの取引関係から生じるリスクをよりよく理解し管理できるようにする	特定ユーザー（上記想定利用者）にセキュリティ、可用性、処理の完全性、機密性、またはプライバシーに関する受託企業の統制に関する情報を提供し、ユーザー自身の内部統制システムに対する評価をサポートする
実施ガイダンス	AICPA Guide SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System	SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy

なる分野間で共有し活用することが模索されています。

こうした状況から、より効率的な全体プロセスを定義し、より良い技術を導入するなどの取り組みが進むことが想定されますが、この相互連関性の強化は、サプライチェーンの潜在的なセキュリティリスクが増大し続けていることも意味しています。ITの世界においては、IPA（情報処理推進機構）の「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」（2018年3月発行、同年10月改訂）などでそのリスクが認識され、対応の流れが出てきていました。IT以外のサプライチェーンについても説明責任に対する注目が高まってきたと言えるでしょう。

その背景としては、国家安全保障の観点のほか、SDGsの目標12「つくる責任 つかう責任」を中心に、サプライチェーンの管理を前提とした企業活動が求められていることもあります。

では、評価の枠組みとして、また保証業務として、こうした説明責任への期待に応えることはできているのでしょうか。まず、枠組みとしてはできていると言えるでしょう。既存のSOC 2からの変化の1形態としてSOC for Supply chainが策定されたことがその一例です。

具体的には、記述規準（Description Criteria）がサプライチェーン用に作成されています。これにより、サプライヤーのシステムがどのように製品を生産、製造、流通させているか、およびそのシステムが標準的な一連の基準に基づいてどのように設計され、実行されているかが詳細に記述されるほか、システム内のサプライヤーの統制に関する詳細、およびサプライヤーの主なシステム目的が該当するTrustサービス規準に基づいて達成されたという合理的な保証をどのように提供できるかについても記載および評価され、管理のための多くの情報を得ることができます。

ただ、海外企業を含めて取得企業は多くなく、普及に関してはまだこれからの枠組みと言えるでしょう。

また、自動運転におけるWP29[※3]でも参照されているドイツのTISAXにおいても、サプライチェーンの先の管理が強く求められています。TISAXはPwCサイトの記事（「TISAX認証取得支援サービス」）[※4]でも詳細に説明していますが、サプライチェーンの川下である完成車メーカー（OEM）からの要請に基づき、部品メーカーやIT企業がその取り扱っている情報に応じて管理策を整備運用し、審査認証機関による評価を行うものです。

ドイツ自動車工業会（VDA）は、達成すべき基準として、ISO27000シリーズをベースにVDA情報セキュリティ評価基準（VDA ISA）を定めており、審査認証結果はENX（European Network Exchange）に登録されるなど、日本のISMAPと似たようなスキームが設けられています。こちらは、日本におけるISMAP取得企業が増えているのと同様、ドイツの完成車メーカーからの要求が強まっていることで、急速に取得企業が増加しています。日本の完成車メーカーも今後同等の動きを見せる可能性は高く、また自動車業界の影響度から他の

※3 WP29（自動車基準調和フォーラム）：安全で環境性能の高い自動車を容易に普及させる観点から、自動車の安全・環境基準を国際的に調和することや、政府による自動車の認証の国際的な相互承認を推進することを目的とし、1つの運営委員会と6つの専門分科会を有している。

※4 TISAX認証取得支援サービス（Trusted Information Security Assessment Exchange）、PwC
https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/tisax-authentication-service.html

業界にも広がり、事実上の世界標準になってくる可能性すらあると言えます。

5 日本企業に向けての提言

ここまで、SOC 2の報告書の委託先管理の考え方と、そこにサプライチェーンも取り込まれたことについて述べてきました。また自動車業界のTISAXのように、業界としての取り組みも簡単に紹介しました。では、これらの保証やこうした考え方を業務委託先やサプライチェーンの川上企業が採用すれば、企業は十分に説明責任を果たしたことになるのでしょうか。その答えはもちろん「No」です。その他にどのような取り組みが求められるのかについて、2点提言を行いたいと思います。

(1) セキュリティの管理範囲の主体的かつ継続的な見直し

「サイバーセキュリティ経営ガイドラインVer. 2.0」※5の3原則には「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」と明記されています。このように、組織をまたいだ業務の連携（サプライチェーン等）や業務委託先を含めた情報把握や対策を行うことは重要であるものの、これまではそれができていないどころか、どのように情報が取り扱われているかすら把握できていないケースも見受けられました。「業務を移転すれば各種リスクも移転できる」と考えるような傾向も根深く、委託先やサプライチェーンの川上を管理する必要性もなかなか共通認識となっていなかったのが実態でした。

たしかに以前は、委託先やサプライチェーンの川上の管理の必要性を急に叫ばれても、管理方法やコミュニケーション方法が分からない企業がほとんどでした。受託企業（委託先）側も金融や製薬業といった規制の厳しい業界以外においては、委託元から強く管理水準の向上や説明責任の担保を求められていませんでした。

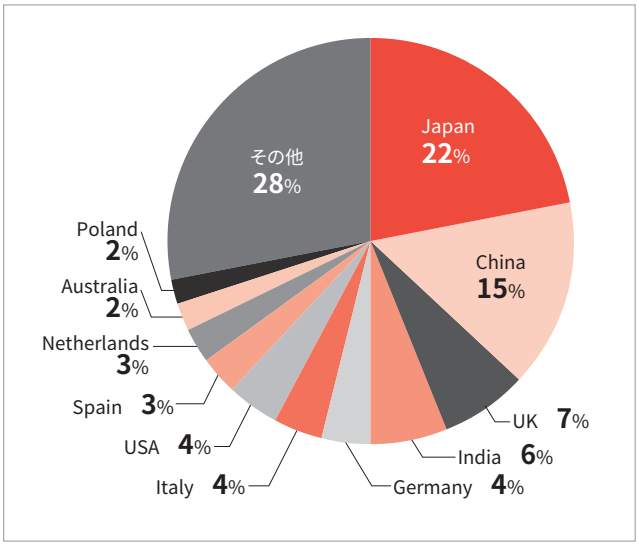
その結果、各種説明責任を果たすためのコストが織り込まれず、一部の企業を除き情報セキュリティの観点から十分な管理ができていたとは言いがたい状況にありました。しかし現在においては、数年前から言われ出した責任共有モデルや責任分界点、保証業務における相補的内部統制などの考え方が汎用的なものとなってきています。業務全体をエンド・ツー・エンドで洗い直し、委託先での業務の状況や、企業間の結合点での取り扱いを見直すことが十分にできる環境になったとも言えるでしょう。

先進的な企業では、今までも自社のセキュリティ上の取り組みを第三者に保証してもらい、その取り組みを積極的に発信していくことで差別化を図っているケースもありました。しかしながら、全体としてはここ数年間に委託先やサプライチェーンの川上の企業も含めた業務の見直しや明文化を行った企業はどれくらいあるでしょうか。本来であれば、業務の明文化やリスクアセスメントは新しい業務が発生する都度、新しい取引先ができる都度、あるいは新しく営業等の拠点が展開される都度、実施され見直される必要があります。内部環境の変化としても組織の統廃合や役割の変化、ITシステムの変更時にも見直しを行う必要があります。

例えば、一般的な製造業であれば、研究開発情報、生産機密情報（部材、生産計画）、製品検査情報、営業情報（商品戦略・キャンペーン情報）などは何かしら他社と連携した動きが起きているはずですが、そうした動きに伴う変更はどこまで情報管理に取り込まれたでしょうか。

日本企業においては、ISO/IEC27001（ISMS）の取得数は、全世界の約22%を占めており、群を抜いて多い状況です（**図表3**）。ISMSの取得により、本来であれば情報セキュリティのマネジメントにおいて、PDCAサイクルを回し、組織としてリスク評価や対応計画の策定・実行ができているはずです。ただし、委託先やサプライチェーンの川上の企業がこの枠組みに含まれない可能性も高いため、経営陣はこの取り組みを自組織内に閉じることなく、そうした企業に広げていこうと

図表3：国別ISMS取得数



出所：International Organization for Standardization, “The ISO Survey 2020” に基づき著者作成

※5 http://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

いう意識を強く持つ必要があります。それでこそ、「サイバーセキュリティ経営ガイドラインVer. 2.0」で求められて、組織をまたいだ業務の連携（サプライチェーン等）や業務委託先を含めた情報把握や対策を真の意味で行うこととなります。

(2) 業務のモニタリング強化

委託先やサプライチェーンに対して直接監査を実施したり、入手した各種の報告書を自社の業務やリスクとして取り込み、不明点を質問し、指摘事項や例外事項が生じた場合の対応などを真摯に協議検討した企業がどれくらいあるでしょうか。報告書を受け取っても単に「お守り」として使っているケースが多いのではないでしょうか。

このような状況においては、形式的な説明はできたとしても実際のリスク管理にはつながらず、いくらさまざまな評価の枠組みが存在したとしても十分に活用していることにはなりません。報告書や認証を聖なるものとして崇めるのではなく、委託先やサプライチェーンの川上の企業と適切なコミュニケーションを行うためのツールと考えることが肝要です。

実際にこれらの取り組みを漏れなく遅滞なく行うためには、現場部門だけに任せたままにせず、リスク管理部門や法務部門等などのいわゆる2線部門が主体的に音頭を取ることが大事です。また関連する現場部門への継続的な研修をはじめとした具体的な意識付けも欠かすことができません。また、なにより経営者自身の主体的な関与が最大の成功要因であることは言うまでもありません。

6 最後に

最後に、セキュリティリスク管理の取り組みは、各種規制に対して形式的に、また一時的に対応すれば完了するものではありません。対応を実施した際に得た知見を組織内で維持・強化し、他のリスクも含めて統合的に取り組み続けることが最適な管理につながります。日本企業が組織全体で日常的なセキュリティ管理の取り組みを充実させ、企業の中長期的な価値創造に資する活動とすることで、その果実を早期にまた確実に得ることを強く願い、支援を進めてまいります。

加藤 俊直（かとう としなお）
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー
外資系コンサルティング、日系コンサルティングの立ち上げを経て現職。会計監査・内部統制監査およびシステムリスク関連の各種業務に幅広く従事している。日本公認会計士協会情報セキュリティ等対応専門委員長およびIT委員、日本セキュリティ監査協会幹事。