PwC's View

Vol. 37
March
2022

特集

デジタルトラスト

pwc

www.pwc.com/jp

目次

特集 デジタルトラスト

特集

デジタルトラスト

昨今のわれわれを取り巻く急速なデジタル化はビジネスの在り方を大きく変え、従来とまったく異なる新しい環境に突入したと言える状況です。このデジタル化は社会生活に大きな発展をもたらしていますが、一方で急激な環境変化へ対応が追い付かず、新たな課題を提起している局面も見られます。

「デジタルトラスト」、すなわちその急激な変化の中でも関係者が安心してデジタル社会の中で活動できるための信頼感の確保は、デジタルを利用して健全な成長を図るための不可欠な要素であると言えます。

本号では、「デジタルトラスト」をテーマとして、デジタル社会における活動を支える基本的な考え方や取り組みの方向性、内外における昨今の議論や制度的な変化の状況について考察しました。

1つ目の論考である「経営課題であるサイバーリスク――IT部門だけで対応できるリスクではない」では、サイバーセキュリティに関するリスク認識とその対応はITに精通した専門家だけの課題ではなく、マネジメント目線でそのリスクを管理し必要な対策を講じていくことの必要性を訴えています。

続いて、2つ目の論考である「デジタルトラストを支える保証・第三者評価」では、デジタル社会において新たな信頼を付与する第三者評価に関する海外および国内の動きを紹介し、あわせてこれらの動きに対して各企業が取るべき対応についての提言を行っています。

さらには、3つ目の論考である「信頼性を確保したデータ流通の促進――EUデータガバナンス法によるデータガバナンス」において、マルチステークホルダー間のデータ流通におけるトラストの構築を推し進めることの社会的な意義や、そのメリットを確認したうえで、データ流通におけるトラストの構築を支えるための仕組み例として、EUにおける「データガバナンス法」を紹介しています。

経営課題であるサイバーリスク
—— IT部門だけで対応できるリスクではない

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　**綾部 泰二**

はじめに

サイバーセキュリティと聞くと、セキュリティ部門やIT部門で対応すべきリスクと認識されている方もまだまだ多いのではないでしょうか。本稿では、サイバーインシデントへの対応や対応状況によっては経営者の責任、企業への格付け評価に影響があることに触れながら、サイバーリスクが経営課題であることを解説します。

1 インシデント対応から理解する

各企業が生産性の向上や新たなビジネスの創出のためにデジタルトランスフォーメーション（DX）を推進し、またコロナ禍への対応としてリモートワークを急激に導入した昨今において、サイバーリスクが顕在化する機会は飛躍的に増大したと想定すべきでしょう。

まずは公開データに基づいて、サイバーインシデントの傾向を把握しておきましょう。**図表1**からも分かるように、最近のサイバーインシデントの傾向として次の3点が挙げられます。

① ランサムウェアによる被害
② 不正アクセス
③ 内部犯行

近年その被害が急増しているランサムウェアは、主に身代金を目的としてシステムを暗号化、もしくはデータを搾取する悪意のあるプログラムですが、金銭を要求する攻撃者に対してどのように対応するかという問題があり、その対応はIT部門やセキュリティ部門の通常の役割を超えるものと想定されます。そのため、会社のポリシーとしてこのような身代金要求には応じないとの意思をあらかじめ決定しておくことが必要です。

身代金要求に応じない場合には、システムが暗号化されたままになったり、搾取されたデータが公開されたりすることが想定されます。そのような場合に必要な対応は以下のとおりです。

(1) システムが暗号化される場合

暗号化されるシステムにもよりますが、システムが復旧されるまで業務をいかに維持すべきかをあらかじめ検討してお

図表1：最近発生したサイバーインシデント

年月	被害組織	概要	攻撃手段
2021年1月	A社	技術情報を持ち出し、転職先企業へ提供した疑い	内部犯行
2021年2月	B社	サイバー攻撃により、水酸化ナトリウムの濃度を通常の100倍超に変更	不正アクセス
	SaaSサービス利用企業	設定ミスにより、複数企業で住民・顧客情報などが漏洩	設定ミス
2021年3月	C社	国際航空情報通信機構（SITA）の旅客系システムへ不正アクセス	不正アクセス
2021年4月	多数	偽名で日本国内レンタルサーバーを契約し、国内約200の組織へサイバー攻撃などに悪用した疑い	不正アクセス（ITサプライチェーン）
2021年5月	D社	ランサムウェア感染のためパイプラインの操業が停止し、約100 GBのデータ漏洩が発生	ランサムウェア
	E社	サイバー攻撃を受け3TBの機密データがリークサイトで公開	ランサムウェア
	F社	テスト環境で利用する「Codecov」への不正アクセスにより、同社ソースコードの一部および約2万8000件の同社顧客情報が漏洩	不正アクセス（ITサプライチェーン）
2021年6月	Webサービス提供会社	大手ITベンダーが提供する共有システムへの不正アクセスにより、政府をはじめとする利用組織から情報漏洩相次ぐ	不正アクセス（ITサプライチェーン）
	G社	食肉加工大手の支社システムがランサムウェア感染。バックアップをもとに復旧するも、身代金として約12億円を支払う	ランサムウェア
	非営利団体組織	2020年4月にランサムウェア攻撃の被害を受けていたことが報道された。被害端末約60台の全面入れ替えを行い復旧	ランサムウェア
2021年7月	H社顧客	自社の顧客企業がランサムウェアに感染	ランサムウェア（ITサプライチェーン）
	I社	ランサムウェア感染のため、企業情報および個人情報の一部が流出	ランサムウェア

出所：公開情報をもとにPwC作成

く必要があります。

あるインシデントにおいては、バックアップを含む大量のデータが暗号化されました。この影響により、被害を受けた企業は決算発表や四半期報告書の提出を延期せざるを得ない状況に陥りました。

（2）搾取されたデータが公開される場合

搾取されたデータの内容を把握できないとインシデントに対応できません。データオーナーがユーザー部門であることから、その対応はユーザー部門が中心となって行うと想定されます。また漏洩データがビジネスパートナーから預託を受けているデータであったり、顧客情報であったりする場合は、その対応はより複雑性を増すことが想定されます。

このように、上記（1）と（2）の対応からも、IT部門やセキュリティ部門だけで対応できるものではないことが分かります。

また、ITサプライチェーン経由の感染、つまり自社またはビジネスパートナーがランサムウェアに感染したことで2次被害が生じたケースがある点には留意が必要です。ITサプライチェーンの被害事例は取引先に留まりません。いわゆるSaaSサービスを提供している企業が感染することで、当該サービスを利用している企業も被害に遭うというケースが発生しています。このため、取引先のサイバーリスクへの対応状況についても理解し、一定水準以上の対応を取っている企業と取引を行うなどの対応が必要です。

このような対応を実行するには、既存の取引先へのアセスメントや、定期的な更新が必要です。これらはセキュリティ担当部門によって推進されるべきですが、実際にビジネスパートナーを管理している部門の協力も不可欠です。

インシデントに対応するときだけでなく、サイバーリスクの発生可能性を低減する際にもIT部門やセキュリティ部門だけでは対応は不十分ということになります。

2 インシデントに対する責任から理解する

インシデントが発生した場合、企業がその責任を問われるケースもあります。そのような事例は国内でも起きていますが、国外においてはその傾向は顕著で、グローバル展開している企業においては特に留意が必要です。

責任が問われる結果としてCEO退任、役員報酬返上といった対応を取らざるを得ないケースがあります。場合によっては被害者から訴訟を提起される、刑事事件に発展して有罪判決を受けるといった可能性もあります。企業が有罪判決を

受けた事例を1つご紹介しましょう。

ある企業ではセキュリティインシデントの公表を予定していました。そのことを事前に知る立場にあったある従業員は株価下落による損失回避を目的として、公表前に自身が保有する自社株を売り抜けたのですが、インサイダー取引と認定されて有罪判決を受けたのです。この事例のような、インシデント情報を知り得る従業員や役員の自社株売却については、制限を設けるなどの措置が必要であることは明らかです。

以上のように、インシデント発生時にはさまざまな部門が対応に関与します。インシデント発生時に関与が想定される部門を事前に特定することは難しく、IT部門やセキュリティ部門だけで対応できる問題ではありません。

3 企業の格付け機関の評価項目から理解する

セキュリティ対策をはじめとする非財務情報の開示は、機関投資家の各種企業格付けに影響を与えています。例えばある格付け機関によると、多数の非財務情報の評価項目としてプライバシーへの対応やデータセキュリティに関し全体の評価に反映させているとのことです。ここで企業から情報が得られない場合には、評価は最低スコアになることもあると言われています。

このようにサイバーリスクへの対応は、非財務情報の開示項目として企業価値に影響を及ぼすものであることから、当該対応もIT部門やセキュリティ部門を超えて全社的に対応しなければならないことが分かります。

4 最後に

ここまでインシデントへの対応、インシデント発生後の責任、そしてサイバーリスク対応の開示といった観点から、サイバーリスクを経営課題として捉えるべきである点について解説してきました。いずれのケースにおいてもIT部門やセキュリティ部門のみの対応ではなく、複数の部門による横断的な対応が求められる課題であるとご理解いただけたのではないでしょうか。

このような部門横断的な課題への対応には、トップマネジメントによるリードが必要です。ぜひ今一度、サイバーリスクへの対応という観点から、インシデントの発生が自社の利害関係にどのようなインパクトを及ぼすかを整理し、現状の体制で十分であるかどうかを検討してみてください。また、将来にわたってサイバーリスクを防ぐための「戦略」を立案し、実行することが必要です。事業戦略、特にデジタルやデータを活用した戦略を立案する際には、サイバーリスクへの対応を当該戦略の一要素として検討すべきでしょう。また、次々と登場するマルウェアの脅威に対抗するためにも、「何を守るのか」を明確にした上で戦略を立案・実行し、対応いただければと思います。

綾部 泰二（あやべ たいじ）

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

2006年CISA（公認情報システム監査人）、2001年にPwCへ参画。以後、セキュリティやITガバナンス等のリスクマネジメント業務に多数従事。2019年7月よりPwC Japanグループのサイバーセキュリティ Co-Leaderを務める。共著に『クラウド・リスク・マネジメント』（同文舘出版）、『経営監査へのアプローチ――企業価値向上のための総合的内部監査10の視点』（清文社）がある。

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。

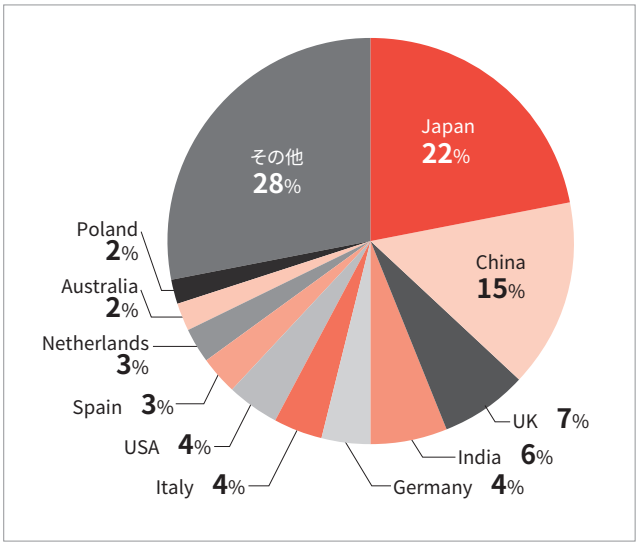
その結果、各種説明責任を果たすためのコストが織り込まれず、一部の企業を除き情報セキュリティの観点から十分な管理ができていたとは言いがたい状況にありました。しかし現在においては、数年前から言われ出した責任共有モデルや責任分界点、保証業務における相補的内部統制などの考え方が汎用的なものとなってきています。業務全体をエンド・ツー・エンドで洗い直し、委託先での業務の状況や、企業間の結合点での取り扱いを見直すことが十分にできる環境になったとも言えるでしょう。

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。

信頼性を確保したデータ流通の促進
—— EUデータガバナンス法によるデータガバナンス

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　**三澤 伴暁**

はじめに

DXの推進、Society5.0、デジタルツイン、メタバース経済など、社会における経済活動の中心が徐々にサイバー空間に移りつつあります。Society5.0が実現した社会においては、サイバー空間と物理空間が融合され、データの存在なしには経済活動が成り立たなくなるでしょう。

こうした状況の中、特定の企業が収集したデータを独占的に用いて利益を得ることに対する批判も強くなり、公平で公正かつ安全なデータ利用を求める声も高まっています。2019年のダボス会議とG20において提唱されたDFFT（Data Free Flow with Trust）も、こうした安全で自由なデータ流通の重要性を背景とした重要な概念の1つと言えます。

一方、プライバシー保護の観点からは、データ流通量の増加が漏洩リスクの増加につながることから、なし崩し的にデータが流通することに対する懸念も大きくなっています。そのため多様なステークホルダー間でのデータ流通がなかなか進展していません。

本稿では、信頼性を確保したマルチステークホルダー間のデータ流通の促進の枠組みの例として、EUにおけるデータガバナンス法（Data Governance Act）を取り上げ、内容を確認するとともに、今後のデータガバナンスのあり方について考察します。なお、本稿における見解は、筆者の私見であることをあらかじめ申し添えておきます。

1 データ流通の促進における課題

冒頭に記したとおり、今後の経済発展の重要な役割を担うのがデータ流通であることは論をまたないのですが、現状、必要なデータが簡単に誰でも利用できる形で十分に流通しているとは言えません。これについて、少し掘り下げて検討してみます。

データを共有する主体側の視点からは、データが流通しない原因を以下のように分析できます。

① データを自社で保持し、利用することにメリット（インセンティブ）がある

いわゆるプラットフォーマー企業と呼ばれる一部の企業が収集したデータを収益の源泉としていることからも、データを収集し、保持することで得られる金銭的対価を代表とするメリットが大きいことは周知の事実であると言えます。

② データを提供し、共有することにメリット（インセンティブ）がない

データを提供することに対する金銭的な見返りが短期間で得られなければ、一般的なビジネスを遂行している会社においては、データを共有することの経済的合理性を見いだせません。もちろん中長期的な視点で考えることが可能な体力のある企業が率先してデータを提供することもありますが、現状こうした事例は多くはありません。

③ データを提供することによるデメリット（コンプライアンス上の制約や追加の対応事項の存在など）がある

例えば個人情報保護法を順守することを前提とした場合、収集した個人情報を二次利用するためには、情報提供者の同意を得ることが必要となります。近年プライバシーデータの取り扱いに対しては規制が強まる傾向があることにも鑑みると、データを提供することによるメリットが、コ

ンプライアンス上で求められる対応によるコストやリスクといったデメリットを上回ることは難しいと考えられます。

また、提供したデータの正確性に対する責任や、不正確なデータを流通させることによって生じる不利益に対する保証や訴訟リスク、データ伝送におけるリスクへの対応等、他にもデメリットを挙げればきりがありません。

このように、データを保持する主体がそれぞれの立場でそれぞれの利益を得ようとすれば、データを流通させることに対して後ろ向きになる理由ばかりが見つかり、流通させることによる将来的な自社の利益や社会全体の利益について検討する方向には向かわないことになります。データ流通を促進させるためには、データの生成、保管を行っている主体のみを対象とした枠組みの整備だけでは不十分で、主体間を横断する取り決めが必要であることは明白だと言えます。

また、一般的なビジネスを遂行している企業が保有するデータを流通させることが難しい状況を踏まえると、個人情報を含むプライバシーデータを多く保有する公的機関が、データ流通のプラットフォーマーとして機能する可能性についても検討する必要があります。

こうした背景もあり、各国において国家レベルでデータ戦略の策定が進められています。そしてその実効性を担保するために、法令などにより主体間のデータ流通の枠組みを定義することで、ガバナンスを構築する動きが加速しています。日本政府による「包括的なデータ戦略」の公開、DFFTの推進によるデータ流通に向けた取り組みといった動きは、こうした背景に呼応するものと理解することができます。

こうした動きの中でもEUにおける取り組みは、特定の企業によるデータの独占的利用に対抗すべく、主体間におけるオープンなデータ流通を志向するものとして先進的であると言えます。その詳細を次節で見ていきます。

2 データ流通の促進および信頼性の確保

2.1 EUデータ戦略

まず、データガバナンス法（Data Governance Act）の成立に向けた動きの前提として、「EUデータ戦略」について触れておきます※1。

EUデータ戦略は2020年2月19日に公表され、その中で以下の課題が示されています。

- データの可用性
- 市場の不均衡
- データの相互運用と品質
- データガバナンス
- データインフラと技術
- 個人の権利行使、スキル、セキュリティ

これらの課題に対応するために、以下の戦略が掲げられています。

A. データアクセスおよび再利用のための法的枠組みなどの構築
B. 投資など
C. 中小企業を含む能力開発
D. 戦略的個別分野でのデータスペースの構築

2.2 データガバナンス法の概略

この戦略における「A. データアクセスおよび再利用のための法的枠組みなどの構築」のために、EU圏内におけるデータ流通の法的枠組み、およびデータアクセスと再利用のための分野横断的な措置を行うための法的枠組みとして、2020年11月25日にデータガバナンス法案が提示されました。この法案は、2021年11月30日には欧州議会とEU加盟国で合意に至り、今後、欧州議会と欧州理事会による法文の最終承認を経て、その15カ月後に規則の適用に至る予定です。またEUデータ戦略の構成要素の1つとして位置づけられ、当該戦略の下で制定される初の法案となります。

データガバナンス法は、データプラットフォーム企業によるデータの独占に対抗し、EU経済圏の発展と市民の利益確保を目指した法律です。この法律により、信頼性を確保した上でデータ流通を促進し、経済発展を目指すとともに、データに基づく方針決定を可能とすることも目標となっています。

信頼性を確保したデータ流通の促進のため、特に特徴的な仕組みが4つ提示されています※2。

1. 公的機関内にある機密性の高いデータを二次利用できる仕組み

※1 European Commission「A European Strategy for data」
https://digital-strategy.ec.europa.eu/en/policies/strategy-data
内閣官房 情報通信技術（IT）総合戦略室「世界のデータ戦略」2020年10月23日
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai1/gijisidai.html

※2 European Commission「European data governance act」
https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

2. データ共有やデータの保存を担う「データ共有サービスプロバイダー」の信頼性を確保する仕組み
3. 市民や企業が社会の利益のためにデータを提供できるようにするための仕組み
4. 目的に合ったデータを業界や国境を越えて利用できるようにするための仕組み

データガバナンス法の各章の概要を**図表1**に示します。

2.3 データガバナンス法によるデータ流通の促進と信頼性の確保

データガバナンス法によるデータ流通の促進と信頼性確保に関して、特に重要な項目として、第二章の「公的機関が保有するデータの二次利用」、第三章の「データ共有サービスプロバイダー」、第四章の「データ利他主義」があります。以降、これらについて詳細に確認していきます。

なお、各章の中で引用した条文は、データ流通の促進や信頼性の確保の目的に資するものを中心に紹介しており、その全てを網羅しているわけではないことをお断りしておきます。また今後日本におけるDFFTの推進を含め、信頼性を確保したデータ流通促進の取り組みの進展とともに、国境を越えたデータアクセスに関する規定（CHAPTER Ⅷ Article 30等）の重要度が高まることが予測されますが、この点についての詳説は別の機会に譲ることとします。

◉ 第二章：公的機関が保有するデータの二次利用

本章では、公的機関が保有するデータの二次利用を可能とするための枠組みについて規定されています。これにより、公的機関がデータプラットフォーマーとして機能することで、中長期的な視点に立った、公益に資するデータ流通の促進を目指しています。

第三条：対象とするデータおよび対象外とするデータ

- 本章は公的機関が保有する、下記によって保護されたデータに適用される。
  - ▶ 営業機密
  - ▶ 統計上の機密
  - ▶ 知的財産権
  - ▶ 個人データ保護
- 下記のものは対象外。
  - ▶ 公共事業のためのデータ
  - ▶ 公共放送のためのデータ
  - ▶ 文化施設や教育機関が保有するデータ
  - ▶ 国の安全、防衛、治安のために保護されたデータ

第四条：データの独占的な利用の禁止

- 公的部門が保有するデータを独占的に利用することを禁止する。
- 公的な利益のための利用においては独占的な利用を認めることがある。
- データの独占的な利用の期間は3年を超えてはならない。

第五条：データの二次利用のための要件

図表1：データガバナンス法の各章の概要

章	章タイトル	概要
第一章	General provisions 総則（一般規定）	一般規定が示されている
第二章	Re-use of certain categories of protected data held by public sector bodies 公的機関が保有するデータの二次利用	公的機関が保有する、営業機密情報、統計データ、知的財産情報、個人データ等の二次利用を可能とするための枠組みについて規定されている
第三章	Requirements applicable to data intermediation services データ共有サービスプロバイダーに適用される要件	データ共有をサービスとして提供する、データ共有サービスプロバイダーに関する要件、当該事業者の信頼性を担保するための枠組みが規定されている
第四章	Data altruism データ利他主義	個人、企業が公益のために利他主義的にデータを提供するための枠組みについて規定されている
第五章	Competent authorities and procedural provisions 監督当局および手続き上の規定	監督当局に対する要求事項、データ共有サービスプロバイダーやデータ利他主義組織に対する不服申し立て手続き、司法上の権利について規定されている
第六章	European data innovation board 欧州データイノベーション会議	加盟国の当局代表等で構成される欧州データイノベーション会議の設置、理事会の役割などについて規定されている
第七章	Committee and delegation 常駐代表委員会と委任	常駐代表委員会への委任および権限について規定されている
第八章	Final provisions 最終規定	国境を越えたデータアクセスに関する規定、罰則、経過措置、発効と適用等が示されている

- データのカテゴリー、二次利用の目的、性質が、非差別的で相応のものであり、客観的に正当化できるものでなければならない。
- 知的財産権を順守すること。
- 営業機密を保持すること。

第六条：報酬

第七条：監督機関

第八条：情報提供窓口

◉ 第三章：データ共有サービスプロバイダー

本章では、データ共有サービスプロバイダー（データ提供者とデータ利用者の間に位置し、データ共有手段を提供することを主たるサービスとする主体）が規定されています。

データ共有サービスプロバイダーの登録制度や課せられる要件の明示により、データ共有サービスの信頼性を高めています。データ共有サービスプロバイダーには、データに対する中立性、目的外利用の禁止など、さまざまな要求事項が課されています。

これらの枠組みは、データ共有サービスがオープンで協調的な形で機能することで、個人や法人が多くの便益を享受できるよう設計されています。

第九条：データ共有サービスプロバイダー

- データ共有サービスとは、データ提供者とデータ利用者の間の仲介サービスであり、当該サービスの提供を可能とする技術的な手段を提供するものである。
- サービス提供には、データの交換又は共同利用を可能にするプラットフォームまたはデータベースの作成、データ提供者とデータ利用者の相互接続のためのインフラストラクチャの確立なども含まれる。

第十条：データ共有サービスプロバイダーの届出

- データ共有サービスプロバイダーは、そのサービスの提供を行うにあたり、監督当局に届け出なければならない。

第十一条：データ共有サービスの提供条件

- データ共有サービスプロバイダーは、提供するデータをデータ利用者のための処理以外の目的で利用できず、法的に独立した法人でなければならない。
- サービスへのアクセス手段は、データ提供者、データ利用者双方にとって公正であり、透明性を保ち、かつ優劣をつけない形で提供する必要がある。
- データへの不正なアクセスを防止する手段を講じなければならない。
- 財政状況が悪化したとしても、サービス提供の継続性を確保しなければならない。
- 違法なデータの転送またはアクセスを防止する措置を講じなければならない。
- データの保管および伝送に関する高度なセキュリティ対策を講じなければならない。

第十二条：監督当局

第十三条：監視

- 第十条および第十一条の順守状況について、監督当局による監視および監督が行われる。
- 違反があった場合には、金銭的な罰則やサービス提供の停止や中断が求められることがある。

第十四条：例外事項

◉ 第四章：データ利他主義

本章では、「データ利他主義」として、個人や企業が自発的に社会の利益のためにデータを提供することを促進し、その信頼性を高めるための規定が示されています。具体的には、データ提供者の信頼性を高める目的での当局への登録やその要件、監視などのガバナンスのほか、データ利用に関する同意を効率的に取得するための、EU圏域内共通の同意書についても規定されています。

「データ利他主義」という概念はこれまであまり馴染みのない概念であり、自組織の利益の最大化を目的とする行動原理に立つと、簡単には理解しにくいものかもしれません。しかし、中長期的に社会全体の利益を目指す観点からは、マルチステークホルダー間で公益に資することを目的としたガバナンスを構築するための新たな仕掛けとして、これまでの資本主義経済での常識に一石を投じる取り組みと言うことができます。今後運用の中でどこまで実効性を高められるか、引き続き動向が注目されます。

第十五条：データ利他主義組織の登録

- 監督当局はデータ利他主義組織の登録簿を整備しなければならない。
- 登録簿に登録された組織は、自らを「認定データ利他主義組織」と称することができる。

第十六条：登録要件

- 公的な利益に沿う目的で設立された法人でなければならない。
- 非営利ベースで運営され、営利目的で運営されている組織からは独立していなければならない。
- データ利他主義に基づく活動が、他の活動とは切り離され、法的に独立した構造で行われなければならない。

第十七条：登録

- 登録要件を満たす組織は、監督当局が管理する登録簿への登録を要請することができる。

第十八条：透明性要件

- 認定データ利他主義組織は、以下の事項の完全かつ正確な記録を保持しなければならない。
  - 保有データの処理を行う者
  - データ処理の日付と期間
  - データ処理の目的
  - データ処理者によって支払われた費用
- 認定データ利他主義組織は、以下の事項を含む報告書を用いて、当局に年次活動報告を行わなければならない。
  - 組織の活動情報
  - 公的な目的でのデータ収集がどのように促進されたか
  - 以下の記述を含む、保有データの利用が許可されている者のリスト
    - 当該データ利用によって得られる公的な利益の概要
    - プライバシーおよびデータ保護技術を含めた、データを利用する際の技術的手段
    - データの利用結果の概要
  - 収入源（特にデータの使用許可に関するものはすべて）と支出に関する情報

第十九条：データ主体および組織の権利保護のための要件

- 認定データ利他主義組織は、データ主体に対して、分かりやすい方法でデータ処理の公的な目的を伝達しなければならない。
- 公的な目的のための処理以外にはデータ利用が行われないことを保証しなければならない。

第二十条：監督当局の設定

第二十一条：監視

- 監督当局は、認定データ利他主義組織が本章に定める要件を順守しているかを監視し、監督する。
- データ利他主義組織が要件を順守していないことを通知された後も改善対応を行わない場合、自らを「認定データ利他主義組織」と称する権利を失い、データ利他主義組織の登録簿から除外される。

第二十二条：欧州データ利他主義同意書

- データ利他主義に基づくデータの収集を容易にするために、欧州データ利他主義同意書を整備する。これにより、EU加盟国間で統一された様式により同意を取得することが可能となる。

これまで詳細に見てきたように、データガバナンス法では、次の4つの取り組みを整備することで、信頼性を確保したデータ流通を促進することを目指しています。

図表2：主体別の信頼性確保のための要件

主体	信頼性確保のための要件	章	条項
公的機関	データの独占的な利用の禁止	第二章	第四条
データ共有サービスプロバイダー	監督当局への届け出	第三章	第十条
	利用者のための処理目的以外でのデータ利用の禁止	第三章	第十条
	法的に独立した法人として設立	第三章	第十条
	アクセス手段の公平性、公正性、透明性の確保	第三章	第十条
	不正アクセスに対する手段の整備	第三章	第十条
	サービス提供の継続性の確保	第三章	第十条
	違法なデータ転送やアクセスを防止する措置の実施	第三章	第十条
	データの保管や伝送におけるセキュリティ対策の整備	第三章	第十条
データ利他主義組織	監督当局への届け出	第四章	第十五条
	営利目的で運営されている組織からの独立	第四章	第十六条
	法的に独立した法人として設立	第四章	第十六条
	データ処理実施者、処理目的、費用等の完全かつ正確な記録の保持	第四章	第十八条
	監督当局への年次活動報告	第四章	第十八条
	データ主体の権利保護	第四章	第十九条
監督当局	登録簿の整備	第三章 第四章	第十条 第十五条
	本法令における要件順守状況の監視	第三章 第四章	第十三条 第二十一条

1. 公的機関のデータ二次利用の促進
2. データ共有サービスプロバイダーによるデータ共有の促進
3. データ利他主義の導入による公益に資するデータの強化
4. 上記における信頼性を確保する仕組み（登録要件の設定や監視の実施）の導入

これにより、データ空間（さまざまなデータが集積される場）の中心を特定の企業の中から社会全体で利用できる場所に引き戻し、データの利用によって得られる利益を広く社会全体に還元することが志向されています。

図表2にデータガバナンス法で定められている主体別の信頼性確保のための要件を、**図表3**に同法における信頼性確保の構造を示します。

3 信頼性を確保したデータ流通促進のために

データ空間全体のエコシステムにおけるガバナンス

これまでステークホルダー間のデータ流通におけるガバナンスの例として、データガバナンス法を取り上げて詳細を見てきました。一方、本稿では取り上げなかった観点として、データ生成・保管主体内におけるデータの信頼性の確保の観点があります。

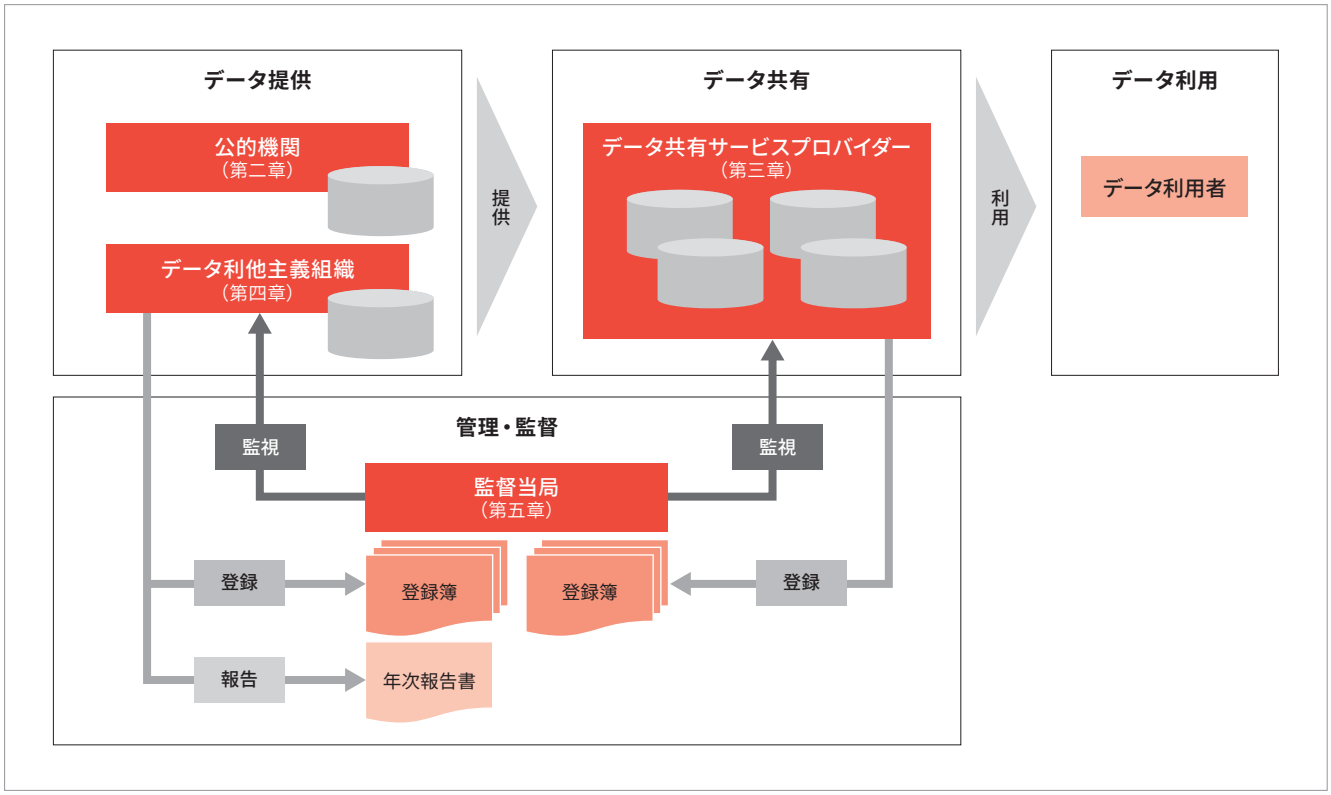
これについては、例えばISO27001シリーズによる認証制度（ISMS認証）やクラウドベンダーの信頼性評価の仕組みであるISMAP、さらには主体内におけるリスクに対する管理策（コントロール）の評価の枠組みであるSOCレポートなど、日本でもすでに一定の効果を上げている枠組みがあります。これらは主にデータ生成・保管主体の信頼性を確保するための枠組みであると言えます。

今後日本国内でもデータ流通におけるガバナンスの検討を深めるにあたり、ステークホルダー間のデータ流通におけるガバナンスに、主体内における信頼性確保の枠組みをつなげて考えることが求められるようになります。重要なのは、データスペースを1つの大きなシステム（系）として捉え、そのエコシステム全体におけるガバナンスを構築していくという視点であると言えます。

日本社会の特徴を踏まえたガバナンスの構築に向けて

Society5.0が目指す社会においては、サイバー空間とフィジカル空間が融合し、データ通信がシステム間で直接やりとりされる割合が増えていくことも想定されています。こうした想定も踏まえ、Society5.0が目指す社会におけるガバナンスについては経済産業省で検討が行われており、検討会

図表3：データガバナンス法における信頼性確保の構造



（Society5.0における新たなガバナンスモデル検討会）の報告書「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」が公開されています※3。

この中で、変化し続ける社会におけるガバナンスとして、マルチステークホルダー間で「ゴール設定」「システムデザイン」「運用」「説明」「評価」「改善」を継続的かつ高速に回転させていく「アジャイル・ガバナンス」の実践や、何層にも折り重なるガバナンスのメカニズムを整理する「ガバナンス・オブ・ガバナンス」の概念が提唱されています。

EUにおけるデータガバナンス法のような法整備を中心としたガバナンスでは、こうした継続的な変化に対応することが難しい側面があります。また日本においては法整備によるいわゆるハードローによるガバナンスよりも、ガイドラインなどの利用によるソフトローによるガバナンスのほうが実効性が高いとの見方もあります。

このため、法整備によるガバナンスの構築の効果や、アジャイルにガバナンスを変化させていくための仕組みの検討など、実効性を伴う仕掛けをどのように現実社会に合わせて実装していくか、広く深い考察が必要となります。さらには、プライバシーに関する規制の動向やAIの発展に伴うAIガバナンスの動向に関しては、国際的なルールとの整合性についても考慮する必要があります。

マルチステークホルダー間のデータ流通の促進は、まずガバナンスの整備によって信頼性を確保することから始まります。なぜなら、安心して社会全体で重要なデータを流通させることが、さまざまなステークホルダーのビジネス上のチャレンジの機会を増やす礎となるからです。

まずビジネスが実行され、そのあとでガバナンスを考えるという世界から、まずガバナンスによる信頼が構築され、そしてビジネスが発展するという世界へのシフトに向け、本稿で取り上げたデータガバナンス法における信頼性確保の枠組みが少しでも参考になれば幸いです。

※3 経済産業省「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」2021年7月30日
https://www.meti.go.jp/press/2021/07/20210730005/20210730005-1.pdf

三澤 伴暁（みさわ ともあき）
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
CISA（公認情報システム監査人）。システム開発、業務改革推進等の経験を経て2007年より現職。会計監査におけるシステムの評価の他、サイバーセキュリティや情報セキュリティに関する第三者評価、セキュリティガバナンス構築等の業務に多数従事。共著に『クラウド・リスク・マネジメント』（同文舘出版）がある。
メールアドレス：tomoaki.misawa@pwc.com

第3回

サステナビリティ情報の信頼性と保証
―― EER保証ガイダンスの視点

はじめに

近年、気候変動情報のように、直接の財務影響がはっきりしなくとも企業の将来を判断する上で無視できない情報が注目されています。これらの情報の多くは財務と非財務の狭間にあって、財務への影響度合いは様々です。ここで取り上げるサステナビリティ情報も同様で、財務・非財務の二分法で整理できるものではありませんが、こうした情報が持つ社会的な重要性は年々大きくなってきています。

サステナビリティ情報は、すでに20年以上も前から多くの企業が自主的に開示していますが、報告にあたってはGlobal Reporting Initiativeの「GRIスタンダード」が多く利用される一方で、近年、気候変動情報に限っては、金融安定理事会（FSB）の気候変動情報開示に関するTCFD提言が開示指針として機能し始めています。

そうした中、国際財務報告の基準づくりに携わってきたIFRS財団が、国際会計基準審議会（IASB）と並列させる形で国際サステナビリティ基準審議会（ISSB）を設置し、2022年には気候変動とサステナビリティ全般に関する2つの報告基準を策定することを発表しました。

その背景には、ESG投資をはじめとするサステナブルファイナンスの急速な拡大があり、投資家を中心にサステナビリティ情報のコンテンツのみならず、その信頼性に対する関心を急速に高めています。そこで本稿では、サステナビリティ情報の信頼性を担保する有力な手段である保証業務について、国際会計士連盟（IFAC）の視点からご紹介します。

なお、本文中に多数ある英略号については末尾の**図表3**をご参照ください。また、文中の意見に係る部分は筆者の私見であり、PwCあらた有限責任監査法人および所属部門の正式見解ではないことをあらかじめご理解いただきたくお願いします。

1 サステナビリティ情報の信頼性を担保する要素は何か

サステナビリティ情報の信頼性を高める要素は、企業内部と開示環境においてそれぞれ以下のように整理できます。

企業内部の要素

- 経営者や従業員のサステナビリティに関する理解の向上
- 企業統治、管理、人事制度などにおけるサステナビリティの考慮
- 定期的なサステナビリティ報告の実施
- サステナビリティ報告のための体制およびルールづくり

開示環境における要素

- サステナビリティに対する社会の関心の高まり
- サステナビリティ報告制度の構築
- 報告クライテリアの策定と普及
- 独立第三者による保証の普及拡大

サステナビリティ情報を信頼できるものにするには、これらの要素が一定の水準でバランスされなければなりません。例えば、サステナビリティの体制を

強化しようとしても、経営者や従業員にサステナビリティへの理解がなければ実効的な体制はできず、逆もまた然りです。一方、企業がいくら頑張ってもそれを社会的に評価する仕組みがなければ取り組みは長続きしないでしょう。

これらの要素の中で、サステナビリティ情報の信頼性を客観的かつ全体的にチェックできるのが独立第三者による保証業務で、任意のサステナビリティ報告が始まって以来、継続的に関わってきたのが会計士を中心としたアカウンティングファームです。

アカウンティングファームは、会計監査の手法を応用することによって、企業が開示するサステナビリティ情報の信頼性を独立第三者の立場で保証してきました。守秘義務があるため、保証報告書以外に個別の内容が公になることはありませんが、この業務に関わってきた筆者は、保証業務の過程で企業のサステナビリティ情報の作成と開示が着実に発展するのを見てきました。

2 サステナビリティ情報の保証業務とは

保証業務は会計監査を含む広い概念です。会計監査に関する基準を作ってきた国際会計士連盟（IFAC）は、会計監査とレビュー業務以外の保証業務に関する保証業務基準「ISAE3000」をすでに策定しています。**図表1**では、そこで示されている保証業務の要素ごとに、サステナビリティ報告書の保証業務を当てはめてみました。

アカウンティングファームがサステナビリティ報告書などの保証業務を行う際は、ISAE3000（もしくは日本公認会計士協会（JICPA）が策定した「保証業務実務指針3000」）に基づいて行われてきましたが、ISAE3000は汎用的な基準であり、サステナビリティ情報の保証業務に特化した基準の策定が期待されていました。

これに対してIFACは、傘下の国際監査・保証基準審議会（IAASB）における数年間の検討を経て、2021年4月にサステナビリティ報告のような「拡張された

図表1：保証業務の要素とサステナビリティ報告書の保証業務の対応

保証業務の要素		サステナビリティ報告書の保証業務
1	三当事者（業務実施者、主題に責任を負う者および想定利用者）の存在	**業務実施者**：監査法人（傘下の組織含む） **主題に責任を負う者**：経営者 **想定利用者**：投資家、社員、取引先、地域住民など
2	**適切な主題** 注）主題に関する企業の状況を明示するものが主題情報	保証契約によって異なるが、以下のような主題の設定が考えられる。 ● サステナビリティ全般に関する企業の状況 ● サステナビリティの特定の側面に関する企業の状況 例：環境、社会、ガバナンス ● 特定されたサステナビリティ要素に関する企業の状況 例：気候変動、有害物質、生物多様性、人権、雇用、製品安全、多様性、ガバナンス構造など
3	**適合する規準**	**GRI**：GRIスタンダード **IFRS財団**：国際サステナビリティ基準 **FSB**：TCFD提言 **WBCSD・WRI**：GHGプロトコル 上記を基礎として策定された特別な規準
4	**十分かつ適切な証拠**	主題情報の妥当性や正確性などを裏づける企業内部のエビデンスおよび主題情報と整合する外部のエビデンス **気候変動情報の例：** ● 排出量の算定根拠となる化石燃料の購買や消費に関する証憑書類および公式な排出係数 ● 再エネ投資や排出量取引の根拠となる請求書など
5	**合理的保証業務または限定的保証業務に応じた適切な様式での書面による報告**	**合理的保証の結論**：「主題情報は、規準に準拠して、すべての重要な点において妥当である」 **限定的保証の結論**：「実施した手続の結果、主題情報が規準に基づき妥当ではないと判断させる事実は、すべての重要な点において発見されなかった」

外部報告（EER）に対する保証業務への国際保証業務基準3000（ISAE3000）（改訂）の適用に関する規範性のないガイダンス」（以下、EER保証ガイダンス）を公表し、新しいタイプの企業報告の信頼性確保に向け本格的に動き始めています。

3 EER保証ガイダンスが指摘するEER（サステナビリティ報告含む拡張された外部報告）の特徴

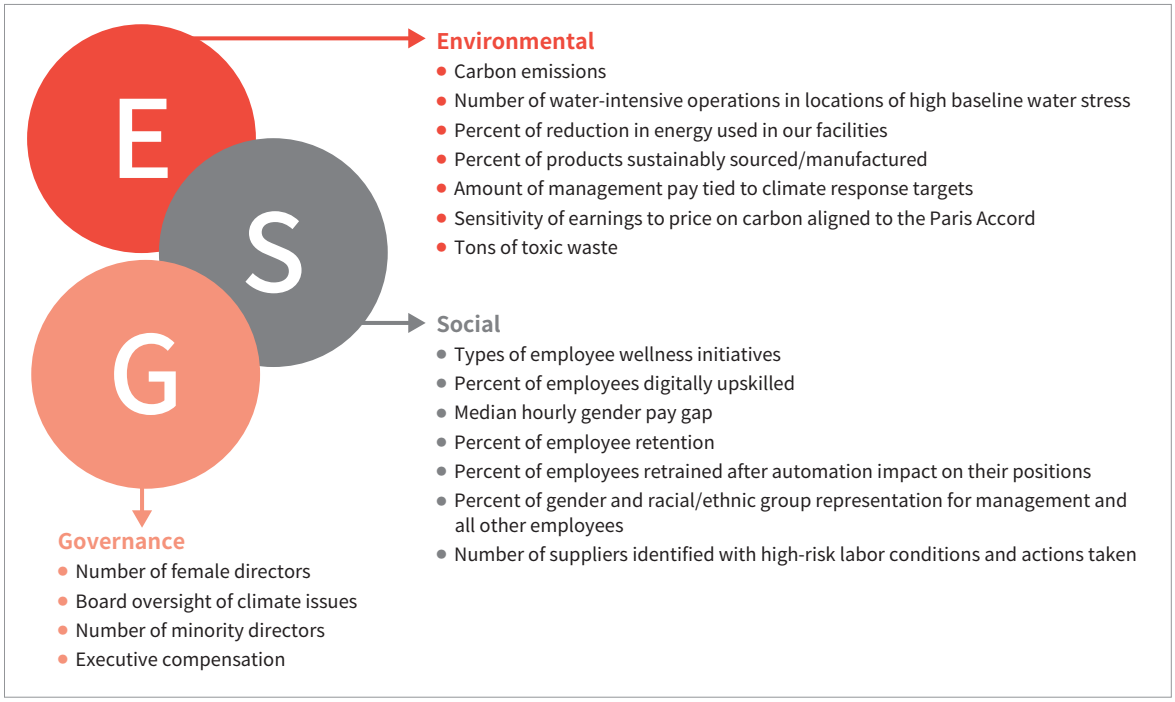
筆者は、1990年代後半から環境報告書やCSR報告書の保証業務の開発と実施に携わってきましたが、当初、こうした報告に対する企業のプライオリティはまだ低く、元データの正確さや網羅性に多くの問題を抱えていました。保証業務の過程ではそうした問題点をひとつひとつ解決してゆき、その積み重ねが保証実施者と企業双方にとって報告すべき情報の本質を考える機会になったことは間違いありません。

例えば、いまや多くの環境報告に見られる原材料や排出物などの物質収支情報については、保証業務が始まった当初、企業は金額的に重要でない物質の出入りをほとんど管理していませんでした。筆者らは企業に対し、個別の環境情報を開示する以上、その前提となる全体的な物質収支の把握と開示が不可欠であることを提案し、それは後に多くの企業に広がっていったのです。

しかし、**図表2**が示すようにEERを構成する情報は極めて多様です。こうした努力を重ねてもなお、EERにはいくつかの課題が残っており、EER保証ガイダンスはその序文で以下のような指摘をしています。

- 客観と主観、過去と将来、財務と非財務といった特徴が組み合わされた極めて複雑な情報である
- 主題の多様性に起因する作成規準の種類と質の多様性は、規準の選択と開発の際、経営者に偏向をもたらす可能性がある
- こうした情報作成に関係する内部統制が未熟である

図表2：EERを構成する多様な情報



出所：PwC、“Making sense of ESG”（2020年10月29日）をもとに作成
https://viewpoint.pwc.com/dt/us/en/pwc/in_the_loop/in_the_loop_US/making-sense-of-esg.html

IFACがこの保証ガイダンスに規範性を持たせなかった理由がここにあると考えられます。とはいえ、現状、サステナビリティ情報の信頼性を考える上でこのガイダンス以上のものは見当たりません。

4 サステナビリティ情報の保証業務が抱える課題と対応

EER保証ガイダンスは、ほぼサステナビリティ情報の保証業務が抱える課題に沿って詳細に書かれています。ここでは、それを集約する形で、筆者の経験上、特に重要と考えている課題を次のように整理してみました。

① 保証実施者に求められる適性と能力
② 保証契約時の留意事項〜前提・規準・範囲の設定
③ 報告トピックの識別プロセスと情報作成プロセスの成熟度
④ 発見した虚偽表示の重要性をどう考えるか
⑤ 定性的な情報と未来志向の情報への対応

なお、EER保証ガイダンスは、上記以外に保証業務の技術的な課題にも言及していますが、内容が専門的なものについては割愛しました。以下では、上で整理した5つの課題について説明するとともに、表題ごとにEER保証ガイダンスの該当する章をカッコ書きしましたので、関心のある方はそちらもご参照ください。

① 保証実施者に求められる適性と能力（第1章）

サステナビリティ情報に限らず企業報告に関する保証業務には、情報開示や保証業務に関する総合的な知見（保証適性）が求められるため、業務全体を統括する責任者は職業会計士が適任と考えられます。

一方、サステナビリティ情報は、環境情報のほかにも人権や雇用関連情報、さらには地域や市場への経済的影響のような情報から構成される多様な情報の複合体であり、また同じ情報でも業界によって測定方法や重要性が異なる可能性があります。そのため、業務を統括する会計士に特定の分野や業界についての知見（主題適性）が十分でない場合は、適切な専門家を必要とする場合があります。

例えば、気候変動やエネルギー情報が重要な情報となる電力会社や数多くの有害物質を扱う化学会社の保証業務では、エネルギー管理士、環境計量士、関連分野の技術士、環境法に詳しい弁護士といった専門家や業界OBなどがチームに加わることでより有効な業務を実施することが可能になるでしょう。

なお、サステナビリティ情報の保証業務を実施する際の業務実施基準となるISAE3000はアカウンティングファーム以外の組織も利用可能ですが、その組織はIFACの品質管理基準を満たす必要があります。

② 保証契約時の留意事項〜前提・規準・保証範囲の設定（第3章、第5章）

契約の前提

保証契約を結ぶためには、保証対象となる主題（例：気候変動への取り組み状況）が適切な規準に従って測定・評価できなければなりません。そうでなければ、保証実施者の結論は単なる主観に終わってしまいます。そこで企業には適切に測定・評価できるデータを収集する仕組みが不可欠となりますが、多くのサステナビリティ情報が重視されてこなかった経緯から、この仕組みが脆弱であるケースが見受けられます。

適切な規準

サステナビリティ報告の規準として一般的なGRIスタンダードは、多くの場合、情報の詳細な作成方法を他の分野別基準に委ねているため、企業は自ら策定した具体的な作成基準を併用しています。保証実施者はそうした作成基準の適切性を判断しなければなりません。その際、報告すべき情報を識別するためのルールや測定・評価および開示の方法が適切なのか、規準が開発されたプロセスが妥当か、さらには想定利用者が適用される規準にアクセス可能であるかといった点に注意が必要です。そうした中、IFRS財団による新たなサステナビリティ基準がどこまで詳細になるのか注目されるところです。

保証範囲の設定

サステナビリティ報告の保証範囲は、報告書全体なのか一部のトピックか、あるいはトピック内の特定の情報なのか、いくつかのパターンが考えられますが、多くの場合、企業が重要と考えるトピックや特定の情報が対象となります。この保証範囲の適切性を考える場合、それが情報利用者にとって有用であるかが重要で、過去には保証しやすい情報だけを保証していると思われる例もありました。EER保証ガイダンスはこうした事例を概して適切ではないとし、保証範囲の段階的拡大や報告全体を数期間に分けて保証するといった対応を提案しています。

③ 報告トピックの識別プロセスと情報作成プロセスの成熟度（第4章、第6章）

報告トピックの識別プロセス

サステナビリティ報告は多様なトピックを扱うため、企業は通常、想定利用者の情報ニーズを考慮に入れた識別プロセスを構築しますが、そうした考慮ができない規準は十分ではなく、また規準が曖昧な場合はトピックの識別に際して経営者の偏向を招く恐れがあります。保証実施者は、規準の適合性を判断する中で当該プロセスについても併せて検討しなければなりません。

情報作成プロセス

識別されたトピックに関する情報の作成プロセスは、財務報告と同種の内部統制を持つ必要があります。保証実施者は保証水準に応じて内部統制を検討しますが、多様なサステナビリティ情報は、必ずしもすべてに十分な内部統制があるとは限らず、特に財務影響が小さいトピックについてはあまり期待できないのが現状です。そうした場合、保証実施者は、入手する証拠の量を増やす必要があるかもしれません。

④ 発見した虚偽表示の重要性をどう考えるか（第9章）

保証業務の結論は、サステナビリティ報告が「すべての重要な点において」規準に準拠して作成されているかについて述べることになります。重要性は報告利用者の観点から検討されなければならないため、規準に重要性の定義がない限り、発見した虚偽表示が利用者の意思決定に影響を与えると見込まれる場合に重要性があると判断されます。しかし、多様なサステナビリティ報告の利用者を特定することは難しく、EER保証ガイダンスでは想定利用者が主要なステークホルダーに限定される可能性を示唆しています。

また、規準が量的な重要性の閾値を特定している場合、業務実施者はこれを利用できます。閾値を特定できていなくても、保証対象が構成要素を持たない個別指標であれば、業務実施者は報告される指標全体に対する一定の比率を適用できます。一方で、例えば温室効果ガスと固形廃棄物の排出量のように基礎となる共通点がほとんどない複数の情報を同時に保証する場合、EER保証ガイダンスは、個別の指標ごとに重要性を検討する場合があるとしており、保証業務の結論が指標ごとに出される可能性があります。

⑤ 定性的な情報と未来志向の情報への対応（第10章、第11章）

定性的な情報

サステナビリティ情報は、ビジネスモデルに関する記述や戦略的な目標のような定性的な情報を多く含みますが、その中でも法令違反や訴訟案件の有無のような事実に基づく情報は、それが直接観察できるか証拠収集手続が実施可能で、かつ適切な規準に基づいて作成されていれば保証業務の対象となる可能性があります。

定性的な情報に関する規準は、それぞれの用語がしっかり定義され合理的に主題を評価できなければならず、その適合性は慎重に検討する必要があります。また、定性的な情報の作成プロセスの有効性については実際の運用状況を評価する必要があるため、保証コストが高くなるかもしれません。

未来志向の情報

サステナビリティ情報には、気候変動による業績影響の予想や今後の戦略といった未来志向の情報が

含まれます。それらは仮定を含み、想定される結果に一定の幅があるため、規準の適合性判断が難しくなる可能性があります。また、仮定を裏づける証拠があったとしても、それ自体が推測を含んでいるため、どこまでが虚偽表示になるのかその識別も容易ではありません。

しかし、EER保証ガイダンスは、規準が経時的な変化や将来の状況、仮定や不確実性の性質などについての開示を求め、また証拠入手の際に、主題の管理状況、仮定の根拠、作成者の能力などを適切に考慮することを条件に保証業務の実施可能性を示唆しています。そうした場合でも業務実施者は、固有の不確実性が適切に想定利用者に伝わるかどうか、また企業が把握していない要因によって影響が大きく変化する可能性があることに留意しなければなりません。

5 おわりに

日々複雑化し、専門性が高まる今の経済社会において、企業は、多様なサステナビリティ情報の信頼性を高めるために様々な要素をバランスよく整える必要がありますが、保証業務はそうした要素を総合的に評価できる唯一の手段と言えます。

とは言え、IFACが定義する保証業務は、厳格な独立性を持つ第三者がサステナビリティに関する企業内部の状況と外部との関係性をつぶさに観察および分析した上で慎重に結論を導き出す複雑なプロセスであり、保証実施者が肯定的な結論を得るまでにクリアすべきハードルは決して低くありません。

しかし、そのハードルが低くないがゆえに肯定的な結論を得た情報は信頼に値し、投資家や顧客の評価を高めた企業の取り組みをより進化させることにつながります。SDGsを掛け声に終わらせないために、今後、この業務の発展が大いに期待されるところです。

【参考文献】

“Non-Authoritative Guidance on Applying ISAE 3000 (Revised) to Extended External Reporting (EER) Assurance Engagements”（IAASB）2021年4月
［上記の翻訳版］『拡張された外部報告（EER）に対する保証業務への国際保証業務基準3000（ISAE 3000）（改訂）の適用に関する規範性のないガイダンス』（日本公認会計士協会）2021年8月

図表3：本文中で使用した英略号とその正式名称

英略号	正式名称	日本語による一般的な呼称
EER	Extended External Reporting	拡張された外部報告
FSB	Financial Stable Board	金融安定理事会
GHG	Greenhouse Gas	温室効果ガス
GRI	Global Reporting Initiative	ジーアールアイ
IAASB	International Auditing and Assurance Standards Board	国際監査・保証基準審議会（アイダブルエーエスビー）
IASB	International Accounting Standards Board	国際会計基準審議会
IFAC	International Federation of Accountants	国際会計士連盟
IFRS	International Financial Reporting Standards	国際財務報告基準（イファース）
ISAE	International Standard on Assurance Engagements	国際保証業務基準
ISSB	International Sustainability Standards Board	国際サステナビリティ基準審議会
JICPA	The Japanese Institute of Certified Pubric Accountants	日本公認会計士協会
SDGs	Sustainable Development Goals	持続可能な開発目標
TCFD	Task Force on Climate-related Financial Disclosures	気候関連財務情報開示タスクフォース
WBCSD	World Business Council for Sustainable Development	持続可能な開発のための世界経済人会議
WRI	World Resources Institute	世界資源研究所

【関連情報】

PwC’s View 第32号、特集：サステナビリティ経営

- なぜ「本物のサステナビリティ経営」が求められているのか

https://www.pwc.com/jp/ja/knowledge/prmagazine/pwcs-view/202105/32-01.html

- ESG情報開示における日本企業の現状と課題

https://www.pwc.com/jp/ja/knowledge/prmagazine/pwcs-view/202105/32-02.html

- サステナビリティ経営を加速するデジタルトランスフォーメーション（DX）

https://www.pwc.com/jp/ja/knowledge/prmagazine/pwcs-view/202105/32-03.html

寺田 良二（てらだ りょうじ）

PwCあらた有限責任監査法人 PwCあらた基礎研究所主任研究員／PwCサステナビリティ合同会社執行役員

1989年公認会計士登録。監査業務を経てサステナビリティ事業部門を立ち上げ、企業や国・自治体のサステナビリティに関する取り組みを支援。現在は、主にサステナビリティに関する調査研究を行う。日本公認会計士協会サステナビリティ副専門委員長、同グリーンボンド保証専門委員（現在）のほか、経済産業省資源エネルギー庁省エネルギー政策に関する検討会委員、環境省環境報告に関する手引きの改訂等検討委員会委員、東京都排出量取引の運用に関する専門家委員など実績多数。『自然資本入門』（2015年NTT出版）、『サステナブル不動産』（ぎょうせい、2009年）、『グローバルCSR調達』（日科技連、2006年）、『環境経営なるほどQ&A』（中央経済社、2003年）などの共著ほか、大学やセミナー等の登壇多数。

メールアドレス:ryoji.r.terada@pwc.com

銀行等によるAML/CFT業務の共同化の方向性
――金融審議会／資金決済ワーキング・グループでの討議結果を踏まえて

PwCあらた有限責任監査法人
レギュラトリー・フィナンシャルマーケッツ・アドバイザリー部
チーフ・コンプライアンス・アナリスト　**井口 弘一**

はじめに

国際的なマネー・ローンダリング／テロ資金供与防止（AML/CFT）に係る高度化の要請が強まるなか、日本はFATF（Financial Action Task Force／金融活動作業部会）による相互審査において厳しい指摘を受けています。その対応の一環として、国としてのAML/CFTの底上げを図るべく、複数の銀行によるAML/CFT業務共同化の実施に向けての協議を本格化させ、今般、金融庁傘下の金融審議会に設置された資金決済ワーキング・グループ（以下、資金決済WG）において、主要議題のひとつとして共同化の意義・方向性が報告書にまとめられました※1。本稿では、資金決済WGにおける審議結果のポイントを解説するとともに、今後、銀行等が進めるべき対応について考察します。

1 資金決済WGの設置

(1) 共同化の検討経緯

共同化の検討は、全国銀行協会（全銀協）にAML/CFT態勢高度化研究会が2018年6月に設置され、銀行間での事務共同化等について、会員行共同で研究を行うことからスタートしています。

一方、政府では2019年10月に開催された第31回未来投資会議（首相を本部長とする「日本経済再生本部」直下の会議体）において、AML/CFT業務の共同化、効率化の検討が課題とされました。2020年1月に経済産業省所管の新エネルギー・産業技術総合開発機構（NEDO）から公募された「マネー・ローンダリング対策に係るシステム開発及び調査」について全銀協ほかが受注し、2021年7月に実証実験結果が公表されています。

また、「成長戦略フォローアップ」（2021年6月18日閣議決定）では、日本における金融業界全体のAML/CFT対応の高度化として、共同システムの実用化および関連する規制・監督上の所要の措置の検討・実施が打ち出されました。さらに、FATFの対日相互審査結果の発表を受け、同年8月30日に公表された「マネロン・テロ資金供与・拡散金融対策に関する行動計画」では「取引モニタリングの共同システムの実用化」が掲げられました。

こうした流れを受け、金融庁の諮問会議である第47回金融審議会総会（2021年9月13日開催）は「資金決済ワーキング・グループ」（以下、資金決済WG）の設置を決定しました。同年10月13日から12月28日の間に5回の会議が開催され、2022年1月11日に報告書が公表されました。

(2) 共同化の意義

資金決済WGにおいては「銀行等によるAML/CFT業務の共同化」が最重要課題として討議されました。今般公表され

※1　金融審議会「資金決済ワーキング・グループ」報告書の公表について、金融庁、2022年1月11日
https://www.fsa.go.jp/singi/singi_kinyu/tosin/20220111.html

た報告書では共同化の意義について「マネー・ローンダリング等の犯罪は、対策が十分でない銀行等が狙われる等の指摘があり、銀行等が業界全体としてAML/CFTの底上げに取り組むことは意義がある。その実効性向上は、詐欺等の犯罪の未然防止や犯罪の関与者の捕捉に直結するほか、被害者の損害回復にも寄与し、利用者保護の観点からも重要な意義を有する」と記されています。

ひとつの銀行等が強い予防措置を強いても、他の銀行の対策が甘ければ、水が高きから低きに流れるように、その銀行が狙われて、犯罪を根絶できません。その意味において、全体の底上げが重要ということです。ただし、システムの整備や人材の確保などの面で課題が多く、海外でも政府の支援の下に対策を進めるケースが散見されます。このことからも、日本においても政府には銀行等を支援する、全体の枠組みを定めるといった対応が求められていたと言えます。

2 共同機関の概要

資金決済WGの報告書において最も注目すべき点は、業務の共同化を担う共同機関の在り様です。審議結果、見解の概要は**図表1**のとおりです。資金決済WGの報告書において、特筆すべき点について解説します。

(1) 共同化の対象／為替取引の取引フィルタリング・取引モニタリング

共同化の対象業務については「顧客等が制裁対象者に該当するか否かを照合し、その結果を銀行等に通知する業務（取引フィルタリング業務）および、取引に疑わしい点があるかどうかを分析し、その結果を銀行等に通知する業務（取引モニタリング業務）」とすることが考えられるとしています。これは、FATFの審査結果で有効性が疑問視されるコメントが散見されたほか、システムや要員負担が大きいため、対応状況に濃淡があり、出遅れている金融機関の支援余地が大きいためです。

また、対象取引は「銀行等（預金取扱等金融機関・資金移動業者）」からの委託を受けた「為替取引」が想定されています。マネー・ローンダリングに悪用された取引の約5割が内国為替、外国為替に係るものであることから、まずは、リスクベースで対象取引を選定しています。

対象業務・取引は、第1回の資金決済WGにおいて言及されています。フィルタリングに関しては、「外国送金のスイフトメッセージタイプというスイフトプラットフォームでやり取りする情報」を対象に検討されており、「将来的には、例えば、貿易書類等も検証の対象にしていくということは、今後の検討課題としてあり得る」とのことです。

また、各銀行等から共同機関に提供する情報は第2回の資金決済WGにて以下の案が提示されています。

① 依頼主情報（氏名・生年月日・顧客番号・住所・国籍・業種・口座情報＜預金種別・口座番号・残高＞など）
② 受取人情報（氏名・金融機関名・口座番号など）
③ 取引チャネル（店頭、ATM、ネットバンキングなど）、送金金額、取扱通貨、送金目的、取引日時など

詳細は、今後設立されるであろう共同機関での検討に委ねられますが、これらの情報が完全かつ正確に提供されるのであれば、取引モニタリングにおいて、ルールベース（一定の条件に合致しない取引の検知）だけでなく、プロファイリング（過去の取引履歴からみて異常な取引を検知）での対応も可能とみられます。一方で、為替取引以外の商品・サービスに関しては対象外であり、属性情報に焦点を当てた不審取引の検知などに課題が残るとみられるほか、銀行等以外の業態の取引も対象外です。また、対象の為替取引に関しても、第

図表1：共同機関の適正な業務運営の詳細／業務内容および規制に関する審議結果

		審議結果要旨
対象		●銀行等（預金取扱等金融機関・資金移動業者）からの委託を受け、為替取引に関し、取引フィルタリング・取引モニタリングの関連業務を行う
業規制	参入要件	●一定の財産的基礎が必要。適切なガバナンスの下で業務を的確に遂行できる体制の確保（業務の実施方法等）などから株式会社形態を視野に入れる
	兼業規制	●個人情報の適正な取扱い等との関係で、一定の制限が必要。取引フィルタリング・モニタリングに関連するものが基本。情報提供機能等を検討
	個人情報	●銀行等と同様の個人情報保護法の上乗せ規制（一定の体制整備義務 等）
	検査・監督	●業務の適正な運営を確保する観点から当局による検査・監督を実施
個人情報の取り扱い		●各銀行等から提供される個人情報は、分別管理し他の銀行等と共有しない

出所：第5回資金決済WG資料および同報告書をもとにPwCあらた有限責任監査法人が作成

1回資金決済WGでは、「当初は、各銀行等で一定の篩（ふるい）にかけられて不審取引の可能性があるとみられる取引を受け付けの対象にする」との発言がありました。

取引フィルタリング、取引モニタリングはAML/CFTフローのなかでは、コア部分を構成する重要プロセスです。全てを網羅することは容易ではないため、まずは、効果的とみられる一部に絞ってスタートするという、現実的な対応が提示されたと言えます（**図表2**）。

（2）業規制の導入

各銀行等はそれぞれの経営判断に基づき共同機関を利用することができると考えられますが、この場合、委託元の銀行等は、他の委託先の場合と同様に、銀行法等に基づき、委託先である共同機関の業務の適正性を管理・監督することが求められます。共同機関の規模が大きくなればなるほど、銀行等による共同機関に対する管理・監督に係る責任の所在が不明瞭となるおそれがあります。また、共同機関の業務はAML/CFT業務の中核的な部分を担うものであり、共同機関の業務が適切に行われなければ、日本の金融システムに与える影響が大きくなります。このため、「一定以上の規模等の共同機関に対する業規制を導入する必要がある」旨の考えが示されました。

これを受け、参入要件として「一定の財産的基礎が必要。適切なガバナンスの下で業務を的確に遂行できる体制の確保」が必要であり、株式会社形態が考えられる旨が方向性として示されました。また、個人情報の適正な取扱い等との関係で兼業を規制すること、銀行等と同様の個人情報保護法の上乗せ規制である一定の体制整備義務等を課すことなども具体的に示されました。さらには、業務の適正な運営を確保する観点から当局による検査・監督を実施することも必要との認識も示されました（前掲**図表1**参照）。

（3）個人情報の取り扱い

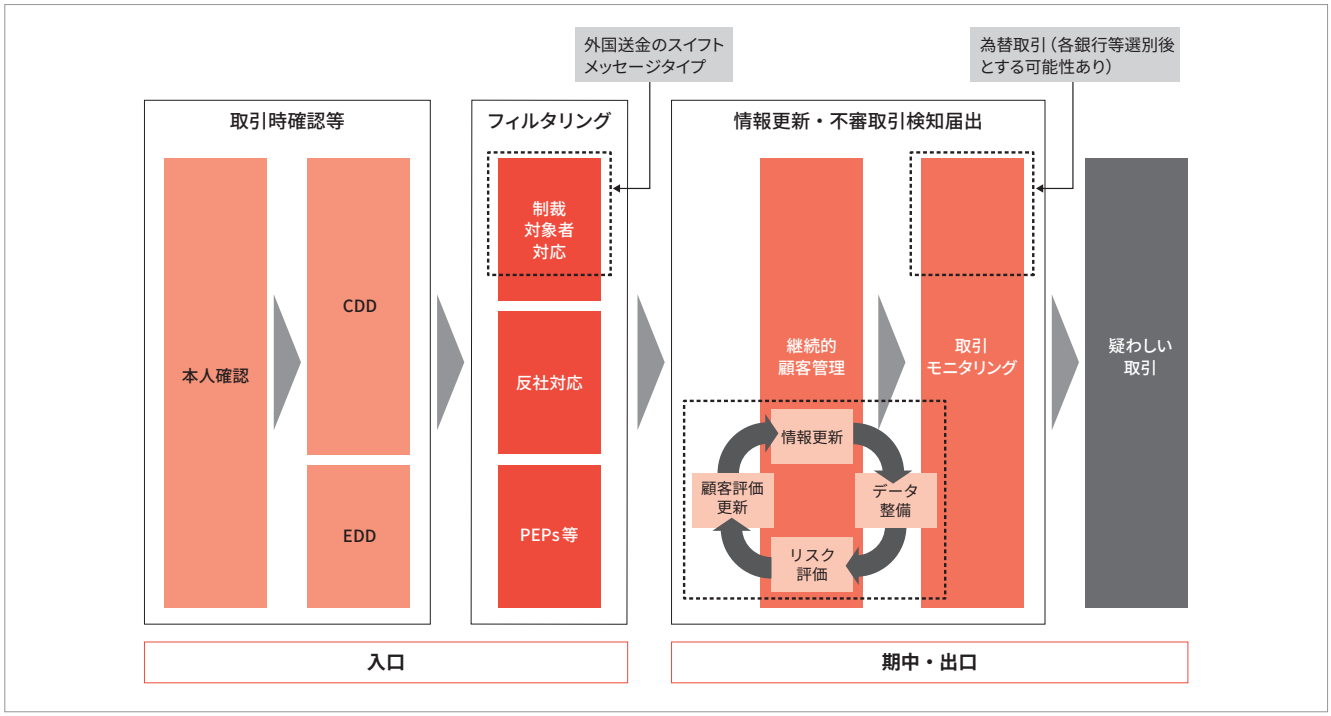
共同機関について、特に慎重に議論が重ねられたのが、個人情報の取り扱いについてです。

①各銀行等が提出した個人情報の分別管理（図表3）

共同機関の運用については「各銀行等から提供を受けた個人データを、各銀行等から委託された業務の範囲内でのみ取り扱い、各銀行等別に分別管理する（他の銀行等のものと混ぜない）」との見解が示されました。米国、シンガポール、オランダなどでは、AML/CFTに係るモニタリングに関して、異なる複数の銀行等による情報の共有や、情報を共有する仕組みが検討されていますが、日本においてはプライバシーへの配慮をより重視すべきと考えられたためです。

また、報告書では「各銀行等の取引等を分析した結果（個

図表2：AML/CFT業務フローと共同化対象範囲のイメージ



出所：PwCあらた有限責任監査法人作成

人データを含む）は、委託元の各銀行等にのみ通知する（他の銀行等と共有しない）」との考えが示される一方、「各銀行等の間の個人情報の共有を可能とする等の対応は、国民の十分な理解を得ていく中で、…（略）… 銀行等に対してより高い水準でのAML/CFTが求められる可能性があること等を踏まえ、検討すべき課題である」とも言及されています。

② 分析ノウハウの共有

報告書では「共同化によるメリットの一つである分析の実効性向上を図る観点から、これに資するノウハウを特定の個人との対応関係が排斥された形（個人情報ではない形）で共有する」という考えが示されています。システムが分析の過程で学習した各種係数を共有する場合、一般論として、「当該パラメータと特定の個人との対応関係が排斥されている限りにおいて個人情報に該当しないと考えられる」ためです。

③ 個人情報保護の手続きに関する考え方の整理

銀行等が利用者の個人情報等を共同機関に提供するに際して、個人情報保護法が定めるところの、銀行等によるその利用者への「利用目的の特定・通知又は公表」は必要か、という論点があります。この点、資金決済WGでは、現在公表されている銀行の「個人情報の利用目的」（犯罪収益移転防止法に基づく本人の確認等や、金融商品やサービスをご利用いただく資格等の確認のため）の範囲内と考えており、「利用目的の特定・通知又は公表」は不要としています。

また、共同機関への個人情報の提供に際しての本人同意の取得等についても、「本人同意不要」としています。銀行等ごとに分別管理し、各銀行等の取引等を分析した結果を他の銀行等と共有しない場合、個人情報保護法第23条（第5項）に第三者提供の例外として示された「利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合」に該当するとの考えを採っているためです。

3 銀行等が留意・対応すべき点

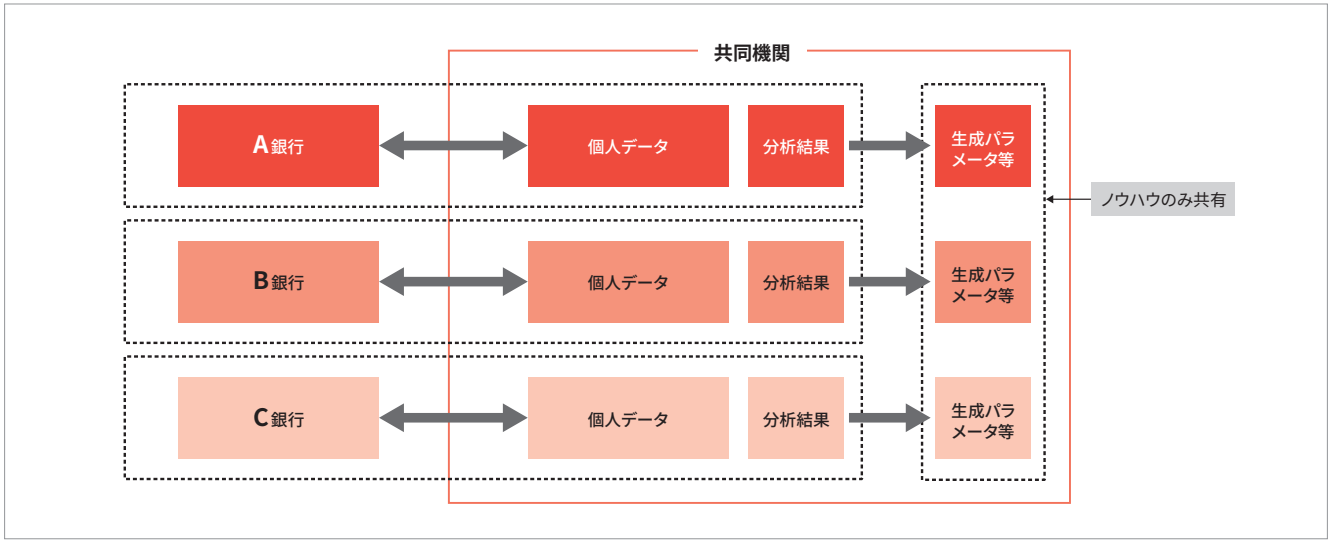
現状は共同機関の概要、方向性が示された段階ですが、今回の資金決済WGでの審議結果を踏まえて、銀行等が留意・対応すべき点を整理します。

(1) 留意点

留意すべきこととして、前述のとおり、共同機関の業務は銀行等に求められる取引フィルタリング、取引モニタリングの業務プロセスの全てを対象としているわけではないという点が挙げられます。また、対象の為替取引であっても、情報を提出するにあたっては一定レベルの抽出・選別作業が必要となることが考えられるほか、個人情報についてもその正確性も問われることになります。

加えて、最終判断業務は銀行等が引き続き担うことになります。すなわち、共同機関の高度な機能を利活用した場合であっても、制裁対象者か否かのチェック結果を受けて取引可否をどのように判断し実行するのか、疑わしい取引の検知や届出を受けてどのように対応するのか、その責任はあくまで

図表3：個人情報の取り扱い（イメージ）



出所：第5回資金決済WG資料および同報告書をもとにPwCあらた有限責任監査法人が作成

も銀行等にあります。共同機関は判断材料を通知するのみであり、銀行等が果たすべき義務は変わりません。これは、第1回資金決済WGにおいて明確にされています。

(2) 対応の方向性

①データガバナンス

取引フィルタリング・取引モニタリングを実行するにあたって、金融庁の「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」では、対応が求められる事項を以下のとおり掲げています。

- 確認記録・取引記録等について正確に記録するほか、ITシステムを有効に活用する前提として、データを正確に把握・蓄積し、分析可能な形で整理するなど、データの適切な管理を行うこと
- ITシステムに用いられる顧客情報、確認記録・取引記録等のデータについては、網羅性・正確性の観点で適切なデータが活用されているかを定期的に検証すること

FATF第4次相互審査結果では、継続的な顧客管理について、情報更新が形式的に行われているに過ぎず、情報を集めることが目的化している旨の指摘が散見されました。最新データをモニタリング等に活用することが求められるなか、共同機関へのデータ提出の前提として、情報の更新および収集データの速やかかつ正確な格納・確認は必須になります。

②フィルタリング・モニタリング体制の整備継続

共同機関が担う対象業務が一部に限定されることに加え、判断義務が従来と同様に求められることから、銀行等は不審取引の検知・判断体制の整備・高度化を継続的に進める必要があります。共同機関はひとつの支援ツールであり、業務を全て丸投げできないということを認識して対応することが必要です。

そのため、すでに十分なフィルタリング、モニタリング体制を確立している銀行等は、共同機関を活用するか否か、活用するとしてもどのように活用するのかが検討課題になると思われます。

4 おわりに

詳細な内容は今後の検討に委ねられますが、銀行等によるAML/CFT業務の共同化に関しての方向性が纏められたことは、日本におけるAML/CFT業務の底上げに向けて大きな一歩となったと言えます。日本の共同化の取り組みは、今年7月に公表されたFATFのAML/CFTのデジタル・トランスフォーメーションに関する報告書（データプーリング、共同分析とデータ保護にかかるストックテイク）でも好事例として取り上げられており、実現すれば、国際的な評価にもプラスに働くものと推測されます。

一方で、本件が実施されても、しばらくはAML/CFT業務に関する負担が劇的に減少することはないとみられます。また、行動計画に示された「取引モニタリングの共同システムの実用化」の対応期限は2024年春であり、時間もそれほど残されていません。実効性を上げられるかは共同機関の制度設計をどれだけ具体的に検討できるか、そして銀行等がどれだけ準備できるか次第です。共同機関の設立・稼働に向け、官民が力を合わせて尽力することが求められています。

さらに、その後に目を転じると、共同機関は、銀行等による為替取引を出発点にして参加者やビジネスタイプも増やしていくことが期待されます。それが、まさしくAML/CFTの高度化に関する国際的な要請にも合致する対応です。

なお、資金決算WGにおいては、AML/CFT業務の共同化のほかに、以下の事項が協議され、成果を上げました。

①「電子的支払手段に関する規律のあり方」において「ステーブルコイン（法定通貨の価値と連動した価格（例：１コイン＝１円）で発行された電子マネー）について、送金・決済の手段としての規律を検討」
②「前払式支払手段に関するAML/CFTの観点からの規律」において「高額チャージ・移転が可能な前払式支払手段（電子ギフト等）を発行する資金移動業者への犯収法に基づく本人確認等の規律の適用を検討」

本稿では詳述できませんでしたが、今後、法制化等の協議が進む可能性があり、日本における資金決済全体の金融規律が整備されていくことが期待されます。

井口 弘一 (いぐち こういち)
PwCあらた有限責任監査法人 レギュラトリー・フィナンシャルマーケッツ・アドバイザリー部　チーフ・コンプライアンス・アナリスト
1989年4月に大手銀行入行、調査・企画畑を専門に、調査部、営業審査部、企画部、コンプライアンス統括部（マネー・ローンダリング防止対策室、金融犯罪対策室等）、監査部にて勤務。2017年8月より海外大手銀行（日本法人）のコンプライアンス統括責任者。2021年4月より現職。
メールアドレス：koichi.iguchi@pwc.com

2022年度（令和4年度）税制改正大綱
――法人課税を中心に

PwC税理士法人
ディレクター　**荒井 優美子**

PwC税理士法人
シニアマネージャー　**山田 盛人**

はじめに

2021年12月に自由民主党・公明党両党が公表した2022年度（令和4年度）税制改正大綱[※1]（以下、「2022年度税制改正大綱」）は同年12月24日閣議決定されました。2022年度税制改正大綱は岸田政権下で最初の税制措置ですが、いくつか注目すべき変更点があります。本稿では、2022年度税制改正大綱の法人課税に焦点を当てて注意すべき点について解説します。なお、今後の審議状況等によっては、内容に変更を生ずる可能性もありますのでご留意ください。

本稿の内容を含む2022年度税制改正大綱の概要については、オンラインセミナーでも解説を行っております。ぜひご参照ください。

【オンラインセミナー】2022年度（令和4年度）税制改正
https://www.pwc.com/jp/ja/seminars/tax-1220105.html

1 2022年度税制改正大綱の背景

自由民主党・公明党両党は2021年12月10日に2022年度税制改正大綱を公表し、12月24日には当初予算案としては過去最大となる令和4年度予算案（一般会計107兆5,946億円）が閣議決定されました。2022年度税制改正大綱は「新しい資本主義」の実現を掲げる岸田政権下で初めての税制改正大綱として策定されたもので、「コロナ克服・新時代開拓のための経済対策」[※2]（2021年11月19日閣議決定）において示された、「新しい資本主義」を起動させ、「成長と分配の好循環」を実現するための税制措置と位置付けられます。

国際的にはこれまでの資本主義を含めた社会の在り方を見直すグレート・リセットの議論[※3]の展開や、サステナブルな資本主義の提言[※4]等にも見られるように、企業による社会的課題への取り組みが内外で拡大している中で、わが国ではさらなる取り組みの余地があると指摘されています[※5]。米国の「ビルド・バック・ベター」、欧州の「次世代EU」など、世界では、弊害を是正しながら、さらに力強く成長するために新たな資本主義モデルの模索が始まっています。わが国でも、成長と分配を実現する「新しい資本主義」を具体化する[※6]ことが岸田政権の経済対策の柱に据えられました。

2022年度税制改正大綱には、以下の改正が盛り込まれています。

（1）成長と分配の好循環の実現のための既存の特別措置の見直し（人材確保等促進税制、オープンイノベーション促進税制、5G導入促進税制等）

※1　https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2022/20211224taikou.pdf

※2　https://www5.cao.go.jp/keizai-shimon/kaigi/minutes/2021/1119/shiryo_01.pdf
※3　新しい資本主義実現会議（第1回）資料3「新しい資本主義の実現に向けて（論点）」（2021年10月26日）
※4　「新成長戦略」2020年11月17日 日本経済団体連合会
※5　新しい資本主義実現会議（第1回）資料5 参考資料
※6　第207回国会における岸田内閣総理大臣所信表明演説（2021年12月6日）

（2）経済社会の構造変化を踏まえた税制の見直し（個人所得課税、相続税・贈与税等）
（3）国際的な租税回避や脱税への対応も含めた国際課税制度の見直し
（4）円滑・適正な納税環境整備（適格請求書等保存方式、記帳義務、スキャナ保存制度、電子取引情報の電磁的記録保存）等

以下では、2022年度税制改正大綱の法人課税に関わるものを次の項目に分けて解説していきます。

1 成長と分配の好循環の実現のための措置
2 グループ通算制度
3 中小企業関連
4 その他
5 国際課税
6 金融・証券
7 納税環境整備

2 成長と分配の好循環の実現のための措置

（1）所得拡大促進税制（旧賃上げ・生産性向上のための税制）は、2021年度（令和3年度）税制改正により、大企業向けの賃上げ及び投資の促進に係る税制の要件が、新規雇用者の給与等支給額及び教育訓練費の増加に着目した人材確保等促進税制に見直されたところです。岸田政権下では、「成長と分配の好循環」の実現に向けて、長期的な視点に立って賃上げを促すとともに、株主だけでなく従業員、取引先などの多様なステークホルダーへの還元を後押しする観点から、賃上げに係る税制措置を抜本的に強化することとされました（**図表1**）。

2022年度税制改正では、新規雇用者に係る措置を改組し、継続雇用者給与等支給額及び教育訓練費を増加させた企業に対し、給与等支給額の増加額の最大30%を控除する制度に見直され、適用期限が2年延長されます。大企業（資本金10億円以上かつ常時使用従業員数1,000人以上）については、給与等の支給額の引上げの方針、取引先との適切な関係の構築の方針その他の事項についてインターネットを利用する方法により公表したことを経済産業大臣に届け出ている場合に限り、適用されることとなります。

なお、教育訓練費に係る税額控除率の上乗せ措置の適用を受ける場合の教育訓練費の明細書の確定申告書への添付要件が、明細書類の保存要件に見直されます。

（2）研究開発税制その他生産性の向上に関連する税額控除の規定（特定税額控除規定）の不適用措置について、大企業（資本金10億円以上かつ常時使用従業員数1,000人以上）の前事業年度の所得が零を超える一定の場合には、継続雇用者給与等支給額の増加割合が1%（2022年度は0.5%）以上に見直されます（**図表2**）。なお現行制度では、継続雇用者給与等支給額が、継続雇用者比較給与等支給額を超える場合に特定税額控除が適用されます。

（3）オープンイノベーション促進税制とは、特別新事業開拓事業者（スタートアップ企業）に対して特定事業活動として出資をした場合の課税の特例を指します。この税制は、2020年度（令和2年度）税制改正で、「既存企業の有するリソースを最大限活用したオープンイノベーションの促進とユニコーン級ベンチャーの育成を図り、第4次産業革命における日本企業の国際競争力を強化すべく、新たな税

図表1：人材確保等促進税制の改組

	現行	改正案
通常要件	●新規雇用者（雇用保険法の一般被保険者）給与等支給額の対前年度増加率2%以上 ●新規雇用者（雇用保険法の一般被保険者に限定されない）給与等支給額※の15%の税額控除 ※雇用者給与等支給額の増加額が上限	●継続雇用者給与等支給額の対前年度増加率3%以上 ●大企業（資本金10億円以上かつ常時使用従業員数1,000人以上）は、給与等の支給額の引上げの方針、取引先との適切な関係の構築の方針その他の事項の公表を経済産業大臣に届け出 ●控除対象雇用者給与等支給増加額（雇用者全体の給与総額の増加額）の15%の税額控除
上乗せ措置	●教育訓練費の対前年度増加率20%以上 ●新規雇用者（雇用保険法の一般被保険者に限定されない）給与等支給額※の20%の税額控除（5%上乗せ） ※雇用者給与等支給額の増加額が上限 ●税額控除額は法人税額の20%を限度	●継続雇用者給与等支給額の対前年度増加率4%以上の場合には、税額控除率に10%を加算 ●教育訓練費の対前年度増加率20%以上である場合には、税額控除率に5%を加算 ●控除対象雇用者給与等支給増加額（雇用者全体の給与総額の増加額）の20%、25%、30%の税額控除（最大15%上乗せ） ●税額控除額は法人税額の20%を限度（変更なし）

制措置」（経済産業省「令和2年度経済産業省税制改正要望」※7）として創設されたものです。「ウィズコロナ・ポストコロナの世界を見据えて、新たな付加価値の創出・獲得に資する大企業の有する資金・技術・販路等のスタートアップ企業での活用を促進するとともに、企業の事業再構築を加速することが重要」（「令和4年度経済産業省税制改正要望」※8）であるとの認識から、2022年度税制改正では、出資の対象となる特別新事業開拓事業者の要件を拡充し、特定株式の保有見込期間要件等を緩和した上で、適用期限が2年延長されます（**図表3**）。

（4）地方を活性化し、世界とつながる「デジタル田園都市国家構想」の実現に向け、①地方拠点強化税制（地方活力向上地域等において特定建物等を取得した場合の特別償却又は税額控除制度及び地方活力向上地域等において雇用者の数が増加した場合の税額控除制度）の対象資産、対象雇用者および計画の認定要件を見直した上で 、適用期限が2年延長され、②5G導入促進税制（認定特定高度情報通信技術活用設備を取得した場合の特別償却又は税額控除制度）の対象設備および税額控除率等を見直した上で、適用期限が3年延長されます。

5G導入促進税制は、特定高度情報通信等システムの普及の促進に関する法律の認定法人（一定のシステム導入を行う認定特定高度情報通信等システム導入事業者）が、2022年3月31日までの間に、特定高度情報通信用認定等設備を取得し、事業供用した場合に税制優遇措置を与える制度として、令和2年度税制改正で導入されたものです。

デジタル田園都市国家構想実現に向けては、5G全国ネットワークについて、高度なインフラを都市・地方で一体的に整備しつつ、特に条件不利地域における整備を加速することが重要であり、企業等の多様な主体が自らシステムを構築するローカル5Gについても、社会課題解決や事業革新等に向け、導入を後押しすることが必要であるとの認識に立ち、5Gインフラに係るベンダーの多様化と基地局のオープン化に資する形で、より効果的に5Gインフラを整備するため以下のように見直されます。

① 特定高度情報通信技術活用システムの適切な提供及び維持管理並びに早期の普及に特に資する基準について、（i）「特定基地局が開設計画に係る特定基地局の開設時期が属する年度より前の年度に開設されたもの」という要件を廃止し、5G高度特定基地局を加える、（ii）ローカル5Gシステムについては、導入を行うシステムの用途がローカル5Gシステムの特性を活用した先進的なデ

図表2：特定税額控除の不適用措置の改正

	現行	改正案
適用年度	2024年3月31日までに開始する事業年度	現行どおり
対象措置	研究開発税制、地域未来投資促進税制、5G導入促進税制、DX投資促進税制、CN投資促進税制	現行どおり
適用要件	中小企業者（適用除外事業者を除く）等を除く法人について ● 適用年度の所得金額 ＞ 前期の所得金額 →以下のいずれかを満たす場合に上記の税額控除措置を適用 ① 継続雇用者給与等支給額 ＞ 継続雇用者比較給与等支給額 ② 国内設備投資額 ＞ 減価償却費の総額 ×30% ● 適用年度の所得金額 ≦ 前期の所得金額 →上記の要件を課さない	大企業（資本金10億円以上かつ常時使用従業員数1,000人以上）について 前事業年度の所得が零を超える一定の場合 ①の要件を 継続雇用者給与等支給額の対前年度増加率1%（2022年度0.5%）以上

図表3：オープンイノベーション促進税制の改正

	現行	改正案
特別新事業開拓事業者	設立後10年未満	設立後10年未満、ただし売上高に占める研究開発費の額の割合が10％以上の赤字法人の場合は設立後15年未満
特定株式の保有見込期間、特定事業活動の継続期間（株式の継続保有に係る証明）	5年	3年
特定勘定の取り崩し期間	特定株式の取得日から5年	特定株式の取得日から3年

※7 経済産業省「令和2年度経済産業省税制改正要望について」2019年8月30日
https://www.meti.go.jp/main/zeisei/zeisei_fy2020/zeisei_r/index.html
※8 経済産業省「令和4年度経済産業省税制改正要望について」2021年8月31日
https://www.meti.go.jp/main/zeisei/zeisei_fy2022/zeisei_r/index.html

ジタル化の取組みであるものに限定、(iii) 補助金等の交付を受けたものを除外。

② 特定高度情報通信技術活用システムを構成する上で重要な役割を果たすもののうち、一定の周波数の電波を使用する無線設備の要件について、多素子アンテナを用いないものを加え、マルチベンダー構成のもの及びスタンドアロン方式のものに限定。

③ 税額控除率について、令和4年度（2022年4月1日から2023年3月31日）の事業供用設備は15%または9%、令和5年度の事業供用設備は9%または5%、令和6年度の事業供用設備は3%。

(5)「環境と調和のとれた食料システムの確立のための環境負荷低減事業活動の促進等に関する法律」（仮称）において規定される予定の「環境負荷低減事業活動実施計画」（仮称）または「特定環境負荷低減事業活動実施計画」（仮称）に基づき導入される環境負荷の原因となる生産資材の使用量を減少させる設備等（環境負荷低減事業活動用資産）、および「基盤確立事業実施計画」（仮称）に基づき導入される、化学農薬または化学肥料に代替する生産資材を製造する設備等（基盤確立事業用資産）に対し、税制上の措置（法律の施行日から2024年3月31日までに事業供用した資産についての特別償却制度（機械装置等32%、建物等は16%）の適用）が創設されます。

3 グループ通算制度

(1) 2022年4月1日以後開始事業年度より適用となるグループ通算制度について、以下のように見直されます。

① 投資簿価修正制度について、通算子法人の離脱時にその通算子法人の株式を有する各通算法人が、その株式（子法人株式）に係る資産調整勘定等対応金額について離脱時の属する事業年度の確定申告書等にその計算に関する明細書を添付し、かつ、その計算の基礎となる事項を記載した書類を保存している場合には、離脱時に子法人株式の帳簿価額とされるその通算子法人の簿価純資産価額にその資産調整勘定等対応金額を加算することができる措置が講じられます。

② 通算制度からの離脱等に伴う資産の時価評価制度について、時価評価資産には、帳簿価額1,000万円未満の営業権が含まれることとされます。

③ 通算税効果額から、利子税の額に相当する金額として各通算法人間で授受される金額が除外されます。

④ 共同事業性がない場合等の、通算法人の欠損金額の切捨て、損益通算の対象となる欠損金額の特例、通算法人の特定資産譲渡等損失の損金不算入の適用除外となる要件のうち支配関係5年継続要件について見直されます。

⑤ 認定事業適応法人の欠損金の損金算入の特例における欠損金の通算の特例について、各通算法人の控除上限に加算する非特定超過控除対象額の配賦の計算方法が見直されます。

(2) グループ通算制度における外国税額控除制度の適用について、①税務当局が調査を行った結果、進行事業年度調整措置を適用すべきと認める場合には、通算法人に対し、その調査結果の内容（進行事業年度調整措置を適用すべきと認めた金額およびその理由を含む）を説明するものとし、②この説明が行われた日の属する事業年度の期限内申告書に添付された書類に記載された金額等（進行事業年度調整措置を適用した金額）がその説明の内容と異なる場合には、その事業年度に係る税額控除不足額相当額または税額控除超過額相当額に係る固定措置を不適用とする等の見直しが行われます。法人住民税の外国税額控除制度についても同様に見直されます。

4 中小企業関連

(1) 所得拡大促進税制について、税額控除率の上乗せ措置の要件が見直され、その適用期限が1年延長されます。

(2) 中小法人に係る交際費の損金算入の特例の適用期限が2年延長されます。

(3) 中小企業者等の少額減価償却資産の取得価額の損金算入の特例制度について、対象資産（取得価額が30万円未満である減価償却資産）のうち貸付け（主要な事業として行われるものを除く）の用に供した資産を除外した上で、適用期限が2年延長されます。

5 その他

(1) 海外投資等損失準備金制度の適用期限が2年延長されます。

(2) 交際費等の損金不算入制度および接待飲食費に係る損金算入の特例制度の適用期限が2年延長されます。

(3) 少額の減価償却資産の取得価額の損金算入制度につい

て、対象資産（取得価額が10万円未満の減価償却資産）のうち貸付け（主要な事業として行われるものを除く）の用に供した資産が除外されます。

（4）一括償却資産の損金算入制度について、対象資産（取得価額が20万円未満の減価償却資産）から貸付け（主要な事業として行われるものを除く）の用に供した資産が除外されます。

6 国際課税

（1）過大支払利子税制について、国内に恒久的施設を有しない外国法人の法人税の課税対象とされる以下の所得も、過大支払利子税制の適用対象となります。

① 恒久的施設を有する外国法人に係る恒久的施設帰属所得以外の国内源泉所得

② 恒久的施設を有しない外国法人に係る国内源泉所得

（2）保険会社等に関する外国子会社合算税制（CFC税制）の適用については、特定外国関係会社等の判定における特例（保険委託者特例）が設けられ、一定の保険委託者は合算課税の対象外とされています。しかしながら、この保険委託者特例が、保険業法上の保険会社または保険持株会社が保有する外国保険会社を対象にしていることから、国内における中間持株会社を通じて海外に子会社等を保有する場合は、この特例の対象外とされています。2022年度税制改正により、保険委託者特例に関する「一の保険会社等」および「その一の保険会社等との間に特定資本関係のある保険会社等」によってその発行済株式等の全部を直接または間接に保有されている外国関係会社である旨の要件について見直されます。

（3）子会社からの配当と子会社株式の譲渡を組み合わせた租税回避防止措置（子会社株式簿価減額特例）について、①適用除外要件（特定支配日利益剰余金額要件）の判定の見直し、②適用除外基準を満たす子会社を経由した配当等を用いた本制度の回避を防止するための措置（適用回避防止規定）が不適用となる場合の拡充等が改正されます。改正は、2020年4月1日以後開始事業年度に受ける対象配当の額から適用されます（制度開始に遡及して改正を適用）。

7 金融・証券

（1）一定の内国法人が支払を受ける、以下の配当等については、配当等に係る所得税の源泉徴収を行わないこととされます（2023年10月1日以後の配当等から適用）。

① 完全子法人株式等に係る配当等

② 配当等の支払に係る基準日において、当該内国法人が直接に保有する他の内国法人の株式等（当該内国法人が名義人として保有するものに限る）の発行済株式等の総数等に占める割合が3分の1を超える場合における当該他の内国法人の株式等に係る配当等

（2）利益剰余金と資本剰余金の双方を原資として行われた剰余金の配当（混合配当）が行われた場合の最高裁判所の判決（2021年3月11日）を受けて、国税庁は本件最高裁判決を踏まえた今後の取扱い等（「最高裁判所令和3年3月11日判決を踏まえた利益剰余金と資本剰余金の双方を原資として行われた剰余金の配当の取扱いについて」）を2021年10月27日に公表しました[※9]。2022年度税制改正により、みなし配当の額の計算に係る「株式又は出資に対応する部分の金額」の計算方法が、次のように見直されます。

① 資本の払戻しに係るみなし配当の額の計算の基礎となる払戻等対応資本金額等及び資本金等の額の計算の基礎となる減資資本金額は、その資本の払戻しにより減少する資本剰余金の額を限度とされます（出資等減少分配に係るみなし配当の額の計算及び資本金等の額から減算する金額についても同様）。

② 種類株式を発行する法人が資本の払戻しを行った場合におけるみなし配当の額の計算の基礎となる払戻等対応資本金額等及び資本金等の額の計算の基礎となる減資資本金額は、その資本の払戻しに係る各種類資本金額を基礎として計算することとされます。

8 納税環境整備

（1）タイムスタンプの国による認定制度の創設に伴い、スキャナ保存制度等が整備されます。

（2）電子取引の取引情報に係る電磁的記録の保存への円滑な移行のための宥恕措置が整備されます（2022年1月1日

※9 当該取扱いについては、当法人発行の以下のニュースレターをご参照ください。
「令和3年3月11日の最高裁判所判決を踏まえた剰余金の配当の取扱いについて」
https://www.pwc.com/jp/ja/knowledge/news/tax-jtu/taxnews-issue193.html

から2023年12月31日までの間に申告所得税および法人税に係る保存義務者が行う電子取引に適用)。

荒井 優美子 (あらい ゆみこ)
PwC税理士法人　ディレクター
クロスボーダーの投資案件、組織再編等の分野で税務コンサルティングに従事。2011年よりナレッジセンター業務を行う。日本公認会計士協会租税調査会（出版部会)、法人税部会委員。公認会計士、税理士。
メールアドレス：yumiko.arai@pwc.com

山田 盛人 (やまだ もりと)
PwC税理士法人　シニアマネージャー
大手監査法人および税理士法人において、監査業務および税務業務に約9年間従事の後、2004年PwC税理士法人に入社。日系および外資系企業の税務顧問業務、組織再編・事業承継・M&Aなどの各種税務コンサルティング業務に従事、証券会社（富裕層向けサービス部門）への出向を経て、2019年よりナレッジセンター所属。日本公認会計士協会実務補習所教材検討委員（税務担当)、一般財団法人会計教育研修機構実務補習所講師。公認会計士、税理士。
メールアドレス：morito.yamada@pwc.com

PwC Japanグループ｜調査レポートのご案内

会計、税務、経営に関連するさまざまな調査レポート、また、海外の拠点から発行されたPwCの各種出版物を掲載しています。

各レポートは、Webサイトより詳細をご確認・ダウンロードしていただけます。
▶ https://www.pwc.com/jp/ja/knowledge/thoughtleadership.html

最新トピック

2022 Global Digital Trust Insights Survey
―サイバーセキュリティのスリム化を目指す経営層のためのガイド―

PwCは60以上の国・地域で2021年7月から8月にかけ、企業の経営層（CEO、企業役員、CFO、CISO、CIO、C-Suite役員）3,602名を対象に、サイバーセキュリティに関する調査「Global Digital Trust Insights 2022」を実施しました。

今回の調査では、経営層がサイバーセキュリティを意図的にスリム化するためのガイドを提供しています。

このガイドでは、一般的に軽視されることが多い以下4つの質問に焦点を当てており、これらの質問を適切に検討することでかなりの効果を見込めます。これらは、データトラストに関する調査でありながらテクノロジーを中心としたものではないので、斬新かつチャレンジングな内容と感じる方もいるかもしれません。なぜテクノロジー中心ではないかというと、テクノロジー自体はセキュリティのスリム化に対する答えにはならないためです。その代わり、私たちは技術スタック（組織の土台となるテクノロジー）から取締役まで、つまりCEOをはじめ組織全体と協調して行動することに焦点を当てています。セキュリティは、ビジネス全体、全ての機能、全ての従業員にとっての懸念事項なのです。

1. CEOは企業のサイバーセキュリティに変化をもたらすことができるか。
2. 組織が複雑すぎてセキュリティを確保しにくくなっていないか。
3. 現在と将来の最重要リスクに対してセキュリティを確保しているか。
4. サードパーティやサプライチェーンがもたらすリスクをどの程度把握しているか。

本レポートの詳細はこちら
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2022-global-digital-trust-insights.html

Viewpoint

会計・監査に関するPwCの総合情報サイト

Viewpointとは、これまでのInformに置き換わる、会計・監査に関する情報を提供するPwCのグローバルのデジタル・プラットフォームです。Viewpointは、IFRS関連情報が中心ですが、US GAAP（米国会計基準）、日本基準についても取り上げています。
Viewpointには、日本サイト（日本語）だけでなく、GlobalサイトやUSサイトもあります。

Viewpointの特徴（今後の新機能）のご紹介

● リアルタイムなアップデートとパーソナライズ

ユーザーが登録した好みを中心にコンテンツが整理されますが、Viewpointを使えば使うほど、ユーザーに最適な情報をタイムリーに提供します。

● 直感的な検索機能（予測変換）

よく検索される用語に基づいて、おすすめの用語やガイダンスが表示され、必要な情報にすばやくアクセスできます。

● PwCの専門家によって編集されたコンテンツページ

コンテンツページを閲覧しているときに、サイドパネル上で関連リンクを見ることができます。また、ユーザーが最初にアクセスするページにホットトピックを集め、関連するニュースや解説資料をワンストップで探すことができます。

● メニューナビゲーション

クリック数を最低限に抑えて、人気コンテンツにアクセスできます。

▼直感的な検索機能（予測変換）

▼PwCの専門家によって編集されたコンテンツページ

いつでも、どこでも、Viewpointは
あなたに最適な情報をお届けします。

外出先で

Viewpointは、モバイルやタブレット、PCで検索履歴などを共有し、シームレスに連携します。また、タイムリーに更新された情報に容易にアクセスできます。

オフィスや自宅で

直感的なインターフェースとナビゲーションにより、必要な情報を容易に見つけることができます。検索に役立つ予測検索機能は、必要なときに必要なものを見つけるのに役立ちます。

チーム内で

SNSなどでのコンテンツ共有機能を使って、チームのメンバー同士で瞬時にPwCのインサイトを共有し、スピード感をもって、重要なトピックを把握することができます。

Viewpointのコンテンツ

Viewpointには、次の3つのコンテンツがあります。

無料コンテンツ

IFRSの速報や速報解説など、どなたでもご覧いただけるコンテンツです。

無料登録会員コンテンツ

（Viewpointサイト上で登録可能）

IFRSおよび日本基準の比較、IFRSに基づく連結財務諸表のひな型など、PwCのナレッジを集約したコンテンツです。

有料会員コンテンツ

IFRS基準書やPwC IFRSマニュアル、詳細解説などIFRSに関する詳細なガイダンスです。

Viewpointの特徴のひとつであるパーソナライズを有効に使うため、まずは無料登録会員の登録からはじめましょう。

https://viewpoint.pwc.com/jp/ja.html

●ニュースレターご登録

Viewpoint 日本サイトでは、更新情報や便利な機能のご紹介など、E-Mailで無料にてお届けするニュースレターを月1回無料で配信しています。是非ご登録ください。

ニュースレター 新規登録
https://forms.jp.pwc.com/public/application/add/329

コンタクト PwCあらた有限責任監査法人 Viewpoint事務局
E-mail: jp_aarata_viewpoint-mbx@pwc.com

会社法計算書類の実務
――作成・開示の総合解説（第14版）

会社法計算書類作成の実務に携わる方々のさまざまな疑問を解消できるよう、最新の記載事例を多数収録し、会社法計算書類の作成方法や会社法の計算関係の実務について詳しく丁寧に解説しています。

本版では、会社法改正の解説に加え、新設された「収益認識に関する会計基準」「時価算定に関する会計基準」「取締役の報酬等として株式を無償交付する取引に関する取扱い」「グループ通算制度を適用する場合の会計処理及び開示に関する取扱い」「時価の算定に関する会計基準の適用指針」の改正など、2021年に適用あるいは公表された最新の会計基準等の概要および実務への影響を解き明かしています。

さらに、国際財務報告基準任意適用企業の増加傾向を踏まえ、指定国際会計基準に基づいて連結計算書類を作成している企業の開示実務についても解説しています。

PwCあらた有限責任監査法人 編
A5判　752ページ
5,700円（税抜）
2022年2月発行
中央経済社

税効果会計の実務ガイドブック
――基本・応用・IFRS対応

PwCあらた有限責任監査法人 編
A5判　370ページ
4,000円（税抜）
2021年11月発行
中央経済社

クラウド・リスク・マネジメント 新版

PwCあらた有限責任監査法人 編
A5判　192ページ
1,900円（税抜）
2021年9月発行
同文舘出版

海外PwC日本語対応コンタクト一覧

PwCは、全世界156カ国、29万人以上のスタッフによるグローバルネットワークを生かし、
クライアントの皆さまを支援しています。ここでは各エリアの代表者をご紹介いたします。

	担当国・地域	写真	担当者名		電話番号	メールアドレス
アジア太平洋	中国大陸および香港		高橋 忠利	Tadatoshi Takahashi	+86-139-198-9251	toshi.t.takahashi@cn.pwc.com
	中国（華中・華北）		吉田 将文	Masafumi Yoshida	+86-150-27-756	masafumi.g.yoshida@cn.pwc.com
	中国（華南・香港・マカオ）		柴 良充	Yoshimitsu Shiba	+852-2289-1481	yoshimitsu.shiba@hk.pwc.com
	台湾		奥田 健士	Kenji Okuda	+886-2-2729-6115	kenji.okuda@pwc.com
	韓国		原山 道崇	Michitaka Harayama	+82-10-6404-5245	michitaka.h.harayama@pwc.com
	シンガポール・ミャンマー		平林 康洋	Yasuhiro Hirabayashi	+65-9627-3441	hiro.hirabayashi@pwc.com
	マレーシア		杉山 雄一	Yuichi Sugiyama	+60-3-2173-1191	yuichi.sugiyama@pwc.com
	タイ・カンボジア・ラオス		魚住 篤志	Atsushi Uozumi	+66-2-844-1157	atsushi.uozumi@pwc.com
	ベトナム		今井 慎平	Shimpei Imai	+84-90-175-5377	shimpei.imai@pwc.com
	インドネシア		割石 俊介	Shunsuke Wariishi	+62-81-1174-0023	shunsuke.wariishi@pwc.com
	フィリピン		東城 健太郎	Kentaro Tojo	+63-2-8459-2065	kentaro.tojo@pwc.com
	オーストラリア・ニュージーランド		牧田 芳朗	Yoshiro Makita	+61-401-643-495	yoshiro.a.makita@pwc.com
	インド・バングラデシュ・ネパール・スリランカ		座喜味 太一	Taichi Zakimi	+91-6366-440227	taichi.z.zakimi@pwc.com
欧州・アフリカ	英国		小堺 亜木奈	Akina Kozakai	+44-7483-391-093	akina.a.kozakai@pwc.com
	フランス		猪又 和奈	Kazuna Inomata	+33-1-5657-4140	kazuna.inomata@avocats.pwc.com
	ドイツ		藤村 伊津	Itsu komura	+49-211-981-7270	itsu.x.fujimura-hendel@pwc.com
	オランダ		新井 赫	Akira Arai	+31-61-890-9968	akira.a.arai@pwc.com
	イタリア		長谷川 愛	Ai Hasegawa	+39-344-343-8487	ai.i.hasegawa@pwc.com
	ルクセンブルク		又木 直人	Naoto Mataki	+352-621-333-735	naoto.m.mataki@pwc.com
	スイス		佐藤 晃嗣	Akitsugu Sato	+41-58-792-1762	sato.akitsugu@pwc.ch
	ベルギー・中東欧全域・ロシア		森山 進	Steve Moriyama	+32-2-710-7432	steve.moriyama@pwc.com
米州	カナダ		北村 朝子	Asako Kitamura	+1-604-806-7101	asako.kitamura-redman@pwc.com
	米国		椎野 泰輔	Taisuke Shiino	+1-347-326-1264	taisuke.shiino@pwc.com
	メキシコ		志村 博	Hiroshi Shimura	+52-1-55-6965-6226	hiroshi.s.shimura@pwc.com

（2022年3月1日現在）

日本企業の海外事業支援の詳細はWebをご覧ください。
https://www.pwc.com/jp/ja/issues/globalization.html

The New Equation
変わりゆく世界で成功し続けるために

The New Equation は、PwC の新たな経営ビジョンです。
多岐にわたる分野の多様なプロフェッショナルがスクラムを組み、
「人」ならではの発想力や経験と「テクノロジー」によるイノベーションを融合しながら、
ゆるぎない成果を実現し、信頼を構築します。

It all adds up to The New Equation.

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

本誌に関するご意見・ご要望ならびに送付先変更などのご連絡は、下記までお願いいたします。
jp_llc_pwcs-view@pwc.com

PwCあらた有限責任監査法人
〒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：03-6212-6800 Fax：03-6212-6801