

## プライバシーとデータ保護

### 第1部：弾力的なフレームワークを構築する際の内部監査の役割

内部監査財団・Crowe

著者：パメラ・S・フルビー CCEP, CIPP/US

R・マイケル・バーニー CPA, CIA

訳者：堺 咲子

内部監査人協会（IIA）専門職資格審議会 委員

インフィニティコンサルティング 代表

CIA, CCSA, CFSA, CRMA, CPA (USA)

#### 目次

序文とエグゼクティブ・サマリー .....	55	の見解 .....	64
1. プライバシーとデータ保護に関する課題の歴史と進展 .....	56	内部監査とデータ保護が交差する場所 .....	65
キロバイトからゼタバイトへ .....	56	一般に認められた10のプライバシー原則 .....	66
問題の定義、用語の定義 .....	58	4. 弾力的にデータ保護に取り組むためのフレームワーク .....	67
保護、プライバシー、およびレジリエンス（弾力性） .....	59	フレームワークの構成要素と構造 .....	68
2. 法規制の状況、コンプライアンス、その他のリスク .....	60	内部監査の役割：統合的アプローチ .....	68
規制環境の進化 .....	61	5. フレームワークの導入と遵守状況の監査 .....	68
GDPRは素晴らしい新世界か .....	61	推奨する導入方法と監査方法 .....	68
EU域外の進展状況 .....	62	事例研究：プライバシー・フレームワークの適用 .....	70
米国のデータ保護制度 .....	63	結論とさらなる研究 .....	71
コンプライアンスを超えるリスク .....	64		
3. 内部監査にとってのデータ保護の課題と懸念 .....	64		
データ保護の課題に対する内部監査人			

#### 序文とエグゼクティブ・サマリー

現在、顧客、従業員、サプライヤー、また

はその他の第三者との関係を持つ事実上すべての組織体は、急増を続けるプライバシーとデータ保護要件の明確な規制対象となってい

る。このような規制は、組織体全体に課題を提起することがあり、また、内部監査人に特有の課題を突き付ける可能性がある。

これらの課題は、この分野で最も有名な最近の規制措置の1つである、欧州連合（EU）の「一般データ保護規則（GDPR）」の2018年の施行に伴い特に注目を集めた。米国では、2020年1月1日に「カリフォルニア州消費者プライバシー法2018年（CCPA）」が施行され、状況がさらに複雑になった。知名度の高いGDPRとCCPAは、このような多くの規制構造の中の2つに過ぎず、これらの規制構造が組み合わさって、急増し絶えず変化する規制環境を生み出している。

テクノロジーの進歩は、プライバシーとデータ保護に関する多くの懸念の根本原因であるが、これらはITの問題だけにとどまらないことに注意することが重要である。データ保護とプライバシーは職務の枠を超えた課題なので、組織体全体で取り組まなければならない。

本稿は、内部監査人がプライバシーとデータ保護の諸問題に関する自身の現在の準備水準を評価する際の一助となることを意図しているが、その理由は、特に内部監査人の取り組み方が、内部監査専門職の現状に関連しているからである。この自己評価の要素の1つには、所属する組織体の現在のデータ環境を理解することと併せて、第三者との関係やテクノロジーのような重要分野の監査手法が変化する可能性を理解することが含まれる。

さらに本稿は、内部監査人が特有のリスクと脅威を理解し、関連するコントロールが効果的に策定、導入、および運用されているかを確認する一助となることも意図している。本稿の後半の節で示すフレームワーク、監査計画、および導入に関する議論は、内部監査部門の体制を構築する基礎を提供するためのものである。

本研究プロジェクトの今後の段階では、本

稿の第2部を今後1年から1年半の間に公表する予定である。これらの段階では、内部監査財団会員に対するアンケートや実地インタビューに基づいて、専門職としての内部監査がどのようにデータ保護とプライバシーの課題に対応しているかを検討する。プロジェクトの最終段階では、プライバシー担当役員や他のステークホルダーがこれらの同じ問題をどのように捉えているかを検討し、内部監査専門職がステークホルダーの期待にうまく応えているかを評価することを目標とする。

## 1. プライバシーとデータ保護に関する課題の歴史と進展

過去数十年のテクノロジー革命がもたらした多くの影響の1つは、プライバシーとデータ保護の課題が重大な懸念事項として浮上したことである。あらゆる種類の組織体（公共と民間、営利と非営利、ローカルとグローバル）は、顧客、サプライヤー、規制当局、およびステークホルダーなどとの新たな交流の仕方を模索している。

これらすべての交流を推進する原動力は、データである。このようなデータは大抵、機密情報、専有情報、または個人情報である。貴重なデータを盗難、紛失、または誤用から保護する必要があるため、組織体には全く新しい懸念分野が生じ、内部監査人には対処すべき全く新しいリスク分野が生じた。

### キロバイトからゼタバイトへ

いろいろな意味でこれらの課題に対する関心が高まったのは、過去25年間にわたる市場とテクノロジーの大きな変化の必然的な帰結である。1995年には、インターネットは毎秒28.8キロビットのダイヤルアップモデム、パソコンのハードディスク容量は500メガバイト、携帯電話はアナログ、そして人々は依然としてポケベルを使用していた。現在、世界

中のデータ作成量は16ゼタバイト（ZB）を超えており、2025年までに163 ZBに達すると予測されている<sup>1</sup>。

データ量の急増以上に、このようなデータ量の増加を組織体が把握して利用する様々な方法も劇的に変化してきた。ソーシャルメディアやテクノロジー企業は、ユーザーデータの共有方法と共有相手の選択に関して一層厳しい監視に直面しており、個人データや機密データを実際には誰が所有しているのかという問題は、より複雑になってきた。

データ所有権の問題は、文化の影響も受けている。例えば一般論として、最近の欧州の人々の文化的見解によると、個人データは個人のみが所有できるという認識に向かって展開している。この見解は、個人の権利と、組織体がデータを所有しているという認識との間に、深刻な衝突を生み出している。

モノのインターネット（IoT）のようなデータ駆動型の新たなテクノロジーは、データ保護とプライバシーに関して新たな懸念を提起している。なぜならば、インターネットに接続されたセキュリティカメラ、スマートデバイス、双方向テレビのチューナー、スマートウォッチのような画期的なモノが、個人情報情報の使用方法や共有方法を再定義するからである。例えば、2018年に米国国防総省の分析官は、「兵士が身につけているフィットネス・トラッカーなどのウェアラブル・テクノロジーからの位置情報データを介して、敵が部隊の位置を特定する可能性がある」という、IoTの思いも寄らない影響に直面した。その結果、国防総省は在外職員によるIoTデバイスの使用を制限せざるを得なかった<sup>2</sup>。

IoTデバイスの導入が急加速しているため、個人データの保護とセキュリティに関する消費者の懸念は高まり、より切迫している。こうした消費者の懸念は、プライバシーとデータ保護の問題に取り組むようと、組織体とその内部監査人に圧力をかけている。

IoTデバイスに加えて、他の最新テクノロジーも、データのプライバシーに対する懸念をさらに高めている。人工知能（AI）と機械学習テクノロジーは、膨大な量のデータを収集している。これらはまさにその性質上、様々なデータポイントを、個人の行動や嗜好に新たな洞察をもたらす形で結び付け、最近のオンライン分析で指摘されているように、本来は個人的で機密である情報を作り出している<sup>3</sup>。

例えば、携帯電話用の販売アプリケーションは、AIテクノロジーを使用して、営業担当者のスマートフォンから位置情報やインターネットのアドレスを追跡し、その情報を顧客の所在地や購入履歴と組み合わせることができる。このAIアプリケーションによってパターンが明らかになると、会社や営業担当者が出張、時間および資源を効率的に管理するのに役立つ可能性がある。しかし、営業担当者は、雇用主が自分の位置情報、特に夜間や週末のデータを見ることに不快感を覚えるかもしれない。

このような複雑さのため、フォレスター・リサーチ社のバイスプレジデントで首席分析官のアンドラス・クザー氏は、「AIは多くのデータを必要とするため、プライバシーへの影響は一層大きくなる。個人を識別できるデータが、さらに収集される可能性がある」という見解を述べた<sup>4</sup>。

急成長を遂げているもう1つのテクノロジーであるブロックチェーンも、非常にデータ駆動型であり、独特のデータプライバシーの問題を提起している。ブロックチェーンのトランザクションは、すべてのトランザクションがネットワーク上のすべてのノードを通じてブロックチェーン・ネットワーク上のすべてのユーザーに表示されるため、変更や改ざんができないように設計されている。だが、機密情報がたとえ暗号化されていても、トランザクションのパターンを明らかにする可能

性があるので、個々のユーザーの識別に使用されるかもしれない<sup>5</sup>。

サイバー犯罪は、プライバシーとデータ保護について、急速に変化する別の側面を象徴している。サイバー犯罪者とそのツールがより巧妙化するにつれて、情報テクノロジーの専門家と組織体のリーダーも、所有する企業情報や個人情報を含む情報資産の保護というゲームで後れを取らないようにと悪戦苦闘してきた。

近頃注目を浴びた事例は、サイバー犯罪に関連するプライバシー・リスクの規模と範囲を示している。例えばフェイスブック社では、過去1年半にわたって大規模なデータ漏洩が相次いだ。具体的には、2018年9月に5,000万件<sup>6</sup>、2019年4月に5億4,000万件<sup>7</sup>、2019年12月に2億6,700万件的情報漏洩である<sup>8</sup>。

もちろんフェイスブック社は、単なる顕著な一例に過ぎない。近年、あらゆる種類や規模の銀行、医療機関、信用調査機関、小売業者が攻撃されている。調査機関の1つであるコンパリテック社が全米の10年分のデータ漏洩を照合したところ、2008年から2019年半ばまでの間に9,696件のサイバーセキュリティ侵害があり、合計107億件の個人データに影響を及ぼしていることが判明した<sup>9</sup>。政府や規制当局は様々な方法で対応してきたので、次節でその一部を考察する。第3のディフェンスラインという立場にある内部監査人は、所属する組織体が法規制上の義務を遵守して効果的に対応していることを検証する上で、周知の役割を担っている。

しかし、プライバシーとデータ保護に関連するリスクは、規制を遵守しないことによる罰金や罰則の可能性を超えたものである。個人データの不正使用、データ漏洩、不適切な通知や同意の実務、および関連する諸問題により、評判、業務、および事業継続のリスクが影響を受ける可能性もある。

その結果、今日の内部監査人とその所属組

織体は、プライバシーと機密データをどのように維持し保護するかを戦略的に考えなければならない。特に、内部監査人には、データ保護の課題について検証やアシュアランスを提供する明らかなニーズがある。しかし、このニーズと同時に、内部監査人にはさらなる洞察を提供し、組織体がこれらのリスクをモニタリングして対処するために、より積極的なアプローチを取るよう導く機会がある。

## 問題の定義、用語の定義

データ保護とプライバシーの問題をさらに検討する前に、関連する概念と用語を明確にすると役に立つかもしれない。「個人データ」という用語は、一体何を意味するのだろうか。個人の氏名、住所、生年月日、各種のアカウント番号のような、明白な例があることは確かである。しかし、コンピュータのIPアドレスや個人のウェブブラウザに保存されているクッキーのような、あまり明白ではない種類の情報についてはどうだろうか。

欧州のGDPRでは、個人データを「識別された自然人又は識別可能な自然人（「データ主体」）に関する情報」<sup>10</sup>と定義している。GDPRは、特定の人物に関するほとんどあらゆる種類の情報に適用することを目的としているため、定義は意図的に広範かつ一般的である。より明確にするために、GDPRは次のように続けている。「識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者をいう」<sup>11</sup>。

もっと簡単に言えば、個人データとは、誰かを識別するために使用され得るあらゆる情報である。しかし、ある情報が実際に個人情報であるかどうかの判断は、状況次第である。

英国のデータ保護の独立規制機関であるプライバシー監視機関（ICO）がGDPRに先立って公表した文書は、この違いをうまく説明している。ICOの説明は、次のように指摘している。

「氏名は、誰かを識別する最も一般的な手段である。しかし、潜在的な識別子が実際に個人を識別するかどうかは、状況次第である。ジョン・スミスという氏名は、その氏名を持つ個人が多いため、それだけでは必ずしも個人データとは限らない。しかし、氏名が他の情報（例えば、住所、勤務先、電話番号など）と組み合わせられている場合は、通常、1人の個人を明確に識別するのに十分である<sup>12</sup>。」

逆に、その個人の氏名を知らずに個人を識別することも可能である。身体的特徴や他のデータとの組み合わせ（例えば、年齢、性別、自宅住所、仕事、個人の所有物、オンライン・プロフィールなど）は、個人を識別するために使用することができる。したがって、たとえ1つのデータが個人データではないように見えても、それが他のデータと組み合わせると意味を持ち、個人の身元を合理的に証明するために使用される可能性がある。

大抵の組織体は、顧客、従業員、サプライヤー、およびその他のステークホルダーに関する様々な種類の情報を収集している。これらの情報を個人データと見なすべきかどうかは、その情報がどのように収集され、使用され、保存され、また、他の情報と結び付く可能性があるかに、ある程度依存する。結局のところ、あらゆる種類の組織体は、収集や処理をするほぼすべてのデータに注意を払わなければならない。

## 保護、プライバシー、およびレジリエンス（弾力性）

データの完全性、保持、および可用性はすべて、データセキュリティに対するアプローチ全般の重要な特徴である。しかし、データ

保護に対するセキュリティだけのアプローチは十分ではない。

先に示唆した文化的な問題、すなわち、個人データが、データを取得や保存する組織体ではなく個人に帰属すると認識されていることは、今ではGDPRのような規制に成文化されつつあり、プライバシーを基本的人権として確立している。現在のデータ保護実務では、データを安全に保存することと、データ所有者（個人）が特に許可した分野に個人データの使用を制限することの、両方に対応しなければならない。

言い換えると、組織体は、この個人データを特定の事業目的のために基本的には借りており、あらかじめデータ主体が同意した範囲内でこれを使用しなければならない、ということを理解し始めている。

「干渉されない権利」と定義されることもあるデータプライバシーの概念も変化している。現在、データに基づく個人のプライバシーは目に見えない問題ではなく、どのような種類のデータが収集され、誰がアクセスでき、どのように使用され、どのくらいの期間保存されるか、という問題になっている。

プライバシーやデータ保護に関連する法令を遵守していることを実証した企業とのみ、データを共有することを選択する人々が増えている。ソーシャルメディア・サイトが個人を識別できるユーザー情報を収集して、研究機関や他の企業と共有したような有名なデータ侵害は、データ所有者の認識や同意なしに情報が共有される可能性があることを示している。また、このようなデータ侵害例は、個人データの不正使用に関連するリスクを消費者に思い出させる役割も果たしている。

雇用主も、データ運用の実務をデータ保護原則に合わせなければならないと気付いている。個人所有のデバイスを会社のネットワークに接続すると、雇用主がある程度のリスクに曝される可能性があるため、従業員が会社

のネットワーク上で個人のモバイルコンピューティング・デバイスを使用している間は、個人のプライバシー権を大幅に制限、または完全に排除するという利用規定に署名することを、組織体が従業員に義務付けることが次第に一般的になってきている。同時に、雇用主は、従業員のプライバシー関連の期待を、GDPRや他のデータプライバシー規制の下で従業員に与えられたものとして考慮する必要がある。

別の言い方をすれば、セキュリティなしではプライバシーは存在できないが、プライバシーがなくてもセキュリティは存在し得るので、組織体や従業員から見れば理想的な状況ではない。テクノロジーの継続的な進歩に伴い、組織体と個人は、適切かつ効果的なデータ運用をしながら関連のあるソーシャルメディアでやり取りをすると同時に、データの保護、データの脅威、およびセキュリティとプライバシーを提供するために必要な手順についての認識と知識を高めなければならない。

プライバシーとデータ保護は、もはや単なるセキュリティ上の課題ではない。実際、セキュリティだけでは不十分である。セキュリティと同様に、プライバシーは組織体の文化に不可欠でなければならない。その目的は、プライバシーとセキュリティ関連の考え方を総合的なアプローチに統合し、セキュリティとプライバシーの専門家が一緒になって、一般的なデータ保護という共通のゴールに向かうことである。

今日の環境下では、一方では新たな規制と基準が生まれ、他方では消費者とステークホルダーの期待が高まっているため、データ保護とプライバシー・プログラムの重要な要素としてレジリエンスの概念に焦点を当てる先見性のある組織体が増えている。

「レジリエンス」は、プライバシーとデータ保護の問題への取り組み方を考えるときに最初に思い浮かぶ言葉ではないかもしれな

い。ただし、ゼロから出直したり、コンプライアンスの取り組みをやり直したりすることなく、新しい要件を吸収して適応できるという意味で、関連する課題の多くに対処している。

レジリエンスの辞書的な定義は、強靭性や弾力性に加え、困難から迅速に回復する能力のような概念を指す。プライバシーとデータ保護の実務という状況では、強靭性は必ずしも最も重要な要素ではないが、レジリエンスの他の側面である弾力性と回復力は、確かに重要な要素である。規制要件、ステークホルダーの期待、およびテクノロジー自体が進化し続けているので、組織体が迅速に適応するためには、弾力性と回復力の両方が必要だろう。

一方で内部監査は、弾力的なデータ保護策の有効性をしっかりと検証できる品質を示す必要がある。内部監査人協会（IIA）と関連機関（本稿の第3節で詳細に説明）が行った最新の研究によると、内部監査の専門家は、データのプライバシーとそれに関連する諸問題を、対処すべき主要なリスクと考えることが増えている。しかし同時に、これらの諸問題は、内部監査人に貴重な機会ももたらしめている。内部監査人は、データ保護とプライバシー・プログラムの有効性についてアシュアランスを提供することに加えて、組織体の回復力を高めたり、リスクが進化し続けても効果を維持したりするために、積極的な役割を果たすこともできる。

## 2. 法規制の状況、コンプライアンス、その他のリスク

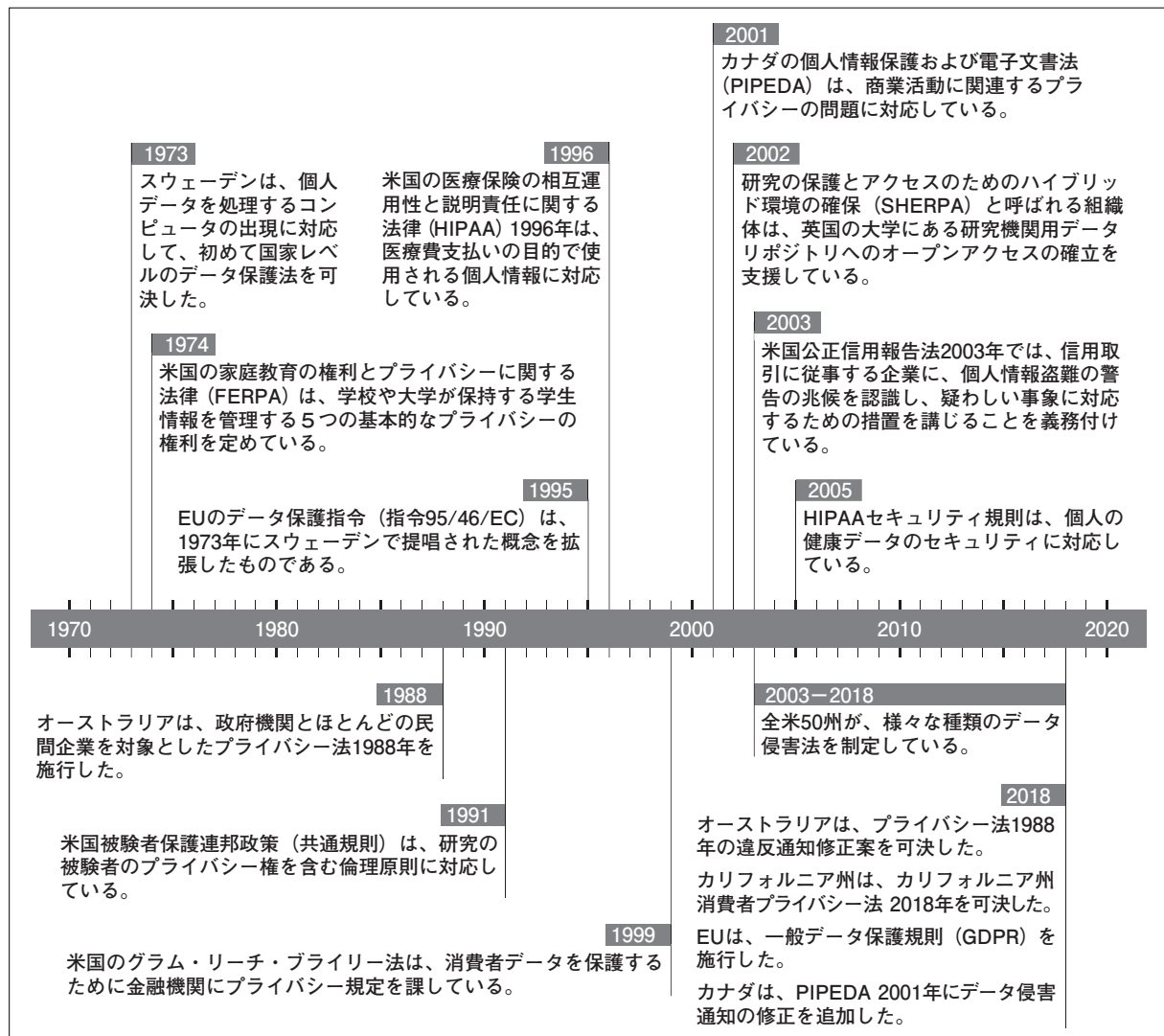
データ主体のセキュリティとプライバシーを保護するために、様々な政府機関と様々な地理的場所の規制当局がデータ保護活動を強化し続けているので、プライバシーとデータ保護の状況は一層複雑になっている。現在、

事実上どの法域においても、顧客、従業員、サプライヤー、またはその他の第三者との関係を持つあらゆる組織体は、増え続ける数々のプライバシーとデータ保護に関する具体的な要件の対象となっていることがわかる。

## 規制環境の進化

本節で後述する有名なGDPRは、既に施行されているか現在検討されている多くの同等の規制構造の1つに過ぎない。デジタルデータが登場して以来、約100か国と全米50州で個人データの保護を目的とした法律を制定している（図表1）。多くの州では、プライ

<図表1> プライバシーとデータ保護の進展



注：例を示したに過ぎず、完全なリストではない。

【出典】 Croweによる分析

バシーに特化した規制はないが、事実上すべての州で、データ侵害の取り扱いに関する法令要件が施行されている。これらの法令の多くは、GDPRと同様に、個々の法域をはるかに超えて効力を持つ包括的な法律である。

## GDPRは素晴らしい新世界か

長期にわたって可決されてきた個人データの保護とプライバシーを規定する多くの新しい規制構造の中でも、EUのGDPRは明らかに近年で最も有名である。GDPRは、1995年の「データ保護指令」に代わって2018年に発効した。GDPRは、EU加盟国の市

民の個人データを処理する組織体に対して、データプライバシーとセキュリティの多数の要件を導入した。

GDPRは、EU市民と居住者の個人データを処理する組織体、あるいは、EU内に居住者または訪問者として滞在している個人にサービスを提供する組織体に適用される。営利と非営利の両方を含む、あらゆる業界やセクターの組織体は、物理的にEU域内に拠点を置くか、EU域内で事業を行っているか、単にEU居住者に商品やサービスを販売しているかを問わず、この規制の対象となる。ただし、EU居住者に対する商品やサービスの販売でGDPRが発動されるのは、その販売が目的に合ったものである場合、つまり商品やサービスが明らかにEU居住者に販売される場合のみであることに注意されたい。EU域内の誰かが米国を拠点とするウェブサイトから購入しただけでは、GDPRは自動的に発動されない。

前述のように、GDPRの個人データの定義は、当該自然人に関する「身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性」に特有な要素を含む、「識別された自然人又は識別可能な自然人」に関するあらゆる情報を対象としている<sup>13</sup>。これは、以前のEUデータ保護指針からの重要な拡大である。

GDPRは組織体に、個人データの処理方法に関して個人の選択を尊重するよう義務付けている。同意の文書は、わかりやすい言葉で作成しなければならず、また、どのような個人データを収集し、どのように使用し、どこでどのように共有するかを説明しなければならない。さらに、データ侵害を確認したら72時間以内に関係当局に報告しなければならない。

多くの組織体はGDPRを遵守するために、通知、同意、およびデータ収集のために、新たなプロセスを開発したり既存のプロセスを

大幅に改善したりしなければならなかった。GDPRの影響は、影響を受けた組織体全体で感じられたことであって、決してIT部門に限定されないと認識することが重要である。

## EU域外の進展状況

EU域外の多くの国々でも、データプライバシー制度を再構築している。例えばブラジルでは、従来のデータ保護法のフレームワークは、様々な経済セクター間で矛盾していたため広く施行されていなかった。しかし、長年の努力の末、新たな一般データ保護法が2018年に可決され2020年に施行される。

この新法は、EUのGDPRの多くの概念に基づいているが、その他の事項も加えている。ブラジル市場にサービスを提供し、ブラジルに所在するデータ主体の個人データを収集する外国企業は、ブラジル国内に物理的な拠点があるかどうかに関わらず、同法の対象となる。

多くの人々は、ブラジルの新しいデータ保護法が最終的には他のラテンアメリカ諸国の模範になるかもしれないと期待しているが、地域全体で一貫している状況とは程遠い。例えば南米大陸では、EUが適切と認める一般的なデータ保護法を施行しているのはアルゼンチンとウルグアイの2か国だけであり、EU加盟国とこの2か国との間では、EU居住者の個人情報が自由にやり取りできる<sup>14</sup>。

コロンビアは、強力な規制に支えられた進歩的なデータプライバシー制度があると、一般に認識されている。実際、プライバシーの権利とデータを修正する権利という2つの基本的な個人データの権利が、憲法に規定されている<sup>15</sup>。メキシコは、2010年と2017年に包括的な連邦データ保護法を可決し、政府機関は近年4つの規制文書や指針を追加で公表してきた<sup>16</sup>。特定の経済セクターのみを対象とするデータ保護法があるのは4か国であり、データ保護法が全くないのは1か国である<sup>17</sup>。

このように規制体系が多種多様なことから、ラテンアメリカ全域に利害関係のある組織体は、データ保護要件を遵守することがセキュリティチームとデータチームだけでなく、それらの取り組みと結果を検証する内部監査グループにとっても深刻な課題であると認識している。

アジアでも同様に、データ保護の状況は様々である。例えばインドでは、特に同国の非常に盛んなテクノロジー・セクターを考慮して、多くの人々が不十分と考えてきた要件を満たすべく、初めての包括的なデータ保護法をめぐる論争が展開された。この法案の詳細をめぐる議論は数年間続いたが、2019年12月4日、連邦内閣は「個人情報保護法案」を可決した<sup>18</sup>。この長年の議論は、バックオフィス機能をオフショアからインドに移したいと考えている多くの企業に課題をもたらしているが、欧州企業や多くの多国籍企業は、強力で包括的なデータ保護の規制構造がない場所で、自社のデータ処理機能が運営されることには反対している。

中国のデータプライバシーのフレームワークは、最近まで、様々な法律とセクター固有の法令で構成されていた。しかし、2017年と2018年に、中国の消費者はソーシャルメディアとインターネット企業による個人データの使用をめぐる数件の注目すべき論争を受けて、より具体的なプライバシー権を要求し始めた。中国の全国人民代表大会は、2018年後半に、新しい個人情報保護法が正式に次期の議会の議題となったと発表した。一方で新法が起草されている間、国家最高のインターネット規制当局である中国サイバースペース管理局は、新法の今後の方向性を示す新しい指針を発表した<sup>19</sup>。

日本は最近、「個人情報の保護に関する法律」を改正してGDPR基準に近付けた。2019年初頭、日本政府はEU諸国から移転されたデータにのみ適用される一定の補完的ル

ールを採択した<sup>20</sup>。韓国で個人データは、包括的な一般データ保護法とセクター固有の法令によって保護されている。2019年にはテクノロジー・セクターの改正法令が施行され、さらに、他のデータ保護法の改正法案が現在、数件検討されている<sup>21</sup>。

## 米国のデータ保護制度

米国内では、大半の州が過去15年間にデータ保護規制を公表しているが、大多数はデータ侵害への対応に重点を置いている。多くの州の法令には共通の要素があるが、それらは実質的には個々の法令の寄せ集めのようなものである。現実問題として、個々の法令に対する遵守状況は、通常、各州の要件に照らして個別に分析する必要がある。

また、個人情報を処理する際に事業者がデータセキュリティの実施を義務付けることに加えて、11州ではさらに進んで、事業者とベンダーとの契約にデータセキュリティ規定を組み込むことも義務付けている<sup>22</sup>。同様に、特定の業界に対してデータプライバシーの問題に対処する法令を施行している州もあるが、あらゆる経済セクターに適用される広範なデータプライバシー施策を策定している州は、ほんの数州に過ぎない。

カリフォルニア州では、「カリフォルニア州消費者プライバシー法2018年（CCPA）」がこれまでで最も包括的なアプローチと考えられており、プライバシーへの広範な対応が始まっている。2020年1月に施行されたCCPAは、主に包括的かつ広範であることから、米国版GDPRと呼ばれることもある。しかし、このような比較は、2つの構成の多くの重要な違いを見落としている。

GDPRと同様にCCPAは、他の州や国に拠点を置く多くの組織体に遵守を求めている。CCPAの場合、年間5万人以上のカリフォルニア居住者の個人情報を取得する組織体、年間総収入が2,500万ドルを超える組織

体、またはカリフォルニア居住者データの販売によって収入の過半数を得ている組織体は、同法を遵守しなければならない<sup>23</sup>。

GDPRとCCPAは、基本的な用語や定義といった根本的なものを始め、多くの重要な点で異なる。GDPRの個人データの定義が広範で多少包含的なとは異なり、CCPAは、「個人情報」（「個人データ」ではない）を、具体例の長いリストにして非常に明示的に定義している。また、「個人情報」に含まれない情報も列挙している<sup>24</sup>。

CCPAでは、カリフォルニア州の居住者は、組織体が保有する個人情報の開示を請求し、その個人情報を消去させ、その情報の販売に異議を申し立てる権利がある。また、要請があれば、組織体はデータの使用方法や共有者についての情報を提供することが義務付けられている。さらに、同法は、検証プロセスの策定、明示的なオプトイン<sup>a</sup>同意の取得、広範な通知と文書化要件の遵守など、組織体が取らなければならない一連の事前措置の概要を説明している<sup>25</sup>。

### コンプライアンスを超えるリスク

急増しているデータ保護やプライバシー規制の対象となる組織体は、たとえ気付いていなかったとしても違反していれば違反ごとに数千ドルの罰金が科せられることがあるため、重大な財務リスクに直面する可能性がある。しかし、罰金や制裁金は、規制に違反した場合に組織体に生じ得るリスクの1つに過ぎない。

多くの場合、プライバシーとデータ保護の規制当局は、救済策が講じられるまで、データの国際的な移転を停止するよう命じることができる。また、規制構造を遵守するために外部の支援を求めることを、組織体に強制す

ることもできる。

さらに、規制要件に違反したことが確認されると、有名な報道機関から公表されることが多いため、コンプライアンス違反に関連する評判の低下は著しく、また長期間続く。組織体が加害者であるか、データ侵害や盗難の単なる被害者であるかに関わらず、様々な法域のステークホルダーに適用される各種の通知や軽減措置に従わないと、重大な責任を負うことになる。

組織体は個人のデータプライバシーの問題だけでなく、ミッション・クリティカルな情報<sup>b</sup>や他の業務上の機密情報を危険に曝す、データ侵害に関連する業務運営上や財務上のリスクも認識しなければならない。研究成果、独自の公式、または重要な業務データなどの盗難や取り返しのつかない損失は、組織体を存続の危機に曝すことになり、最終的には、事業継続性に関する問題や懸念を引き起こす可能性がある。財務から存続までの様々なリスクは、内部監査が十分な注意を払うに値する。

## 3. 内部監査にとってのデータ保護の課題と懸念

現在の組織体にとって、プライバシーとデータセキュリティの課題は広範かつ多大な影響を及ぼすため、データ保護に関連するリスクは、内部監査専門職の大きな懸念事項となっている。

### データ保護の課題に対する内部監査人の見解

サイバーセキュリティとデータプライバシーは、新たに発表された「Risk in Focus 2020（2020年に注目するリスク）」調査に参

訳注<sup>a</sup> 企業などが個人情報を収集・利用しようとする場合、事前に本人が承諾すること。

訳注<sup>b</sup> 障害などによる中断を許されず、年中無休体制を要求される基幹業務およびそれを支えるITシステムの情報。

加した欧州の内部監査専門家にとって突出した懸念事項であった。この調査結果は、英国、アイルランド、ドイツ、ベルギー、オランダ、スペイン、スウェーデン、フランス、イタリアのIIA国別代表機関の連合体が2019年9月に発表した。

この調査の回答者の4分の3以上（78%）は、所属する組織体が現在直面している上位5つのリスクの中にサイバーセキュリティとデータセキュリティを挙げている<sup>26</sup>。これは3年連続であり、データ保護関連の問題は監査人の最大の懸念事項であった<sup>27</sup>。

データの公表にあたり、調査レポートは、GDPR導入後最初の8か月間に、欧州全体で推定5万9,000件の個人データの侵害が発生したと指摘している。同レポートによると、サイバーセキュリティは「現代では永遠のリスク<sup>28</sup>」であり、「サイバーセキュリティとデータ保護やプライバシー・リスクの収れんは継続する」と予測している<sup>29</sup>。

欧州の連合体の調査結果は、IIAが行った最新のグローバルな調査結果と一致している。IIAの新刊「OnRisk 2020（2020年のリスク）」は、内部監査専門家、取締役および経営幹部を対象に行った定量的・定性的調査結果を組み合わせたレポートである。

この調査結果を分析したところ、サイバーセキュリティ、データ保護、およびデータ倫理は、2020年に組織体へ影響を及ぼすと認識されたトップリスクの1つであることが明らかになった。同レポートは、内部監査を含むリスク・マネジメント機能に携わる人々の一部にとって、「サイバーセキュリティ、およびデータや新たなテクノロジーは、知識がかなり不足している分野である」と指摘した。さらに同レポートは、「知識が不足している分野と関連性の高いこれらのリスクは、リスク・マネジメントの担当者が優先的に知識を身につけるべき2つのリスク分野であることを示唆している」と述べている<sup>30</sup>。

## 内部監査とデータ保護が交差する場所

プライバシーとデータ保護に関連するリスクについて洞察とアシュアランスを提供する内部監査人の取り組みは、これらのテーマに関連するリスクと優先順位が常に変化しているために、明らかに複雑になっている。現在のプライバシーやデータ保護プログラムと、それらをモニタリングする責任を負う内部監査機能は、弾力的で適応力がなければならない。内部監査機能は、現在の環境においても有効であると同時に、未確定の将来のリスクや状況を積極的に予測しなければならない。

有効なプライバシー・プログラムを策定することは、気の遠くなる作業かもしれない。関与するプロセス数の多さ、データが使用される場所と方法の多さ、収束しない規制要件、および作業の規模は、圧倒的かもしれない。このような環境は、問題を理解して第3のディフェンスラインの役割を果たすために必要な資源を揃える際に、内部監査機能にリスクをもたらす。しかし同時に、この環境は、内部監査が助言業務で組織体に価値を付加する機会を開くことにもなる。

強固で先を見越した内部監査プログラムは、もともとリスクベースであり、組織体が認識している最も高いリスクを最も重視している。データ保護とプライバシーの分野では、組織体は最もリスクの高いデータを特定し、それがどのように使用されているかを追跡するための体制を構築しなければならない。最もリスクの高い分野に最初に焦点を当てれば、組織体は幅広く重要な、そして戦略的でさえある、個人データの使用と保護に関連する以下のような質問に答えることができるようになる。

- 最もリスクの高い分野は何か。あらゆる組織体が最も高いリスクと見なす事業上の機密情報以外で、組織体が保持するユーザーの個人情報の観点から見てリスク

や機密性が高いデータは何か。

- 組織体は、プライバシー侵害の可能性を予測し、侵害を事後検出するのではなく事前に防ぐための先を見越した強力なプライバシー・プログラムを、どうすれば策定できるか。
- 組織体は、データ保護プログラム全体を最初から再設計することなく、強力な弾力性があり、新たな規制の影響を吸収できるデータ保護基盤を、どうすれば構築できるか。
- データ主体のプライバシーの保護が、追加手続ではなく初期設定となるように、業務プロセスをどのように改訂できるか。
- プライバシー保護をどのようにITシステムに組み込むことができるか。
- 必要な機能を犠牲にすることなく、プライバシーを設計上組み込むためにどのような措置が取れるか。
- プライバシー規制によって特定の機能が継続的に使用できない場合、組織体はどのような措置を取るのか。
- プライバシー・バイ・デザインの要件<sup>6</sup>は、プロセスまたはシステムのライフサイクルを通じてどのように拡張できるか。
- 監査人とプライバシー担当役員の間、優先順位や懸念事項に関する期待ギャップはあるか。

内部監査部門も準備をすべきであり、また、進んで自部門の役割と実績を熟考すべきである。自問すべき重要な質問には、次のようなものがある。

- 内部監査は、組織体に過度の圧力や極端な追加コストをかけずに、どうすれば迅速かつ効率的に対応できるか。
- 要件の遵守を検証する以外に、内部監査は、アカウントビリティや開示性をさら

に提供するために、他に何ができるか。

- データのプライバシー、データの完全性、およびデータのアクセス可能性の問題について、組織体内での認識を高めるために、内部監査はどのような役割が果たせるか。これらの同じ分野において経営者のアカウントビリティを高めるために、内部監査はどのような支援ができるか。
- 内部監査は、データ保護において、どのような役割を果たすべきか。
- コンプライアンスの観点から、内部監査自体のエクスポージャーはどの程度か。

## 一般に認められた10のプライバシー原則

組織体がこのような質問へ取り組み始めるための方法の1つは、プライバシーとデータ保護に弾力性のあるフレームワークを採用することである。一般向けや業界固有の様々なサイバーセキュリティ・フレームワークがあるが、2つ例を挙げると、米国国立標準技術研究所（NIST）が策定したNISTサイバーセキュリティ・フレームワーク、および国際標準化機構（ISO）と国際電気標準会議（IEC）が公表したISO/IEC 27000サイバーセキュリティ・フレームワークは、データの漏洩、侵害、およびその他の問題に迅速に対応して回復するための基盤を提供している。2020年1月、NISTはさらに一歩進んで、新しいNISTプライバシー・フレームワークの第1.0版を公表した。このフレームワークは、「全社的リスク・マネジメントを通じてプライバシーを改善するためのツール」と説明されている<sup>31</sup>。

NIST以外にも多くの組織体が、基本的なデータ保護プロトコルの域を超えることの重要性を認識して、特にデータのプライバシ

訳注<sup>6</sup> GDPR Article 25 Data protection by design and by default（GDPR 第25条 データ保護バイデザイン及びデータ保護バイデフォルト）の内容を指すものと解される。

一の問題に取り組んでいる。そうした中でも、明確なプライバシー・フレームワークを策定するためのモデルとして、米国公認会計士協会（AICPA）などの組織体が策定した一般に認められた10のプライバシー原則（GAPP）が多くの注目を集めている（図表2）。

＜図表2＞AICPAの一般に認められたプライバシー原則

1. **管理。**組織体は、プライバシー方針と手続を定義し、文書化し、伝達し、アカウントビリティを割り当てる。
2. **通知。**組織体は、プライバシー方針と手続に関する通知を行い、個人情報の収集、使用、保持、および開示の目的を明らかにする。
3. **選択と同意。**組織体は、個人が利用できる選択肢を説明し、個人情報の収集、使用、および開示に関して黙示的または明示的な同意を得る。
4. **収集。**組織体は、通知で明らかにした目的のためにのみ個人情報を収集する。
5. **使用・保持・廃棄。**組織体は個人情報を、通知で明らかにして黙示的または明示的な同意を得た目的に限定して使用する。組織体は個人情報を、明示した目的の遂行に必要な限り、または法令等により要求された場合に限り保有し、その後は適切に廃棄する。
6. **アクセス。**組織体は個人に対して、個人情報のレビューと更新のためのアクセスを提供する。
7. **第三者への開示。**組織体は、通知で明らかにした目的のために、個人から黙示的または明示的な同意を得た場合に限り、個人情報を第三者に開示する。
8. **プライバシーのセキュリティ。**組織

体は、(物理的および論理的の両方の)不正アクセスから個人情報を保護する。

9. **品質。**組織体は、通知で明らかにした目的のために、正確で、完全で、関連性のある個人情報を保持する。
10. **モニタリングと執行。**組織体は、プライバシーに関する方針と手続の遵守状況をモニタリングし、プライバシーに関する苦情や紛争に対処するための手続を整備する。

[出典] <https://iapp.org/media/presentations/11Summit/DeathofSASH02.pdf>

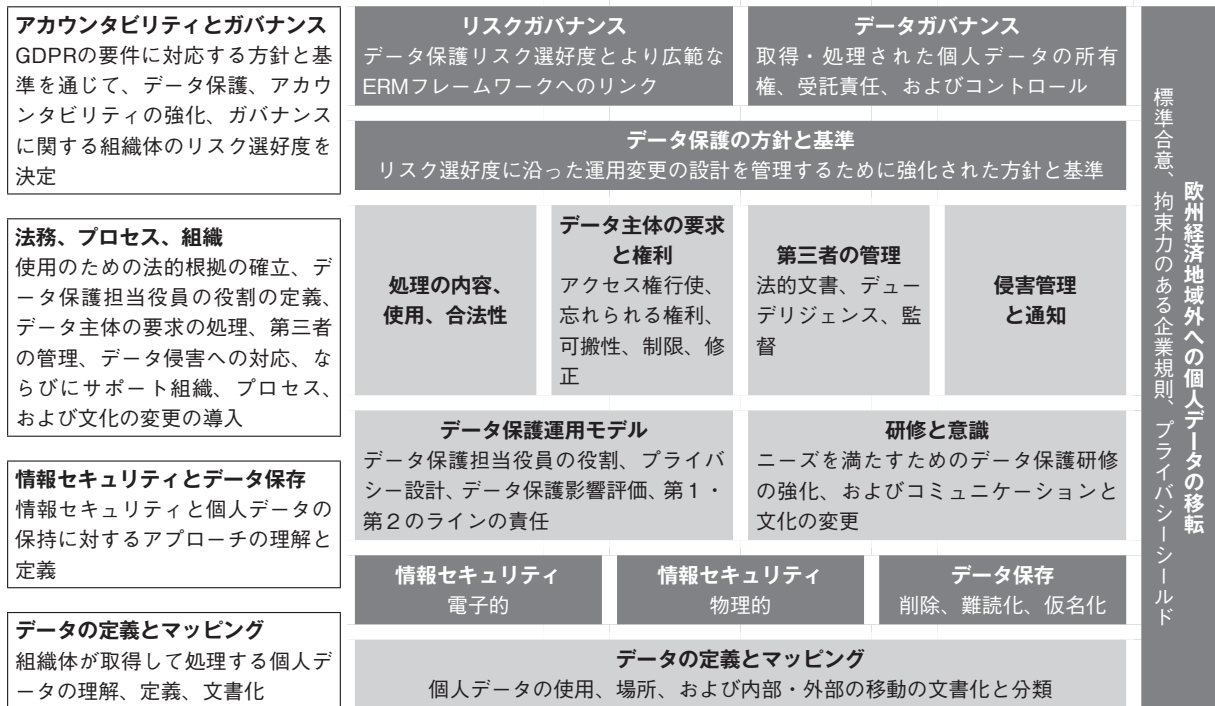
これらの10の原則は、すべてのリスク担当者が弾力性のあるプライバシーとデータ保護プログラムを構築するための一般的な基礎を提供するものであり、特定の関連リスクについて監査を計画する際のフレームワークと方法論も含まれている<sup>d</sup>。より技術的なサイバーセキュリティ基準と比較すると、GAPPの構成はプライバシーの基盤を構築し始めるための、より簡単でアクセスしやすい方法も示している。

#### 4. 弾力的にデータ保護に取り組むためのフレームワーク

前述のように、強固で弾力的なリスクベースのプライバシー・プログラムを策定して導入するプロセスは、難問かもしれない。GAPPの10の原則は、基礎知識や基盤となり得るし、様々なサイバーセキュリティ・フレームワークは、策定用のテンプレートとして利用することができる。しかし、大抵の組織体は、最終的には構成と方向性を示す明確なプライバシーとデータ保護のフレームワークを備える必要があると認識している。

訳注<sup>d</sup> GAPP「CPA and CA Practitioner Version」には、付録として監査実務家用のガイダンスや監査報告書の雛形も示されている。

<図表3> プライバシーとデータ保護のフレームワーク例



[出典] Croweによる分析

### フレームワークの構成要素と構造

図表3は、フレームワークの構成方法の一例である。この例でフレームワークは、効果的なプライバシーとデータ保護プログラムの一部として考慮すべき重要な要素に対応するように設計されている。このフレームワークには、必要とされるアカウントビリティとガバナンスの体制、対処しなければならない法的問題と組織的問題、および、効果的なプライバシーとデータ保護プログラムの不可欠な要素である重要データのセキュリティとデータ管理機能の詳しい説明が含まれている。

### 内部監査の役割：統合的アプローチ

内部監査には、弾力的なフレームワークの策定と適用を支援する上で果たすべき重要な役割がある。そのような中で内部監査は、組織体に価値を付加する重要な機会に遭遇する可能性もある。

通常の場合と同様に、内部監査チームがフレームワークを策定して導入するプロセス全体で他のステークホルダーとチームを組め

ば、プロセスはより効率的になり、最終的にプライバシーとデータ保護プログラムが、より効果的になる。様々なステークホルダー間のコミュニケーション、調整、および統合は、リスクと機会を明らかにして最初に評価する際、すなわち、プロセスの初期段階で特に重要である。

## 5. フレームワークの導入と遵守状況の監査

プライバシーとデータ保護プログラムを策定して導入し、その後、遵守状況と有効性を監査することは、当初は、圧倒的に複雑で入り組んだプロセスのように思えるかもしれない。しかし、あらゆる複雑な施策と同様に、作業を数段階に分割すると、より管理しやすくなる。

### 推奨する導入方法と監査方法

図表4に示すように、第1段階は、プライバシーとデータ保護のフレームワーク自体の

選択である。前節で示したフレームワーク例のような、関連性のある適切なフレームワークを選択すると、作業を始める手掛かりとなり、範囲を決定し実施手順を伝達するための基礎になる。それ以外にもフレームワークは、評価やコミュニケーションの形式を確立するので、プライバシーとデータ保護プログラムの要件をリンクさせて明確にする際と、導入したプログラムの全般的な有効性に関する監査結果を報告する際の両方、つまりプログラム全体を通して使用することができる。

#### <図表4>プログラム導入手順

##### 1. 関連性のあるプライバシー・フレームワークを見極める。

- 複数の規制に対応するフレームワークを選択する。
- フレームワークを使用して、内部監査と主要なステークホルダーとの共通用語を作成する。
- 規制要件、関連するビジネスリスク、認められたプライバシー手続を関連付け、それらを導入されたコントロールと結び付ける。

##### 2. 組織体のプライバシー関連リスクを評価する。

- 製造業者の営業秘密や従業員のデータ、金融機関の顧客や従業員のデータなど、組織体が収集・保持する重要な種類のデータを特定する。
- 国内、地域、国際的に、組織体がどこで、どのように事業を行っているかを評価する。
- 選択したプライバシー・フレームワークによって特定した最も高いリスク分野を強調する。

##### 3. リスク評価結果を活用して監査計画を策定する。

- 範囲を決める。
- 監査計画を決定する理由となるリスク

を伝える。

- 実施する監査手続がどのように結論を裏付け、影響力のある提言を導き出すのに役立つかを説明する。

##### 4. 策定した内部監査計画を実施する。

- 策定したフレームワークを使って発見事項を伝達し、特定されたりリスクと緩和するためのコントロールとの結び付きを、ステークホルダーとプロセスオーナーが理解できるようにする。
- 例外を特定し、現状と原因の両方を明らかにする。
- 修復または是正措置のための提言を作成する。

##### 5. 経営者が策定した是正措置の完了をモニタリングする。

- フレームワークを利用して、現状と比べた望ましい状態を示す。
- ステークホルダーとプロセスオーナーに視覚的イメージを示して、適切なコントロールの相対的な水準を明らかにする。

[出典] Croweによる分析

第2段階は、プロジェクトのリスク評価を実施して、組織体のプライバシーとデータ保護の真のリスクを明らかにし、協働すべきステークホルダーを見極め、関連するプロセスオーナーを特定することである。回答すべき重要な質問には、次のようなものがある。

- 組織体が収集または保持する重要な種類のデータはどれか。
- 組織体はどのような法域で事業を行っているか。
- 研修、ガバナンス、所有権などの問題を扱った、データプライバシーに対する体系化された手法はあるか。

リスク評価の結果、より高いリスクとして明らかにされた分野を強調すべきであり、第3段階である監査計画を策定して範囲を決め

るために使用すべきである。初年度のリスク評価結果を使用して、将来的に（リスク対応を）強化したり策定を進めたりする分野を特定している組織体もある。また、初年度のデータマッピング手続に主に焦点を当てて、アプローチと結果が完全で持続可能であるというアシュアランスを提供することを選択する組織体もある。リスク評価結果を理解することにより、組織体は関連データを特定して適切なコントロール活動を実施することができる。

第4段階は、内部監査計画を実施し、選択したフレームワークを使用して結果を伝達することで、特定したリスクと期待するコントロールとの間の明確な関連性を示すことである。例えば、当初の監査範囲では完了したデータマッピング作業の評価に焦点が当てられていて、監査の結果、すべての重要なプロセスが組織体のデータマッピング作業に含まれていないことが判明したと仮定する。この発見事項は、以下を明らかにするような方法で、明確に伝えるべきである。

- 規準（考慮すべきすべての重要なプロセス）
- 現状（考慮していなかったプロセス）
- 原因（そのプロセスが含まれていなかった理由）
- 結果（影響の財務的な定量化）
- 是正措置（何をいつ行うか、経営者が是正措置に同意しているかを含む）

監査報告書での記載例は、以下の通りである。

「手続の実施中、品質保証書の管理に関連するプロセス活動が組織体のデータマッピング作業に含まれていないことが判明した。このプロセスをデータマッピング作業に含めないと、組織体が取得、保持、および使用するデータを完全に識別できなくなる可能性がある。このデータを識別できないと、データ保持方針に従ってデータが保持されているか、

顧客との接触データに追加の同意コントロールを適用する必要があるか、適切なデータセキュリティ対策が適用されているか、個人を識別できるデータが存在するか、を判断する組織体の能力が制限される。これにより、組織体は規制違反に対して罰金や制裁が課されるリスクが増加するとともに、そのような違反の結果として評判リスクに曝される。」

監査報告書の意見には、是正措置の提言も含めるべきである。

監査意見を表明した後は、第5段階である、経営者が策定した是正措置の完了のモニタリング、およびプライバシーとデータ保護に関連したリスク分析を行うことに進む。フレームワークに簡単な色分けの方法を取り入れると、適切にコントロールされていない分野（赤）、部分的にコントロールされている分野（黄）、および適切にコントロールされている分野（緑）といった視覚的なイメージが示せる。リスクに関連する分野とは見なされない要素（例えば、国内だけで事業を行う組織体における国境を越えた移転など）は、青で示すことができる。

このようにして、組織体が重要な要素への取り組みを開始して弾力性を高める方向に進むと、フレームワークは、プログラムの成熟度の向上とコントロールの有効性の改善に向けて、進捗状況を視覚化、追跡、伝達する明確で直感的に理解しやすい方法が示せる。

### 事例研究：プライバシー・フレームワークの適用

高性能のトラック部品（専用ライト、カスタムグリル、車内宿泊設備など）の開発・販売に力を入れているA社は、B2B企業として30年以上、北米全域で事業を行ってきた。同社は大手の長距離輸送トラック会社から買収を提案されており、合併会社の年間収益は20億ドルと推定された。

経営陣は、この買収提案に色めき立った

が、その主な理由は、トラック部品事業の収益目標達成の可能性である。しかし、長期的な観点から、経営陣は顧客の販売データを他の利用可能なデータベース（典型的なドライバーの移動ルート、買収候補となる他の運送会社、その他の関連データなど）と組み合わせる潜在的な機会も見出した。

取締役会での取引の検討中に、取締役の1人が、会社が計画した方法で情報を統合することに付随するプライバシー関連の影響について質問した。議論の後、取締役は内部監査部門長（CAE）に、新たな合併会社のプライバシーとデータ保護の現状に関する監査を実施するよう提案した。

ここで概説したフレームワークと内部監査のアプローチを使用することにより、CAEは以下を対象とする明確な監査計画を策定することができた。

- ドライバーの移動ルートや顧客の販売データに関するデータガバナンスなど、取り上げるべき重要な要素
- データの使用方法に関する顧客への連絡を含む必要な同意要件
- 監査結果を取締役に報告するための明確な報告の仕組み

買収の一環として説明された、関連する事業目標に合わせたリスクベースのアプローチを使用して、CAEは経営陣が関連するリスクを特定して定量化し、提案された買収を支援し迅速化し得る適切なリスク軽減策の策定に役立つことができた。

## 結論とさらなる研究

現在の急速に進展している規制環境は、データ・テクノロジーの継続的な進歩やプライバシーとデータ保護の課題に対する認識の高まりと相まって、内部監査人に特有の課題を提起している。これらの課題の緊急性は、欧

米双方で近頃行った内部監査専門職の調査で示された懸念に反映されている。

事実上すべての場合において、データ保護とプライバシーに関する懸念に適切に対処するには、組織体内の様々な部門や機能を越えた連携による職務横断的な取り組みが必要である。内部監査人は、所属する組織体の現在のデータ環境に照らして自身の準備水準を評価することによって、この分野でより積極的な役割を果たし始めることができる。

本稿で示したフレームワークと導入方法は、組織体がデータプライバシー関連のリスクを管理して軽減するために、関連するコントロールの策定と実施を支援する上で成功した1つのアプローチである。しかし、テクノロジー環境と規制環境の双方ともに進化し続けているので、組織体全体、とりわけ内部監査部門は、ステークホルダーの期待の変化に迅速に適応できるようにする必要があるだろう。

今後数か月間、本稿の著者は、これらの課題に対する内部監査専門職の対応を評価し続けることになる。本研究の次の段階では、内部監査財団会員に対するアンケートと、非公式な事例研究や現地インタビューなどの追加調査を行う。この第2段階の目標は、専門職が継続中の課題にどのように対応しているかを評価することであり、発見事項のレポートは2020年後半までに公表予定である。

2021年初頭に完了予定の本研究プロジェクトの第3段階では、様々なステークホルダーがデータのプライバシー問題をどのように捉えているか、そして何よりも、この分野における内部監査の役割と実績をどのように認識しているかを報告する。現在の資料で明らかになった具体的な問題点、懸念事項、事例については、プライバシー担当役員への現地インタビューで得た意見も付記する。

最終的な目標は、様々な状況下の内部監査専門家がプライバシーとデータ保護の懸念にどれだけうまく対応したかを報告すること

と、プライバシーとデータ保護の問題に対するステークホルダーの認識が内部監査の取り組みとどの程度整合しているかを検討して、内部監査専門職がステークホルダーの期待を予測して対応することに成功してきたかを評価することである。当面、本研究の次の段階が継続する間、本稿で取り上げた背景、フレームワーク、導入方法が、内部監査部門がこの重要な懸念分野に対する自らの対応を発展させ向上させる上で有益な基礎となるよう、期待する。

<sup>1</sup> Timothy King, “IDC: Data Creation to Reach 163 Zettabytes by 2025,” Data Management News, April 11, 2017, <https://solutionsreview.com/data-management/idc-data-creation-to-reach-163-zettabytes-by-2025/>

<sup>2</sup> “New Policy Prohibits DoD Employees From Using GPS Services in Operational Areas,” Defense Logistics Agency Public Affairs Department news release, Aug. 8, 2018, <https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1597116/new-policy-prohibits-dod-employees-from-using-gps-services-in-operational-areas>

<sup>3</sup> Alyssa Provazza, “Artificial Intelligence Data Privacy Issues on the Rise,” TechTarget Network, May 26, 2017, <https://searchmobile.computing.techtarget.com/news/450419686/Artificial-intelligence-data-privacy-issues-on-the-rise>

<sup>4</sup> Ibid.

<sup>5</sup> Matteo Cagnazzo and Chris Wojzechowski, “Security and Privacy in Blockchain Environments,” dotmagazine, June 2017, <https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/security-and-privacy-in-blockchain-environments>

<sup>6</sup> Kate O’Flaherty, “Facebook Data Breach —What To Do Next,” Forbes, Sept. 29, 2018, <https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#6779f4f02de3>

<sup>7</sup> Karl Utermohlen, “Facebook Data Breach 2019: 540 Million Users’ Records Exposed,” InvestorPlace, April 4, 2019, <https://investorplace.com/2019/04/facebook-data-breach-2019/>

<sup>8</sup> Phil Muncaster, “Data Leak Exposes 267 Million Facebook Users,” Infosecurity Magazine, Dec. 20, 2019, <https://www.infosecurity-magazine.com/news/data-leak-exposes-267-million/>

<sup>9</sup> Paul Bischoff, “Which States Have the Most Data Breaches?” Comparitech, June 20, 2019, <https://www.comparitech.com/blog/vpn-privacy/data-breaches-by-state/>

<sup>10</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council (official text of the GDPR) , Article 4, p. 33, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679><sup>e</sup>.

<sup>11</sup> Ibid.

<sup>12</sup> “Determining What Is Personal Data,” U.K. Information Commissioner’s Office online guidance, Dec. 12, 2012, p. 7, <https://ioc.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>

<sup>13</sup> GDPR, Article 4, p. 33.

<sup>14</sup> “Adequacy Decisions: How the E U Determines if a Non-E U Country Has an Adequate Level of Data Protection,” European Commission website, [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

<sup>15</sup> “Data Protection Laws of the World” (Colom-

訳注<sup>e</sup> 日本語訳は、<https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>

- bia), DLA Piper, 2020, <https://www.dlapiper-dataprotection.com/index.html?t=law&c=CO>
- <sup>16</sup> “Data Protection Laws of the World” (Mexico), DLA Piper, 2019, <https://www.dlapiper-dataprotection.com/index.html?t=law&c=MX&c2=>
- <sup>17</sup> Margareth Kang, “What to Expect From Brazil’s General Data Protection Law?” Berkeley Technology Law Journal, University of California, April 22, 2019, <http://btlj.org/2019/04/what-to-expect-from-brazils-general-data-protection-law/>
- <sup>18</sup> Tahira Noor Khan, “India Is Set to Get Its First Data Protection Law,” Entrepreneur India, Dec. 9, 2019, <https://www.entrepreneur.com/article/343612>
- <sup>19</sup> Winston Ma Wenyan, “China is Waking Up to Data Protection and Privacy,” World Economic Forum, Nov. 12, 2019, <https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline>
- <sup>20</sup> “EU Japan Adequacy Decision” fact sheet, European Commission website, January 2019, [https://ec.europa.eu/info/sites/info/files/research\\_and\\_innovation/law\\_and\\_regulations/documents/adequacy-japan-factsheet\\_en\\_2019\\_1.pdf](https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf)
- <sup>21</sup> Kwang Bae Park and Hwan Kyoung Ko, “Korea: Data Protection 2019” (Section 18.2), International Comparative Legal Guides, March 7, 2019, <https://iclg.com/practice-areas/data-protection-laws-and-regulations/korea>
- <sup>22</sup> Melissa Krasnow, “Practical Guidance Overview: State Laws Requiring Data Security Practices,” Bloomberg Law Privacy and Data Security, November 2018, <http://www.vlplawgroup.com/wp-content/uploads/2018/11/Data-Security-Overview-V2.pdf>
- <sup>23</sup> California Consumer Privacy Act of 2018, Section 1798.140, [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)
- <sup>24</sup> Ibid.
- <sup>25</sup> California Consumer Privacy Act of 2018, Sections 1798.105, 1798.110, and 1798.115, [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)
- <sup>26</sup> “Risk in Focus 2020: Hot Topics For Internal Auditors,” European Confederation of Institutes of Internal Auditing, September 2019, p. 7, <https://www.iaa.nl/SiteFiles/Publicaties/Risk%20in%20Focus%202020%20IIA%20NL%20LR%20def.pdf>
- <sup>27</sup> Ibid, p. 5
- <sup>28</sup> Ibid, p. 11
- <sup>29</sup> Ibid, p. 13
- <sup>30</sup> “OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk,” Institute of Internal Auditors, 2019, p. 5, <https://dl.theiia.org/AECPublic/OnRisk-2020-Report.pdf>
- <sup>31</sup> “NIST Releases Version 1.0 of Privacy Framework,” NIST news release, Jan. 16, 2020, <https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework>

