bsi.

...making excellence a habit.™

プライバシーの問題

ISO/IEC 27701 による個人情報管理

ビジネスのためのBSIホワイトペーパー

はじめに

デジタライゼーション、グローバリゼーション、そして医師の予約からインターネットバンキングまで様々なサービスの個人化により、個人情報の収集及び処理はこれまでになく増加しています。また、この傾向は新しいサービスの機会が生まれ、新しい業者が市場に参入することで、さらに強まっています。

今や、人々が日常的に使用する様々なプラットフォームで個人情報が収集されています。例えば、モバイルアプリケーション、ロイヤルティスキーム、コネクテッドデバイス、ロケーションベースの広告の増加などが挙げられます。つまり、私たちはよく考えずに定期的にデータを渡し、これまで以上に多くのデータフローを生み出しているのです。出会い系サイト、通信事業者、公共サービス機関など、個人情報が流出したというデータ侵害のニュースを目にしない日はほとんどありません。これにより、個人情報の悪用を取り巻く問題への注目度が高まり、組織は油断することができなくなりました。

こうした問題意識の高まりにより、個人データの収集、利用、保護のあり方について、個人及び政府間で関心が高まっています。これを受けて、一部の政府は、個人データの取扱いに関するガイドラインや要求事項を定めることを目的とした新しい規制を提案または制定しています。

欧州では、一般データ保護規則（GDPR）の導入により、私たちが暮らすデジタル世界の現実を反映したデータプライバシー法の調和が図られています。

また、韓国、オーストラリア、中国など、多くの国でデータ保護法が制定されています。規制環境が強化され、個人データの保護に対処するための共通の概念が必要になることを見越して、国際標準化機構（ISO）と国際電気標準会議（IEC）は、そのようなガイダンスを提供するための規格を策定するためのイニシアチブをとっています。これらの規格は、変化する規制環境の中で、個人データ保護及び様々な法律へのプライバシー準拠を実証するための枠組みを提供するという利点があります。また、認証は、組織がプライバシー及び関連する義務への取組みに信頼性を持たせるための有用なツールとなります。

個人情報の管理

私たちが活動するダイナミックな環境を考えると、個人情報に対するリスクを低減するために、組織がどのようにデータを管理・処理すべきかについてのガイダンスの必要性は、ますます重要になってきています。組織がどのように個人情報を管理し、世界中の最新のプライバシー規制に準拠していることを実証するかについて、新たな国際規格という形でガイダンスを示すことは、非常に大きな意味を持ちます。そのため、プライバシー情報マネジメントのための規格、ISO/IEC 27701が開発されました。

ISO/IEC 27701とは？

この新しい国際規格は、正式には、ISO/IEC 27701と呼ばれています（セキュリティ技術 - プライバシー情報マネジメントのためのISO/IEC 27001 及び ISO/IEC 27002への拡張 - 要求事項及びガイドライン）。

多くの組織がISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を導入し、ISO/IEC 27002のガイダンスを利用していることから、この強固な基盤の上に成り立つプライバシー保護のためのガイダンスを提供することは、自然な流れといえます。

ISO/IEC 27701は、ISO/IEC 27001及び ISO/IEC 27002へのプライバシーの拡張版であり、個人情報の収集・処理によって影響を受ける可能性のあるプライバシー保護のための追加ガイダンスを提供しています。この規格の設計目標は、既存のISMSに追加要求事項を加えて強化し、プライバシー情報マネジメントシステム（PIMS）の確立、実施、維持、継続的改善を図ることです。この規格は、個人識別可能情報（PII）コントローラ 及び PIIプロセッサに対し、個人のプライバシー権利に対するリスクを低減することを目的とした、プライバシー管理策を実施するための枠組みを示しています（表1参照）。 これらの追加要求事項及びガイダンスは、あらゆる規模、あらゆる文化環境の組織にとって実用的で使いやすいように書かれています。

表1 – 個人情報マネジメントの役割

PII コントローラ	PII プロセッサ
個人情報を収集し、その処理の目的を決定する。 しばしば共同コントローラとして知られているように複数の組織がPIIコントローラとして活動することができる。また、ここにはデータ共有契約が必要になる場合がある。	PIIコントローラに代わり、その指示に従ってのみ個人情報を処理する。
ISO/IEC 27701がPIIコントローラにいかに役立つか	**ISO/IEC 27701がPIIプロセッサに役立つ方法**
• ベストプラクティスのガイダンスを提供 • PIIコントローラ間の透明性を確保 • PIIプロセスを効果的に管理する方法を提供	• ベストプラクティスのガイダンスを提供 • PIIが効果的に管理されているという安心感を顧客に提供

ISO/IEC 27701 規格の策定

ISO/IEC 27701は、「アイデンティティ管理及びプライバシー技術」を担当するISO/IECのワーキンググループによって起草されました。その策定は、BSIが指名したプロジェクトエディターが主導し、英国政府により国家標準化機関として任命されたBSIは、ISOとIECの両方で英国の利害を代表しています。

ISO/IEC 27701は、組織がISO/IEC 27001マネジメントシステムの拡張として、認証することを意図しています。言い換えれば、ISO/IEC 27701認証を取得しようとする組織は、ISO/IEC 27001認証も必要になります。これは、情報セキュリティ及びプライバシーマネジメントの両方に対する取組みを実証します。

ISO/IEC 27701の位置づけ

個人情報保護のための要求事項及びガイダンスは、組織の状況、および各国の法律・規制が適用される場所によって異なります。 ISO/IEC 27001では、この状況を理解し、考慮することが求められています。ISO/IEC 27701は、より具体的で、以下へのマッピングが含まれます:

- ISO/IEC 29100で定義されているプライバシーの枠組み及び原則
- ISO/IEC 27018 及び ISO/IEC 29151、ともにPIIに焦点を当てる

ただし、これらのマッピングはすべて、各国の法律・規制を考慮して解釈する必要があります。また、ISO/IEC 27701は、プロセッサ、コントローラ、またはその両方の役割を果たすすべての組織に適用可能ですが、ISO/IEC 27018は、パブリッククラウドプロバイダに特化して適用されるという点も注目に値します。

BS 10012:2017+A1:2018* は、英国に特化した公開規格であり、欧州連合（EU）のGDPRの原則に沿った個人情報マネジメントシステムのベストプラクティスの枠組みを提供しています。ISO/IEC 27701とBS 10012の主な違いの一つは、ISO/IEC 27701は、PIMSがISMSの要求事項及び管理策の拡張であると考えられるように構成されているで点です。

ISO/IEC 27701は、PIIコントローラ（ジョイントPIIコントローラ含む）及び PIIプロセッサ（下請けのPIIプロセッサの使用を含む）が使用することができます。

ISO/IEC 27701の要求事項に準拠している組織は、個人情報の処理方法について文書化した証拠を作成します。この証拠は、個人情報の処理が相互に関連しているビジネスパートナーとの契約を促進するために使用されることがあります。 これは、他の利害関係者との関係にも役立つ可能性があります。これらの文書への準拠を法律や規制への準拠とみなすことはできませんが、ISO/IEC 27701 を ISO/IEC 27001 と併せて使用することで、必要に応じてこの証拠に対する独立した検証を行うことができます。

ISO/IEC 27701のベネフィット

- 利害関係者間の透明性の確保
- 信頼関係の構築に貢献
- より協調的なアプローチを提供
- より効果的なビジネス契約
- 役割及び責任の明確化
- ISO/IEC 27001との統合による複雑さの軽減

*BS10012:2017の改訂版が2018年に発行されました（BS 10012 +A1:2018）。 この改訂は、BS10012:2017のいくつかの箇条の若干の変更を対象としています。これらの変更は、UK Data Protection Act 2018（英国のデータ保護法）を反映しています。

規格の適切な運用管理策が一貫して実施されていることを検証するために、また関連するプライバシー規制のコンプライアンス要件を遂行するために、以下の対策を講じなければなりません:

1. 規格の管理策に対する関連する規制要求事項のマッピング
2. 規格の管理策では十分に対応できない特定の規制要求事項を列挙し、その要求事項が適用可能になる条件を示す
3. 上記を審査サイクルにおけるリスク評価プロセスに組み込む

検討すべき良い例は、ISO/IEC 27701におけるデータ侵害管理の管理策、およびGDPRの侵害通知の要求事項（第33条）です。どう考えても、この規格のセキュリティインシデント管理のための管理策は、GDPRのデータ侵害に関する要求事項と完全に一致しています。

しかし、この規格には、法律で定められている72時間以内の通知のような具体的なものは含まれていません。組織がこのGDPRの特定の要求事項を満たすマネジメントシステムを実施していることを、実務担当者が実証するためには、組織が侵害の確認後72時間以内にデータ主体及びプライバシー規制当局に通知するための統一されたプロセスを導入している、もしくは侵害が欧州市民を巻き込んでいるかどうか、または侵害されたデータ処理が欧州内で行われたかどうかを判断し、その場合、必要な時間枠内で通知を開始するプロセスを導入していることを審査員に示さなければなりません。

コントローラ及びプロセッサが、ISO/IEC 27701を使用して、複数のプライバシー規制に対する規制遵守を検証するためには、規制に対する規格のマッピングや、固有の規制要求事項及び適用可能条件の列挙が必要となります。

データプライバシー法

データの安全性を確保し、侵害のリスクを最小限に抑えることが、組織にとっての課題となる中、ビジネス環境の変化に合わせてプライバシー法が進化しているのは、当然のことです。最も注目されているのが、EUのGDPRです。

GDPRは、誰もが自分に関する個人情報を保護する権利を有するという基本的権利及び自由を守るためのEUの法律です。これらの権利は、データ処理活動及びEU加盟国間の個人情報の自由な流れに関しても保持されなければなりません。データの処理は、そのデータが属する自然人のベネフィットのために行われるべきです。
市民の個人情報及び権利を保護するために、世界中に同様の法律が存在しており、医療、小売、銀行などの分野固有の要求事項もあります。

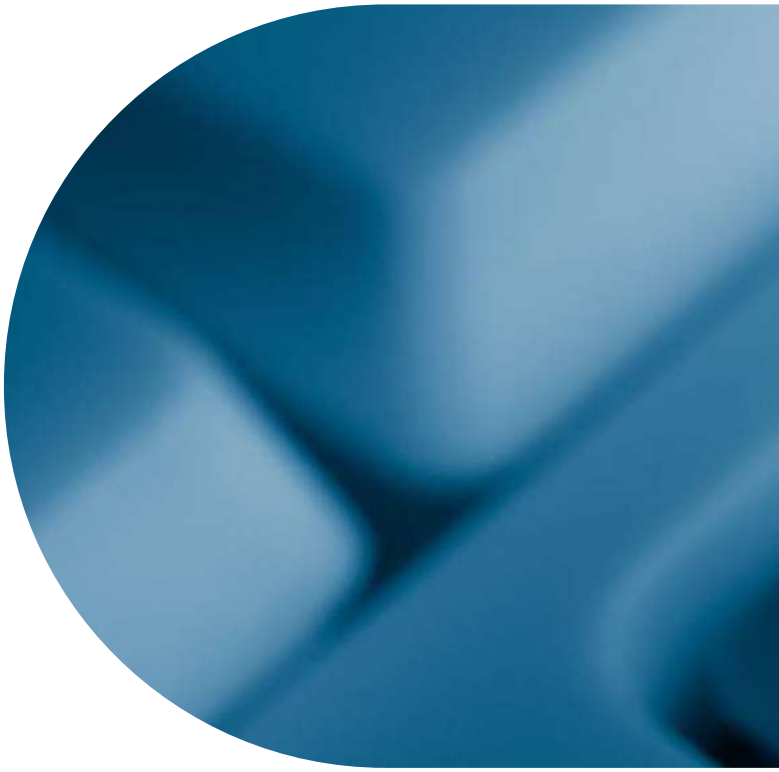
医療分野

最も機密性の高い個人情報を収集する分野であるため、医療に特化したデータ保護法が非常に重要です。例えば、フランス公衆衛生法（Article L.1111-8）では、特定の種類の健康/医療データを保管するサービスプロバイダに、この活動に対する認定を求めています。また、米国の医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）では、機密性の高い患者データ保護に対する基準を定めており、米国のヘルスプラン、医療事務処理会社、医療提供者、または個人の健康情報にアクセスするベンダーや請負業者として活動するすべての組織または個人に遵守を義務付けています。

また、欧州のデジタル単一市場への注目も重要です。これは2015年に発表された、デジタルマーケティング、Eコマース、テレコミュニケーションを対象とした政策で、既存の障壁を取り払い、人々や企業に機会を提供することを目的としています。以下の3つのコアとなる柱があります:

- オンライン製品及びサービスへのアクセス
- デジタルネットワーク及びデジタルサービスが成長し、繁栄するための条件
- 欧州のデジタル経済の成長

これにより、国境を越えたデータ処理や商取引が容易になります。しかしながら、欧州の加盟国間のデータプライバシー法の違いは、欧州デジタル単一市場を成功させるための障壁として認識されていました。 そのため、欧州全体でデータプライバシーを調和させるためにGDPRを導入することは、前向きな変化であると言えます。



データ保護法に準拠していることを実証するための認証メカニズム

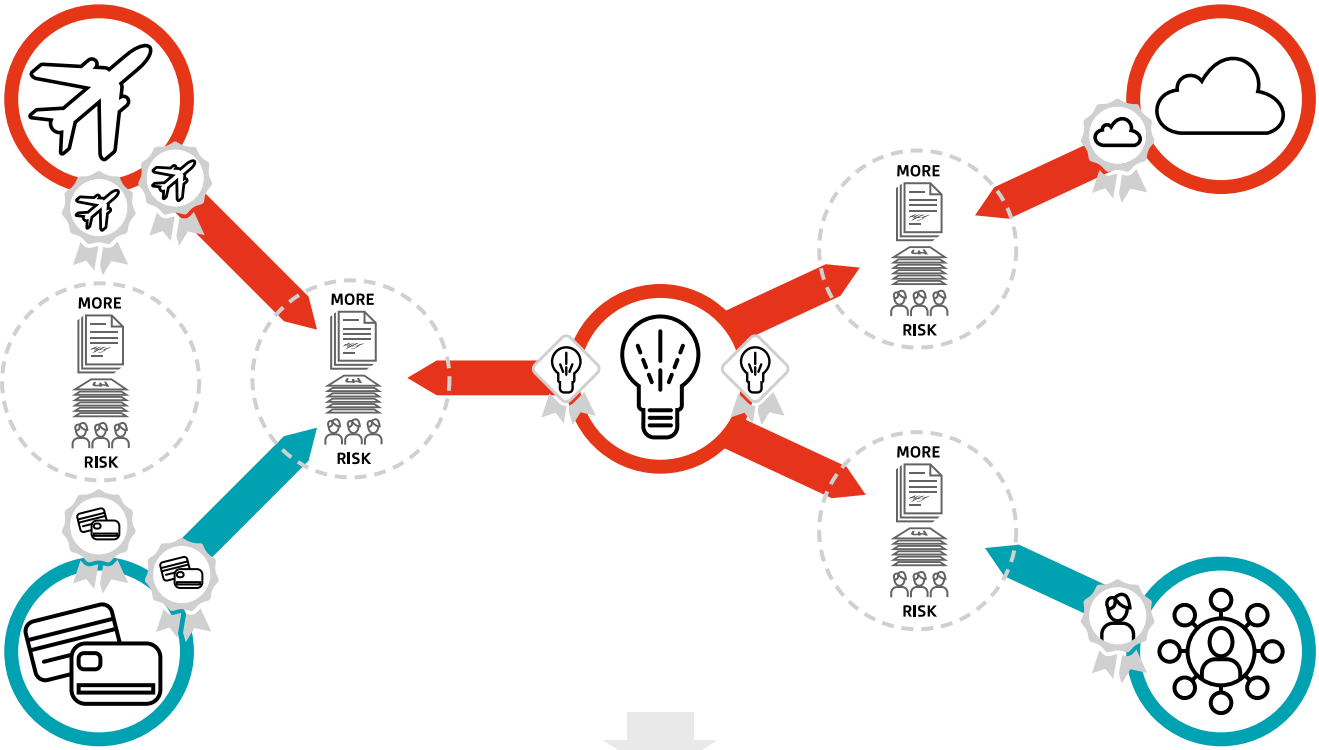
GDPRでは、コントローラ及びプロセッサが処理業務に関する規制を遵守していることを実証するために、データ保護認証メカニズムやデータ保護シール・マークを設けることが奨励されています（GDPR (EU) 2016/679, 第42条）。 さらに、このような認証又はシールは、組織がGDPRに沿った形で個人情報を取り扱うために適切な措置を講じていることを示す目的で使用することができます。

一貫性のある認証メカニズムは、重要な「説明責任」の要素をもたらし、リスクの低減及び個人情報の自由な流れを促進します。 これにより、組織は有用なサービスを提供することができ、同時にプロセスの透明性を高め、**図2**に示すように、個人情報の保護について、顧客に誠実さを示すことができます。

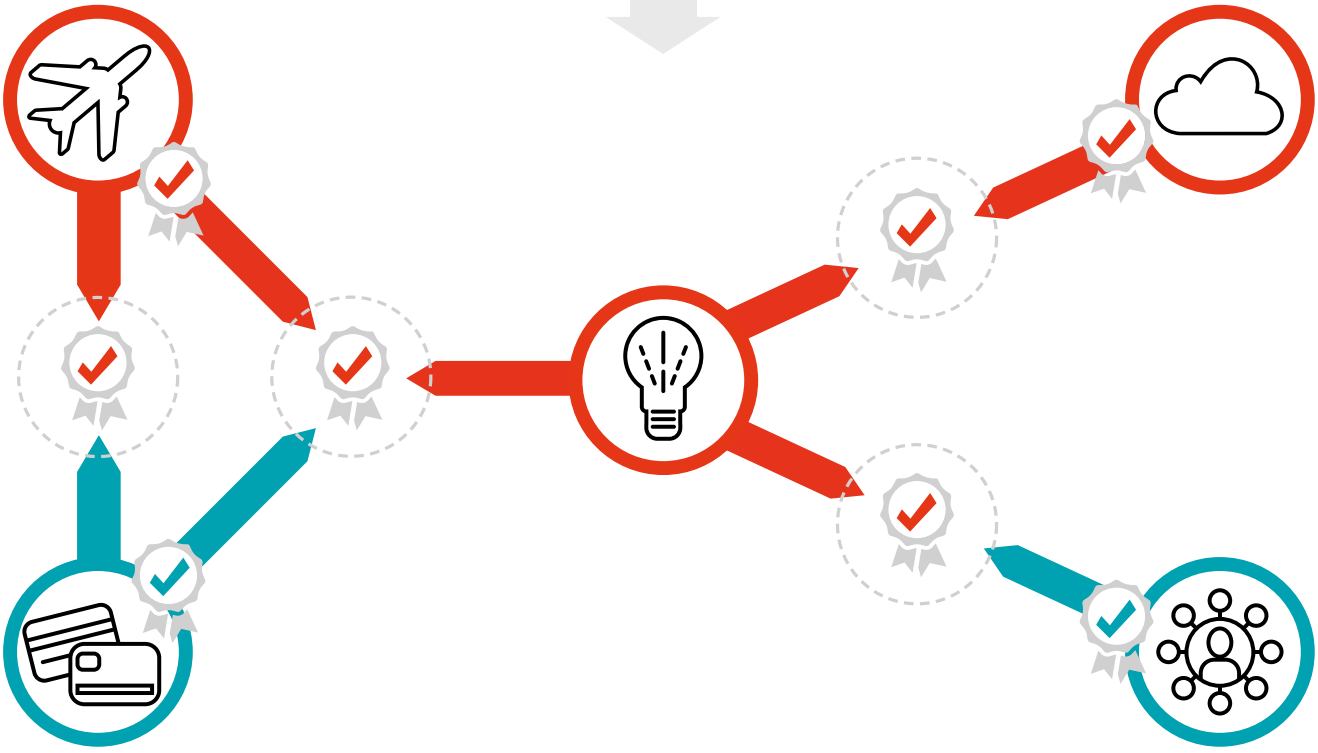
また、コントローラがゆりかごから墓場までデータに対して責任を持つことから、サプライチェーン管理におけるデータ処理の重要性が表面化しています。例えば、航空会社と銀行の共同ブランドであるクレジットカードのような製品を考えてみてください。双方の顧客情報を交換し、どのような顧客が製品を購入する可能性があるかを確認する必要があります。顧客の個人情報のやり取りにはリスクが伴います。双方が、互いに相手が顧客のデータを十分に保護することをどのように検証するのでしょうか？ プレーヤーの数が増えれば増えるほど、そのリスクは大きくなります。顧客ターゲットを絞るためにマーケティング会社と契約したり、ソーシャルメディアで広告を出したりすることもあります。マーケティング会社がこのマーケティングキャンペーンに関連するデータを保存・処理するために、クラウドサービスが使用されることもあります。 認証は、サプライチェーンを通じて組織間で個人情報を交換するリスクを評価するために組織が使用するプロセス及び管理策の有効性を証明する独立した検証として機能します。

しかし、**図2（a）**に示すように、ある組織がある法域で認証スキームを使用し、別の組織が別の法域で適用される別のスキームで認証を受けた場合、顧客に属する個人情報が適切に取り扱われているという必要な保証又は信頼のレベルをビジネスパートナーに提供できない可能性があります。ビジネスのグローバル化に伴い、**図2(b)**に示すように組織が規制を遵守し、個人情報を保護し、ビジネスの成長を可能にしていることを示すために、一貫性のある統一された認証メカニズムが必要になります。リスクを低減し、商業上のパートナー間の取引の障壁を下げるためには、法域及び業界に垂直方向で認識される共通のGDPR認証が必要です。

図 2 – 一貫性のあるデータプライバシー認証メカニズムにより、商取引を可能にする。
(a) 組織間で認証が分断されている。



(b) 一貫した認証



この思いは、最近GDPRの認証に関する勧告を発表した欧州連合ネットワーク・情報セキュリティ機関（ENISA）も同様です 。
[参照-ENISA: Recommendation on European Data Protection Certification, Version 1.0, November 2017; https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification]
ENISAは、認証、シール及びマークは、データコントローラが処理業務におけるGDPR規定への準拠を達成及び実証できるようにする上で重要な役割を果たすと述べています。さらにENISAは、欧州委員会及び欧州データ保護委員会の指導・支援のもと、各国の認証機関及び監督官庁が、GDPR認証メカニズムの導入・展開に関する共通の取組みを追求することを推奨しています。また、この取組みは拡張性があり、承認され広く採用されている基準を使用することが推奨されています。欧州全体の認証メカニズムの一貫性と調和が強調され、認証プロセスの重要な特性として信頼性と透明性が強化されています。

ISO/IEC 27701は潜在的な認証メカニズム

ISO/IEC 27701は、上記の勧告に対応しており、（第42条に規定されている）認証メカニズムの基礎として利用可能なことが期待されています。このように使用することで、国境を越えたデータフローも含めて、組織が顧客の個人情報を法律に準拠して扱っていることを証明することができます。 ISO/IEC 27701は、あらゆる規模、あらゆる文化環境の組織に適用することができます。 これは、従業員及び顧客双方のPIIを収集し、処理するためのものです。 今回策定された一連の管理策は、情報セキュリティを実施するための技術的な手段を拡張して、プライバシーに関する要求事項にも対応しており、組織が実施することにより、GDPRなどのデータプライバシー法に準拠していることを実証するのに役立ちます。

したがって、ISO/IEC 27701の管理策への準拠を実証し組織がPIIを処理する方法の証拠として必要な文書を作成することで次の事項が可能になります:

- 複数の認証をサポートする必要がないため、コンプライアンスに関する作業負荷が大幅に軽減される
- データプライバシー法への準拠を実証することで、組織と顧客間の信頼を高める
- データ保護担当者が、プライバシー規制遵守の進捗状況を示すために、上級管理職及び役員に提出可能な証拠を作成する
- EUデジタル単一市場及び国境を越えたデータフローを通じたビジネス及び商業の機会が増加する

さらに、ISO/IEC 27701は、既存のISMSにプライバシーに特化した管理策を追加し、組織内での効果的なプライバシー管理を可能にするPIMSを構築することを目的としています。ISO/IEC 27701は、情報セキュリティの成功規格として一般的に受け入れられているISO/IEC 27001に対する認証を提供する審査員のネットワークが確立されているため、既存の審査プロセスに統合するのに非常に適した立場にあります。

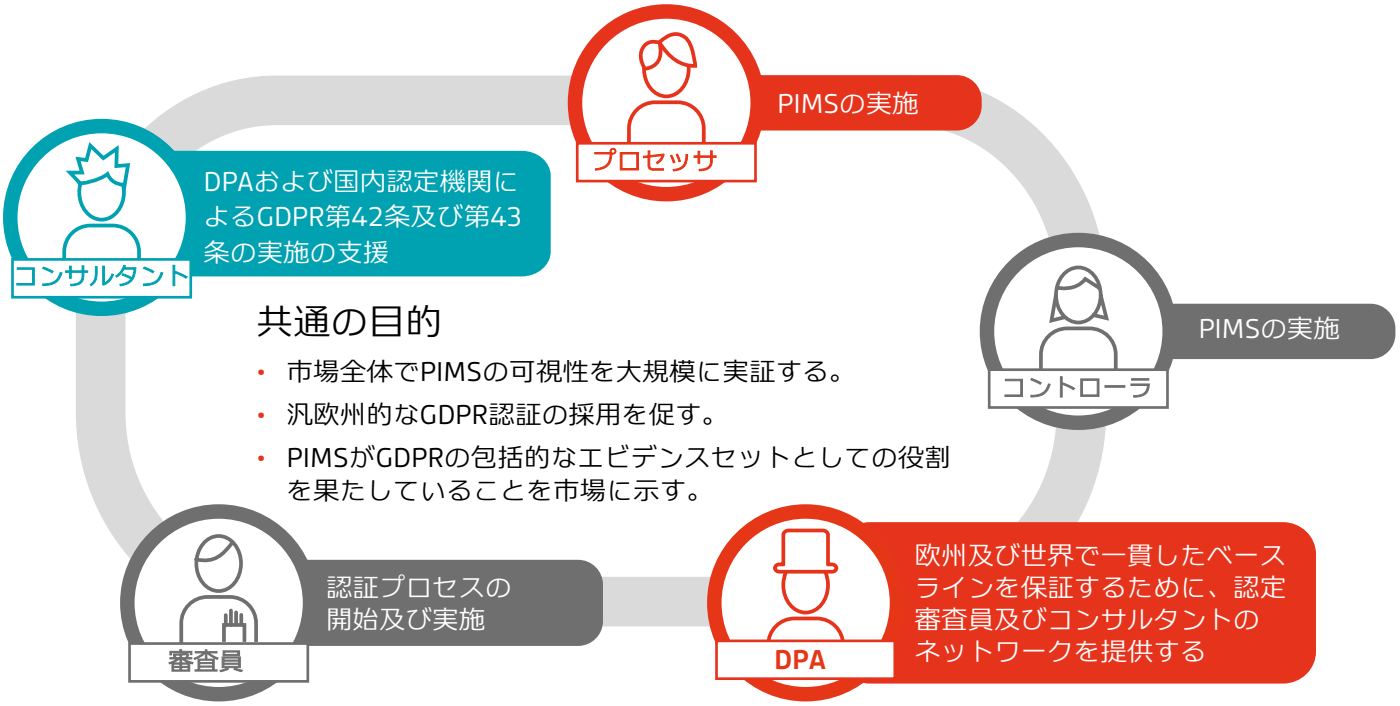
ISO/IEC 27701は、コンセンサスを重視したプロセスで開発されています。これは、規格策定において、重要なタスクの一つです。さまざまな業界及び規制関係者からの意見やレビューがありました。これには、すべてのEU諸国のデータ保護機関（DPA）で構成される欧州データ保護委員会（以前は第29条作業部会）による参加とレビューが含まれます。DPA、および審査員の認定機関は、ISO/IEC 27701に基づく認証メカニズムが、あらゆる業界分野、あらゆる規模の組織にとってプライバシー規制への準拠を実証するのに十分な支援を提供していることに満足する必要があります。さらに、認証メカニズムは、コントローラ及びプロセッサのニーズに対応しなければなりません。これらのどちらにも、ISO/IEC 27701で定義されている多くの管理策があります。

利害関係者の関与の重要性

前述したように、ISO/IEC 27701は、ISO/IEC 27001を拡張した規格であり、ISOのマネジメントシステム規約（通称「Annex SL」）に基づいて構成されているため組織で複数のマネジメントシステムを効率的に導入することが可能です。 **図3**は、利害関係者の状況及びその役割の重要性を示しています。

既存のISO/IEC 27001（ISMS）とすでに連携していることで、これらの利害関係者はすべて、ISO/IEC 27701に取り組む上で非常に有利な立場にあります。これらはみな、個人情報管理の目的を共有しており、個人情報管理に真剣に取り組んでいることを示すために、認められたアプローチが必要であり、そこにISO/IEC 27701の役割があります。

図3 – ISO/IEC 27701に基づく認証のための利害関係者の状況 (情報源: マイクロソフト)



まとめ

結論として、進化する規制環境に準拠して個人情報を管理することは複雑ですが、無視することはできません。個々の個人情報を保護することは、人間の基本的人権の一つです。企業及び個人の生活に関わるデータがますますグローバル化する中、これらの権利を保護するための法律が世界中に存在しています。欧州のGDPRは、PIIの収集及び処理が合法的に行われることを確実にするために導入され、EUデジタル単一市場を実現するために必要な国境を越えたデータフローをサポートしています。

欧州のGDPRでは、規制に準拠していることを実証する認証メカニズムは、組織が個人データをどのように扱うかについての信頼性を高めるために大いに役立ち、また、組織間の保証を提供することでビジネスチャンスを生み出すものであると認識されています。これは、認証がEU加盟国間で一貫して実施され、欧州の国境を越えて、グローバルな商取引やビジネスを可能にする場合に特に当てはまります。

ISO/IEC 27701は、既存の規格ポートフォリオに追加して導入する必要があります。ISO/IEC 27701で規定されている管理策を実施することで、組織は個人情報の処理方法に関する証拠を文書化することができます。このような証拠は、個人情報の処理が相互に関連しているビジネスパートナーとの契約を促進するために使用することができ、また、広く受け入れられている認証メカニズムを得た場合には、GDPRなどのデータ保護法への準拠を実証するのに役立ちます。

Why BSI?

BSIは、1995年に世界初の規格であるBS 7799（現在は世界で最も普及している情報セキュリティ規格であるISO/IEC 27001）を策定して以来、情報セキュリティ規格の最前線で活躍しています。また、それだけにとどまらず、プライバシー、サイバーセキュリティ、クラウドセキュリティなど新たな課題にも取り組んでいます。だからこそ、私たちはお客様のお役に立てるのです。

BSIは、193カ国、86,000を超えるお客様と共に働き、自動車、航空宇宙、ビルトエンバイロメント、食品、ヘルスケアなど、さまざまな分野にわたるスキルと経験を備えた、真に国際的な企業です。規格開発およびナレッジソリューション、認証、プロフェッショナルサービスにおける専門知識を通して、BSIは、業績を向上させ、お客様が持続的に成長し、リスクを管理し、最終的にはレジリエンスを高められるよう支援します。

BSI/UK/1591/SC/0719/JA/GRP

BSIの製品及びサービス

知識

当社のビジネスの核心は当社が創造し、お客様に影響を与える知識にあります。
規格の分野では、業界の専門家を集めて、国内、地域及び国際レベルで 規格を策定することで、専門家団体としての評価を高め続けています。
実際、世界で最も認められた10規格のうち、BSIが起源で作成された規格は8規格になります。

認証

プロセスの適合性の独立評価または特定の規格に準拠した製品を提供することで、高レベルのエクセレンスを発揮します。
当社は、お客様が規格の恩恵を最大限に享受するために、世界クラスの実施および監査テクニックでお客様をトレーニングいたします。

コンプライアンス

真の、長期的な利益のために、当社のお客様は規則、市場のニーズまた規格への現状のコンプライアンスを確認する必要があります。そうすれば、それが習慣となります。
当社はこのプロセスを促進するため様々なサービスと分化されたマネジメントツールを提供しています。

bsi.

BSIグループジャパン株式会社
営業本部
TEL: 045-414-3021
Eメール: Sales.Japan@bsigroup.com