



# ISO/IEC27701(プライバシー情報)

## ビジネスビジョン

データとプライバシーの保護は、今日あらゆる組織にとって重要な課題となりました。企業が収集するデータの量は増えており、各国政府は、その使用方法への懸念と相まって消費者保護の必要性を認識するようになりました。その結果、EU一般データ保護規則(GDPR)などの厳格な規制が導入されました。しかし、規制を強化するだけでは、解決策にはなりません。そこで、国際標準化機構(ISO)は、データプライバシーと消費者保護に取り組む企業を支援するため、ISO 27701(プライバシー情報マネジメントシステム:PIMS)という新たな規格を発行しました。企業が消費者の信頼を得て、競争上の優位性を勝ち取るためには、データプライバシーとセキュリティを最優先に考えなければなりません。新しい、より厳格になった規制を順守することは経営の大前提です。国際的なデータプライバシー規格の認証を得ることは、すべてのステークホルダー(利害関係者)のプライバシーを保護に対する強力なツールとなります。

## ソリューション

### ISO/IEC27701とは


ISO27701はデータプライバシーの新たな国際基準であり、ISOの情報セキュリティのための現行規格(ISO27001)の拡張規格です。ISO27701は、すでにISO27001準拠の情報セキュリティマネジメントシステム(ISMS)を採用している企業が、顧客などの利害関係者のデータプライバシーを保護する措置を講じることにより、さらに対策を進めようというものです。これは、あらゆる分野、あらゆる規模の組織が、使用目的で個人情報を収集・処理する場合の手引書です。


### なぜ、ISO27701を実施するのか？

 消費者の個人情報を保護することで組織のイメージを守る	 ビジネスの核心部分でデータ保護を行い利害関係者の信頼を得る
 データ保護規制などの法令順守に取り組む	 従業員にデータプライバシーに関する自らの役割と責務を理解させる
 厳格なプライバシーコントロールの実施により、リスクを識別し緩和する	 法令違反を避けるためスキルとビジネスプロセスを改善する

## ISO27701の主な特徴

ISO27701の多くは組織の手順と行動、すなわちデータプライバシー文化の醸成に関係するものですが、いくつかの箇条は特にシステム自体の設計を扱っています。PII処理に係るシステムと構成要素は、プライバシー・バイ・デザインとプライバシー・バイ・デフォルト(後述)の原則に従って設計される必要があります。これにより、組織が各種コントロールを実施するのが楽になるという利点もあります。特に、収集するデータは、特定目的に本当に必要なデータだけに限定すべきです。

 **プライバシー・バイ・デフォルト**  
ユーザーの許可なく、デフォルトの状態で個人情報を取得する設計にしないよう求めるもの。情報を取得する際はユーザーによる選択・同意を得るプロセスがあることを求めている。

 **プライバシー・バイ・デザイン**  
組織が個人情報を扱う製品・サービスを設計・開発する段階から、PII保護を尊重するよう求めるもの。



## ビューローベリタスが選ばれる理由

ネットワーク	140か国1,600の拠点 ビューローベリタス各国が持つノウハウを共有 お客様が展開する国内外の事業ネットワークをカバー
認証実績	約150,000社の企業に対する認証実績
ワンストップ審査	各規格の審査の一貫性・最適化・効率化を実現

## 認証取得までの流れ

### 1. 組織の状況进行评估

ISO27001の情報セキュリティマネジメントシステムの実施はお済みですか？実施済みの皆さまは、データプライバシー・コンプライアンスへの道を着実に歩んでいます。現在のISMSをISO27701の要求事項と比較し、足りない部分の評価を行いましょう。ISMSを実施していない場合でもご安心ください。ISO27001とISO27701を同時に実施することが可能です。

「**な**」から始めるべきか」ぜひ、ご検討段階からビューローベリタスにお問い合わせください

### 2. お客様のPIMSを設計

データプライバシーの要求事項に対応するため、お客様のISMSを改良、強化します。その際、マネジメントシステムの成否が「人」にかかっていることを忘れないでください。責任者はシステムと、そのシステムにおける自らの責務を理解する必要があります。

「**ビューローベリタスは、必要に応じてマネジメントシステムの研修をお手伝いします**」

### 3. 認証を取得

ISO27701認証を取得すると、組織全体でこの規格が実施され、不適合があった場合は是正されるという第三者の認証が得られます。この認証は、お客さまが規制順守を実現するための支えとなり、データプライバシーへの真摯なコミットメントを顧客に示す手段ともなります。ISMSの実施がお済みでなくても心配には及びません。ISO27001とISO27701は同時に実施することができます。

「**ビューローベリタスは、ISO27001とISO27701の両方について、認定機関から認定を受けた認証書の提供を予定しています**」

## よくある質問

Q: ISO27701は単独で認証できますか。

A: いいえ。ISO27701はISO27001のアドオン認証のため、ISO27001をすでに取得済みであるか、ISO27001との同時取得が必要です。