bsi.

...making excellence a habit.™

ISO/IEC 27701
プライバシー情報マネジメント

実施ガイド

ISO/IEC 27701とは？

ISO/IEC 27701は、ISO/IEC 27001（情報セキュリティマネジメント）及びISO/IEC 27002（セキュリティ管理策）におけるプライバシーを拡張した、プライバシー情報マネジメントシステム（PIMS）に対する国際規格です。

この規格は、個人識別可能情報（PII）プロセッサ 及び PII コントローラが、堅牢なデータプロセス及び管理策を導入するのに役立つ、プライバシー保護に関するガイダンスと要求事項を提供します。これにより、PIIを管理することへの説明責任を果たし、信頼を得て、強固なビジネス関係を築くことができます。

目次

ISO/IEC 27701のベネフィットを享受できる組織とは？

ISO/IEC 27701は、個人情報の保護に真剣に取り組んでいることを実証したいと考える、あらゆる種類、あらゆる規模の組織にとって理想的な規格です。

上場企業、非上場企業、政府機関、非営利団体など問わず、情報セキュリティマネジメントシステムの中でPIIを処理する責任を負う組織にとって、ISO/IEC 27701は適しています。

具体的な対象は次のとおりです:

- PII コントローラ（ジョイントPIIコントローラ含む）
- PII プロセッサ

ISO/IEC 27701のベネフィット

ISO/IEC 27701の主な要求事項

箇条 1 : 適用範囲

ここでは、マネジメントシステムおよびその適用に対する要求事項を定めています。

ISO/IEC 27701は、ISO/IEC 27001およびISO/IEC 27002を拡張した形で、プライバシー情報マネジメントシステムの確立、実施、維持、改善のための要求事項およびガイダンスを提供することを目的としています。 PIIの処理に責任および説明責任を負う、PIIコントローラとPIIプロセッサに焦点を当てています。

箇条 2 : 引用規格

引用規格とは、規格の中で参照されている規格文書です。ISO/IEC 27701 には以下が含まれます:

ISO/IEC 27000 情報セキュリティマネジメントシステム – 概要及び用語

ISO/IEC 27001 情報セキュリティマネジメントシステム – 要求事項

ISO/IEC 27002 情報セキュリティ管理策の実践のための規範

ISO/IEC 29100 プライバシーの枠組み

箇条 3 : 用語及び定義

このセクションでは、ISO/IEC 27000 および ISO/IEC 29100には含まれていない、規格全体で使用されている重要な用語の定義がいくつか追加されています。

箇条 4 : 一般

この箇条は、ISO/IEC 27701の「舞台設定」であり、ISO/IEC 27001 および ISO/IEC 27002 に関連する、PIMS固有の要求事項の位置をハイレベルで示しています。

箇条 5 : ISO/IEC 27001に関連するPIMS固有の要求事項

この箇条は、ISO/IEC 27001の情報セキュリティ要求事項を拡張し、プライバシーの保護を組み込むためのものです。

組織の状況の一部として、プロセッサおよび/またはコントローラとしての役割を決定し、プライバシー固有の規制および契約上の要求事項など、内部および外部の要因の影響を考慮する必要があります。役割に応じて、附属書Aおよび/または附属書Bの関連する管理策を実施し、既存の適用宣言書（SoA）に適用する必要があります。

また、PIIの処理に関連する利害関係者、PIMSの適用範囲、システムの効果的な導入・維持・継続的改善方法について検討しなければなりません。

プライバシーの保護を確実にするために、ISO/IEC 27001のリーダーシップ、計画、支援、運用、パフォーマンス評価および改善に関する要求事項を考慮し、必要に応じて拡張しなければなりません。 特に、情報及びPIIの処理に対するリスクを評価し、適切に処理することが求められています。

箇条 6 : ISO/IEC 27002に関連するPIMS固有のガイダンス

この箇条は、ISO/IEC 27002の情報セキュリティガイダンスを拡張し、プライバシーの保護を組み込むことを目的としています。

例えば、組織は、コンプライアンス、契約上、利害関係者の要求事項に基づいて、関連するプライバシー声明を組み込むために、情報セキュリティ方針に関する追加の実施ガイダンスを考慮する必要があります。

PIIの処理に関連する役割及び責任について、より明確なガイダンスが提供されています。これにはインシデント報告及びプライバシー侵害の結果についての認識も含まれます。

情報の分類において、PIIを確実に考慮するためのガイダンスを提供します。組織が処理するPII、およびそれがどこに保管され、どのようなシステムを経由しているかを理解しなければなりません。また、PIIとは何か、それをどのように認識するかを意識しなければなりません。

インシデント管理、リムーバブルメディア、PIIを処理するシステム及びサービスへのユーザアクセス、暗号化による保護、以前PIIを保存していたストレージスペースの再割当て、PIIのバックアップ及びリカバリ、イベントログのレビュー、情報転送方針、秘密保持契約など、より詳細な実施ガイダンスが含まれています。

さらに、この箇条のガイダンスでは、公共ネットワークでデータを送信する前、およびシステム開発・設計の一環として、前もってPIIを考慮することが推奨されています。

重要なのは、サプライヤーとの関係、期待、責任に対処することです。

箇条 7 : PIIコントローラのための追加のガイダンス

この箇条では、PIIコントローラに対するPIMS固有の実施ガイダンスを取り上げています。附属書Aに記載されている管理策に関連しています。

例えば、処理するPIIの具体的な目的を特定し、関連する法令を遵守するためにPIIを処理することの法的根拠を持つ必要があります。PIIを処理する目的が変更または拡張された場合には、更新を行うことが望ましいです。

また、このガイダンスでは、特別なカテゴリのデータ及び同意の要求事項、PII主体に対するリスクを最小化するためのプライバシー影響評価の要求事項、PIIプロセッサとの契約、ジョイントコントローラとの明確な役割及び責任についての考慮事項も説明しています。

処理するPIIの個人に対して、その処理理由及び方法を明確にし、要求があった場合には問合せ先を示すことが望ましいです。同意、撤回、PIIへのアクセス、修正、消去に関する詳細なガイダンスが含まれています。また、第三者の義務、要求の取扱い、自動処理による意思決定に関するガイダンスも提供されています。

最後に、プロセス及びシステムのプライバシー・バイ・デザインでは、収集及び処理に対する最低要求事項、PIIの正確性及び品質、処理の目的に基づく収集量の制限、処理の終了要求事項を考慮することが望ましいです。

重要なのは、PIIの共有、移転、開示に関するガイダンスが説明されていることであり、裏付けとなる記録により法域間を移転するのに役立ちます。

箇条 8 : PII プロセッサのための追加のガイダンス

この箇条では、PIIプロセッサに対するPIMS固有の実施ガイダンスを取り上げています。附属書Bに記載されている管理策に関連しています。

例えば、顧客との契約では、PII主体の義務を含む顧客の義務を支援するために、PIIプロセッサとしての役割を規定することが望ましいです。
PIIデータをマーケティング・広告目的で使用する場合は、事前に同意を得なければなりません。

承認済のPII処理への準拠を実証するのに役立つ、必要な記録を特定及び維持するためのガイダンスが説明されています。

顧客が個別の要求に対応する際の支援、処理中に作成される一時ファイルの管理、PIIの安全な返却・移転・廃棄、および適切な伝送管理策に関する詳細なガイダンスが含まれています。

最後にPIIの共有、移転、開示に関するガイダンスが詳細に記載されており、司法権に基づく移転、第三者及び業務委託先の要求事項、法的拘束力のあるPII開示の管理について説明されています。

附属書

ISO/IEC 27701には、多くの附属書が含まれています。附属書AとBは、それぞれコントローラとプロセッサに対するものであり、附属書C～Fは効果的なPIMSの確立及び運用を支援する追加の知識を提供しています。

附属書 A

PII コントローラのための一連の管理策。

すべての管理策が必要になるわけではありませんが、管理策を除外するための正当な根拠を適用宣言書に記載する必要があります。

附属書 B

PII プロセッサのための一連の管理策。

すべての管理策が必要になるわけではありませんが、管理策を除外するための正当な根拠を適用宣言書に記載する必要があります。

附属書 C

PIIコントローラに対する管理策のISO/IEC 2900のプライバシー原則へのマッピング。

これは、ISO/IEC 27701の要求事項及び管理策への準拠が、ISO/IEC 29100のプライバシー原則にどのように関連しているかを示しています。

附属書 D

ISO/IEC 27701の箇条とGDPRの第5条から第49条（第43条を除く）とのマッピング。

これは、ISO/IEC 27701の要求事項及び管理策への準拠が、GDPRの義務を果たすことにどのように関連するかを示しています。

附属書 E

ISO/IEC 27701の箇条と以下の事項へのマッピング:

- パブリッククラウドにおけるPIIプロセッサに対するISO/IEC 27018の要求事項
- PIIコントローラに対する追加の管理策およびガイダンスのISO/IEC 29151

附属書 F

ISO/IEC 27701をISO/IEC 27001及びISO/IEC 27002に適用する方法について詳しく説明しています。

これは、情報セキュリティの用語を拡張してプライバシーを組み込むことを明確に示し、適用例をいくつか挙げています。

BSIの研修

BSIは、お客様が組織にエクセレンスを根付かせるために必要な知識及びスキルを開発することを支援する世界的なリーダーです。 BSIの研修は、組織が認証を取得しようとしている場合や、単にプライバシー情報マネジメントシステムの導入を検討している場合など、知識を定着させ、ISO/IEC 27701のパフォーマンスを最大化するのに役立ちます。

ISO/IEC 27701 の研修には、以下のコースをご用意しています:

コース名：ISO/IEC 27701:2019 要求事項解説研修(JRCA登録CPDコースISMS)

- １日研修
- 個人識別可能情報 (PII)を保護し、プライバシー情報マネジメントシステム (PIMS)のフレームワークを提供する規格であるISO/IEC 27701を理解する。

BSI のビジネス改善ソフトウェア

洞察力を高め、継続的改善を実現

ISO/IEC 27701への投資により最大限の効果を得るために、プライバシー情報マネジメントシステムを効果的に管理するためのソリューションである業務改善ソフトウェアをご活用ください。事前に設定されたISO規格情報により、PIMSの必須要素を管理するために必要なツール及び情報を提供します。

BSIの業務改善ソフトウェアを導入するには、ISO/IEC 27701への取組みの開始時が理想的なタイミングであり、以下のベネフィットが得られます:

- 効率的な文書管理
- サイトおよび認証パフォーマンスの可視化
- 審査、インシデント/事象、リスクおよびパフォーマンスに関する処置を記録、追跡、管理する能力
- カスタマイズ可能なダッシュボードと報告書ツールにより、改善に向けたビジネス上の意思決定に役立つトレンドを把握することが可能

Why BSI?

By Royal Charter

ISO/IEC 27701 Privacy Information Management

BSI は一世紀以上にわたり、「良いものとは何か」を提唱し、世界中の組織にベストプラクティスを推進してきました。その中には、世界で最も普及している情報セキュリティ規格であるBS 7799（現在のISO/IEC 27001）の策定も含まれます。また、それだけにとどまらず、サイバーセキュリティやクラウドセキュリティ、ISO/IEC 27701によるプライバシーなど、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。

技術的なノウハウ、業界の専門家、学識者、専門機関とのネットワークを駆使して組織及び社会のためにプライバシーに関する議題の推進に取り組んでいます。

BSIについて

BSI は、組織がベストプラクティスの基準をエクセレンスな習慣に変えることを可能にするビジネス改善企業です。自動車、航空宇宙、ビルトエンバイロメント、食品、ヘルスケアなど多くの分野に渡るスキルと経験を有し、193カ国、86,000を超えるお客様と取引する、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。

詳しくはウェブサイトをご参照ください: bsigroup.com/ja-JP

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