「月刊誌アイソス2020年5月号 特集:プライバシー保護国際規格ISO/IEC 27701」抜き刷り
https://amzn.to/2RuAvs8

プライバシー保護の国際規格 ISO/IEC 27701

プライバシー保護の国際規格であるISO/IEC 27701:2019はガイドライン規格でもあり認証規格でもある。認証で活用される場合は、ISO/IEC 27001認証を必須としたアドオン認証になるだろう。個人情報保護を対象とするJIS Q 15001とはおそらく棲み分けが行われ、GDPRに対応している日本企業は、ISO/IEC 27701とJIS Q 15001の両認証を取得すると思われる。本特集では、日本規格協会によるISO/IEC 27701の邦訳の3月25日発行に合わせ、同規格に関する開発経緯、GDPR対応、認定・認証動向、企業における取組方法などについて、関係者の取材及び寄稿をまとめてみた。(本誌編集部)

01 規格動向 14P
プライバシー保護ならISO/IEC 27701
個人情報保護なら JIS Q 15001
コンプライアンス対応の選択肢が増える
取材先： ISO/IEC JTC1/SC27/WG5 エキスパート
一般財団法人日本情報経済社会推進協会（JIPDEC）
客員研究員　佐藤 慶浩 氏
主任研究員　都司 哲也 氏

02 規格解説 19P
ISO/IEC 27701 とプライバシー関連規格
～開発経緯と要求事項・ガイダンス及び
附属書の意図を理解する～
執筆： ISO/IEC JTC1/SC27/WG5 エキスパート
一般財団法人日本情報経済社会推進協会（JIPDEC）
客員研究員　佐藤 慶浩

03 規則解説 27P
GDPR 対応のアプローチ
～GDPRの概要、個人情報保護法との比較、日本
企業に必要な対応及びISO/IEC 27701の活用～
執筆： ISO/IEC JTC1/SC27/WG5 エキスパート
一般財団法人日本情報経済社会推進協会（JIPDEC）
主任研究員　都司 哲也

04 認定動向 34P
認定基準のアウトラインが見え出したら
独自基準で認定をスタートしたい
取材先： 一般社団法人情報マネジメントシステム認定センター(ISMS-AC)
事務局長　星 昌宏 氏
事務局次長　野中 武志 氏
主任研究員　富永 典子 氏

05 認証動向 36P
BSI でプライベート認証を発行
認証組織のほとんどがグローバル企業
取材先： BSIグループジャパン株式会社
認証事業本部 部長 プロダクトマネージャー
中村 良和 氏

06 取組方法 38P
日本の組織は ISO/IEC 27701 に
どう取り組むべきか
～学習手順と重要ポイントを提案～
執筆： 株式会社シーピーデザインコンサルティング
代表取締役社長
鈴木 靖

01
規格動向

プライバシー保護ならISO/IEC 27701 個人情報保護なら JIS Q 15001 コンプライアンス対応の選択肢が増える

取材先：
ISO/IEC JTC1/SC27/WG5 エキスパート
一般財団法人日本情報経済社会推進協会（JIPDEC）
客員研究員　佐藤 慶浩 氏
主任研究員　郡司 哲也 氏

ISO/IEC 27701は、ISO/IEC 27001と27002の拡張規格として実際にはどのように使われるのか、個人情報保護マネジメントシステム規格であるJIS Q 15001とどのように棲み分けることになるのか、GDPR対応として活用できるのか、今後の規格開発に与える影響は何か － ISO/IEC 27701規格を開発したISO/IEC JTC1/SC27/WG5にエキスパートとして参加している佐藤慶浩氏と郡司哲也氏から話を聞いた。（本誌編集部）

ISO/IEC 27701はISO/IEC 27001規格に追加されて使用される

－ISO/IEC 27701はプライバシー保護に関する要求事項でありガイドラインでもあります。この規格はISO/IEC 27001と27002の拡張という位置付けがされていますが、実際にはISO/IEC 27001認証の中でどのような使われ方をされるのでしょうか。

ISO/IEC 27701はISO/IEC 27001と27002に対する拡張規格として発行されました。ISO/IEC 27001は情報セキュリティマネジメントシステム（ISMS）要求事項の規格であり、ISMS認証の基準となる規格です。ISO/IEC 27701は、ISO/IEC 27001への追記事項を記述したものなので、単独で認証基準として使うものではなく、ISMS認証を受ける中で拡張審査に使うことが考えられます。

もともと個人情報保護に関する国際規格としては、ISO/IEC 27002（情報セキュリティ管理策の実践のための規範）の拡張規格としてISO/IEC 29151（個人を特定できる情報保護のための実施標準）がありますので、現時点でもISO/IEC 27001+ISO/IEC 29151で個人情報保護のためのマネジメントシステムを構築することは可能です。ただ、ISO/IEC 27002の拡張としてのISO/IEC 29151では、管理策対応だけなので、個人情報保護への対応としては不十分ではないか、やはりリスクマネジメントを扱うISO/IEC 27001についても拡張が必要ではないか、という議論が行われて開発されたのが、ISO/IEC 27701なのです。

ISO/IEC 27701のタイトルの表記は、Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information managementとなっています。つまり、ISO/IEC 27001とISO/IEC 27002の両方の拡張なのです。当初は、ISO/IEC 27002への拡張としてすでにISO/IEC 29151があったので、ISO/IEC 27001への拡張としての規格を開発するという選択肢もあったのですが、そうするとユーザーは参照する規格が増えるし、規格を開発する側も各規格との整合を取る作業が大変なので、1個の規格でISO/IEC 27001とISO/IEC 27002の両方に対応できるようにしたのです。

では、実際にどういう使われ方をするのかというと、個人情報も情報セキュリティマネジメントの対象としてISO/IEC 27001を基準としたISMS認証を取得している企業が、その拡張としてISO/IEC 27701を追加するというのが一番自然な使われ方だと思います。ISO/IEC 27701は、ISO/IEC 27001とISO/IEC 27002の規格を参照し

佐藤 慶浩（さとう よしひろ）氏

オフィス四々十六（ししじゅうろく） 代表
一般財団法人日本情報経済社会推進協会 客員研究員

ISO/IEC JTC1/SC27（情報セキュリティ技術）で長年エキスパートを務める。SC27/WG1では、ISO/IEC 27002の初期（2001年）開発から参加。その後SC27/WG5（アイデンティティ管理とプライバシー技術）設立時には主査を務める。現在はWG5にのみ参加。JIS Q 15001改正時には原案作成委員会委員を務めた。

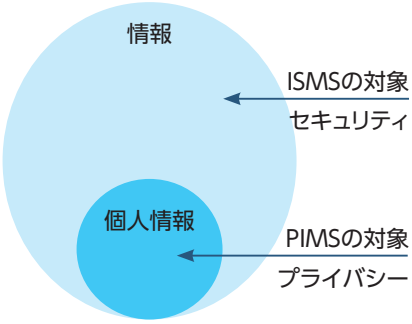
た上で、そこに追加部分だけを書いた内容になっています。なぜそのような構造になっているかというと、追加部分だけが書いてあって、元の部分は、ISO/IEC 27001とISO/IEC 27002の規格書を参照することで、ISO/IEC 27701によって、ISO/IEC 27001とISO/IEC 27002には変更がなく、従来のISMSと同じものとして読むことができるようにするためです。

ただ、ISMSを構築していない組織が、ゼロから個人情報保護に取り組むために、ISO/IEC 27701をマネジメントシステム規格として利用することはあまりないと考えられています。現状では、ISO/IEC 27701は拡張規格なので、組織はISO/IEC 27001とISO/IEC 27002に対応できていることが前提になっています。そのため、個人情報保護だけをやりたい組織にとっては、ゼロからISO/IEC 27701に取り組もうとすると、個人情報保護以外のセキュリティ対策までやらなければならなくなるので、対象範囲がやりたいことよりも広くなり、規格としての需要がそれほど見込めないからです。

ISO/IEC 27001は情報セキュリティ、ISO/IEC 27701はプライバシーが対象

—ISO/IEC 27701の特徴について、ISO/IEC 27001との比較、JIS Q 15001との比較の中で説明していただけますか。

ISO/IEC 27001はISMSの規格ですが、ISO/IEC 27701はPIMSの規格です。PIMSというのは、Privacy Information Management Systemの略称です。ISO/IEC 27701の中に出て来るPIMSの定義は「PII（個人を特定できる情報）の処理により潜在的に影響を受けるプライバシーの保護に取り組む情報セキュリティマネジメントシステム」（information security management system which addresses the protection of privacy as potentially affected by the processing of PII〈Personally Identifiable Information〉）と書かれています。つまり、この規格で管理の対象になっているのは、personal informationではなく、privacyなのです。ISMSですと、組織が扱うすべての情報に関して、セキュリティの観点で管理します。一方、PIMSですと、組織が扱う情報の中の個人情報に該当する部分に関して、プライバシーの観点で管理します。両者の関係を図で表すとこのようになります。



郡司 哲也（ぐんじ てつや）氏

一般財団法人日本情報経済社会推進協会 電子情報利活用研究部 主任研究員
国際調査グループ グループリーダー
ISO/IEC JTC1/SC27/WG5エキスパート。ISO/PC317にもエキスパートとして参加し、国内では同PCの国内審議団体の事務局も担当。経済産業省の「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」作成やJIPDECがウェブ上で公開しているGDPRの仮訳作成にも参加。

日本のJIS Q 15001（個人情報保護マネジメントシステム）は、保護の対象が個人情報です。一方、ISO/IEC 27701の保護の対象はプライバシーです。両者は似て非なるものです。

個人情報というのは、概ね「個人を特定できる情報を含む情報」のことです。JIS Q 15001は、個人情報保護法の改正に合わせて改訂されています。個人情報は、取り扱われる状態によって必要な保護の程度が変わって来ますので、個人情報保護法では個人情報を段階化しています。まず、個人を特定する情報を含む情報として「個人情報」がありますが、それが、例えば検索できるように体系化されると「個人データ」になり、さらに個人データが6カ月以上保管されると「保有個人データ」になります。ある情報があって、その内容が変わるわけではないのに、呼び方が「個人情報」「個人データ」「保有個人データ」と変わっていくのです。出世魚で言えば、魚のブリは同じなのに、ワカシ（ツバス）→イナダ（ハマチ）→ワラサ（メジロ）→ブリと呼び名が変わるようなものです。このように定義を状態に合わせて分けることで、各状態において個人情報保護の要求事項が段階的になるようにしているのです。同様に匿名加工情報があり、現在はさらに仮名化データについても改正案を検討中で、個人情報の定義にさらにもう一枠を設けるような議論が行われています。つまり、個人情報の定義が複雑になり始めているのです。

このような日本の動きに比べ、ISO/IEC 27701は、あくまでも個人情報をプライバシーの観点で保護するための規格ですから、個人情報の定義は細分化せずに、日本の個人情報保護法における個人情報の定義に相当するところだけで終わっています。規格自体も、個人情報の取り扱い方によって、プライバシーの観点から懸念のあるものに対しては保護するという構造になっています。

ですから、個人情報の観点から保護したいのか、プライバシーの観点から保護したいのかによって、JIS Q 15001かISO/IEC 27701かを選ぶことができると思います。

ISO/IEC 27701はプライバシー保護の観点で規格が書かれていますが、これは欧米の発想であり、個人情報を保護するという法律を作っているのは、おそらく日本と韓国くらいでしょう。それ以外のほとんどの国の法律は、保護の目的はプライバシーです。日本の個人情報保護法は、個人の権利・利益を保護するためと書いているものの、個人情報そのものを保護するという運用がされているように思われます。

欧米の考え方に合わせたいというのなら、ISO/IEC 27701の方が、相性がいいでしょう。ですが、ISO/IEC 27701では、日本のように細かい個人情報の定義、例えば個人情報と保有個人データの区別などはしていません。なぜなら、ISO/IEC 27701は、個人情報を細分化して段階的に保護するのではなく、その情報が取り扱われた時にプライバシーの侵害があれば保護しなければなら

ISO/IEC 27701の附属書Dに掲載されているGDPRとの対応表の一部

Subclause of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)

ないという発想なので、個人情報を細かく定義する必要がないのです。

法律へのコンプライアンスとしてなら、グローバルにビジネスを展開している会社であればISO/IEC 27701とJIS Q 15001の両方を使うという手もあるでしょうし、国内だけでビジネスを行っている会社ならJIS Q 15001だけを使うという選択肢もあるでしょうから、ISO/IEC 27701の発行によって、コンプライアンス対応として規格の選択肢が増えたと考えるべきでしょう。

企業にとって魅力的なのはGDPR対応表

ーグローバル対応で言えば、GDPR（General Data Protection Regulation:一般データ保護規則〈EU域内の個人データ保護を規定する法律、2018年5月25日に施行〉）に対応しなければならない企業は、ISO/IEC 27701に高い関心を持つのではないでしょうか。

ISO/IEC 27701発行以前から、ISO/IEC 27001+ISO/IEC 29151で個人情報保護のためのマネジメントシステムを構築することが可能であり、それを使ってGDPRに対応することはできたのです。

ですが、ISO/IEC 27701にはGDPR対応表というのが附属書として付いています（**上図表参照**）。ここがおそらく、GDPR対応をしなければならない企業にとっての大きな関心事だと思います。なぜなら、通常はその対応表を自分で作るか、あるいはコンサルタントに作ってもらわなければならないからです。ですが、自分たちで対応表を作っても、EU当局から指摘を受ける可能性もありますので、このように国際規格に載っている、言わばお墨付きの対応表があることは、企業にとっては魅力的だと思います。

ー英国の認定機関であるUKASが、ISO/IEC 27701にはGDPR対応表が載っているのに、GDPRの第42条「認証」・第43条「認証機関」の条文の中にはISO 17021-1（マネジメントシステムの審査及び認証を行う機関に対する要求事項）に基づいて認定されたISO/IEC 27701認証のことが掲載されていないと述べています（2019年10月3日発表）*。ISO/IEC 27001認証の拡張としてISO/IEC 27701が使われるとなると、GDPRと認証制度の関係はどうなるとお考えですか。

ご指摘の通り、UKASの公表

＊ https://www.ukas.com/news/call-for-expressions-of-interest-iso-27701-2019-security-techniques/

文には、ISO/IEC 17021-1に適合する認証機関が実施するISO/IEC 27701の認証は、GDPRの42条及び43条の要求を満たさないと記載されています。ただし、ISO/IEC 27701に関する認証を法律の枠組みの中でどう使うかというのは、GDPRが定めるのではなくて、GDPR配下にあるEU各国が自国の認証制度の中で決めることですので、EUの部外者としては何とも申し上げられません。

認証を取得する組織の立場からすると、より重要なことは、ISO/IEC 27701は拡張規格なので、ISO/IEC 27001/27002をやらずして、ISO/IEC 27701だけをやるという選択肢がないことです。GDPRが求めているのは、個人情報のプライバシー保護に関わる部分だけです。他方、ISO/IEC 27701はISO/IEC 27001/27002の拡張規格ですから、プライバシー保護対策だけでなく、個人情報以外の情報セキリュティ対策もやらなければなりません。すると、本来GDPRが求めていない領域にも、認証を取得するための追加の対応をしなければならないのです。

例えば、個人情報が含まれていない機密文書や図面の管理は、ISMSの対象にはなりますが、GDPRとは関係ありません。すると、GDPRにおいて、ISO/IEC 27701を追加したISO/IEC 27001の認証を取りなさいと言うことは、法律の根拠がなくなってしまいます。

EU各国が、本来のプライバシー保護を行うためには、情報セキュリティ対応まで実施しなければならないと考え、自国の認証制度として採用するようになってくれば、GDPRの認証の条項にISO/IEC 27701が入ってくるかもしれません。

ISO/IEC 27701に取り組む上で必要なガイドラインがどんどん出て来る

—ISO/IEC 27701の発行以降、プライバシー保護に関する国際規格の新たな開発動向について教えてください。

ISO/IEC 27701が発行されたことで、リスクマネジメントの中でプライバシー保護をどう考えていくかについての検討が始まりましたので、プライバシー保護に関心のある方にとっては、これから有益な情報がどんどん出て来ると思います。

例えば、2014年に経済産業省は「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」を発行しており、この中で、ウェブ上でユーザー登録をする時にはどういう通知をして、どういう同意の取り方に注意すればいいか、といったことが書かれていますが、このガイドラインをベースに日本が国際規格案を提案し、2020年3月にはISO/IEC 29184（Information technology − Online privacy notices and consent:情報技術−オンラインのプライバシーに関する通知と同意）として発行される予定です。これは日本提案の国際規格なので、JIS規格化される可能性が高いと思います。

今後はこのように、ISO/IEC 27701に取り組む上で必要となる具体的なガイドラインが出て来ると思います。ISO/IEC 27001は、認証目的で取り組む企業がほとんどだと思いますが、ISO/IEC 27701は、認証とは関係なく、ガイドラインとして使うためだけに取り組む企業も出て来るかもしれません。

また、ISO/PC317という消費者保護に関する国際規格を審議するプロジェクト委員会では、「privacy by design for consumer goods and services（消費財及びサービスの設計によるプライバシー）」についての規格を作成中です。これは、消費者向けの製品やサービスに、プライバシー・バイ・デザインを実装するためのガイドラインです。先ほど述べた経済産業省の「ガイドライン」は、ウェブサイトやオンラインゲームなどの入口のところで通知を行い、同意してもらうためのガイドラインですが、この規格は、製品やサービスの企画・設計・製造・リリース、さらにはユーザーが利用するプロセスまでのライフサイクルの中で、きちんとプライバシーに配慮したものにしようというものです。

このPCのメンバーは、ISO/IEC 27701を気にしていて、プロダクトの設計においてはマネジメントシステムと似たような配慮が必要であると考えています。同PCが作成中の規格は現在WD（作業原案）段階で、IS（国際規格）として世に出るまでは3年くらいかかりそうです。

（取材日:2019年11月12日）

02

規格解説

ISO/IEC 27701 とプライバシー関連規格 ～開発経緯と要求事項・ガイダンス及び附属書の意図を理解する～

執筆：
ISO/IEC JTC1/SC27/WG5 エキスパート
一般財団法人日本情報経済社会推進協会（JIPDEC）
客員研究員　佐藤 慶浩

1. 規格開発の背景と発行までの議論の経緯について

ISO/IEC JTC1/SC27委員会には5つのWG小委員会があるが、そのWG1小委員会（以下、「WG1」）はISO/IEC 27000ファミリー規格に代表される情報セキュリティ・マネジメントシステム（以下、「ISMS」）などを開発しており、2006年に設立されたWG5小委員会（以下、「WG5」）はアイデンティティ管理、バイオメトリクス、プライバシーに関する規格を開発している。筆者は、2000年からWG1に参加してISO/IEC 27002（以下、「27002」）の開発を担当した後に、WG5設立方針の審議を担当し、設立後はWG5国内小委員会の主査を務めた。

WG5におけるプライバシー関連の規格は、「ISO/IEC 29100 Privacy framework」（以下、「29100」。英語版は無償。日本語は「JIS X 9250プライバシーフレームワーク」として有償JIS化されている）を中心にして開発されている。2019年10月時点で、プライバシー関連で発行している規格と審議中の規格の一覧を**次頁図表1**に示した。

「ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management」（以下、「27701」）の開発経緯には、「ISO/IEC 29151 Code of practice for personally identifiable information protection」（以下、「29151」。日本語対訳は発行されていない）が関係する。そこで、まず、29151の開発経緯を紹介する。

WG5では、WG1におけるISMSに相当するプライバシー保護のマネジメントシステムをどのように規定するかの検討が、2011年から始まった。

その審議の初期において、当時から存在していた日本の「JIS Q 15001個人情報保護マネジメントシステム－要求事項」（以下、「15001」）を参考資料として提供することが国際会議で求められ、英語の仮訳まで準備したが、日本としては、内容が日本固有であり、15001を国際規格化する方向性がないことから提出しないことになった。このため、審議では、15001の規格が参照されることはなかったが、その規格名を英訳したPersonal information protection management systemという言葉だけは残り、その略語であるPIMSが「ピムズ」と呼ばれた。WG5では、個人情報のことを当初は、Personal informationとしていたが、その後、米国で使われていたPII (Personally identifiable information)として定義したため、29151は、もはや、PIMSではなくなっていたが、その後もPIMSが使われ続けた。

審議はWG1と合同で行われ、新しいマネジメントシステム規格を開発するのか、既存の27001又は27002の拡張とするのかを検討した。情報管理に関するマネジメントシステムは、基本的にISMSに集約し、個別にマネジメントシステム規格を開発しないことが合意され、PIMSは、ISMSの下で構築することになった。次に、27001と27002のどちらか又は両方を拡張するのかが検討されたが、ちょうどその時期にWG1で27002に分野別に追加事項を規定するISMSセクター規格という考

図表1　ISO/IEC JTC1/SC27 WG5 のプライバシー関連規格と審議案件

（行頭の数字は、ISO/IEC の規格番号）

プライバシー関連で発行されている規格（発行順）

29100 Privacy framework
29191 Requirements for partially anonymous, partially unlinkable authentication
29101 Privacy architecture framework
27018 Code of practice for PII protection in public clouds acting as PII processors
29190 Privacy capability assessment model
29134 Privacy impact assessment
29151 Code of practice for personally identifiable information protection
20889 Privacy enhancing data de-identification techniques
27701 Extension to 27001 and 27002 for privacy information management
27550 Privacy engineering for system life cycle processes

プライバシー関連で開発中の規格（発行までのステージの高いもの順）

29184 Guidelines for online privacy notice and consent
20547 Big data reference architecture – Part 4: Security and privacy fabric
27551 Requirements for attribute-based unlinkable entity authentication
27570 Privacy guidelines in smart cities
27555 PII deletion concept in organizations
27556 User-centric framework for PII handling based on privacy preferences

プライバシー関連で規格を開発する投票が行われている案件

Consent record information structure
Organizational privacy risk management
Privacy enhancing data de-identification framework
Requirements for bodies providing audit and certification of privacy information management systems according to 27701 in combination with 27001

プライバシー関連で規格を開発するか審議中の案件

Guidelines for privacy in Internet of Things (IoT)
Privacy consideration in practical workflows
Impact of Artificial Intelligence on Privacy
Privacy engineering model
Guidance on processes of a privacy information management system
Privacy for fintech services

え方ができたため、それと同じ位置付けで開発することにして、27002に対する拡張規格として29151を開発することが決まった。そして、2013年に開発が始まり2017年に発行された。

29151が完成に近づくと、27002の拡張だけではなく、27001への拡張も必要であることがわかり、2017年から新たに審議が行われた。個別のマネジメントシステムを開発しないという方針を維持して、27001に対する拡張規格として27552という規格の開発を始めたが、利用者がより利用しやすくするために、27002に対する拡張も統合して、27001と27002の両方の拡張を27552で規定することになった。27552は、発行の直前で、マネジメントシステムの要求事項規格であることから、規格番号の末尾を01として発行されることになった。それが、27701である。

2. 規格のタイトル、全体構造、27001/27002との関係、適用範囲について

27701のタイトルには、privacy information managementとあるが、これは本来正しくない。なぜなら、privacy informationという情報は扱っていないし、規格本文で使ってもいない。保護の対象はPIIであり、本文で使っているPII protection又はprotection of PIIが正しいだろう。しかし、WG5の内部ではPIMSが既に10年間近くも定着してしまっていた。そのため、略語をPIMSになるように合わせるために、Privacy information management systemをPIMSと定義し、そこから切り取られて、タイトルに、privacy information managementという造語ができあがっている。

もしも、27701のタイトルを見て、「privacy informationって何?」と思われたなら、このような経緯で名付けられただけであり、この規格が何のための拡張であるかを正しく表すならば、PII protection managementであり、ISMSに習うならば、Information privacy managementが正しい。

27701は、そのタイトルのとおり、27001と27002のそれぞれに対応した拡張規格と関連する附属書から構成されている。(**図表2を参照**)

27701を理解するためには、引用規格である、27001と27002、29100について理解している必要がある。27701については、本書執筆時点では、JIS化の予定は決まっていないが、日本語対訳書が2020年3月以後に発行される予定と聞いている。27001と27002については、それぞれに対応しているJIS規格解説本によって理解を深めることができる。29100については、JIS X 9250を参照することができる。

ISMSにおいては、27001でマネジメントシステムを規定し、その附属書Aで管理策を示し、それらの管理策に対応する実施の手引きが27002で規定されている。27001におけるリスクアセスメントの必須事項を27001の附属書Aで規定し、その判断や管理策を採用した場合の手

図表2　27701 規格の構成

1　適用範囲
2　引用規格
3　用語，定義及び略語
4　一般
5　ISO/IEC 27001 に関連する PIMS 固有の要求
6　ISO/IEC 27002 に関連する PIMS 固有の手引
7　PII 管理者のための ISO/IEC 27002 の追加の手引
8　PII 処理者のための ISO/IEC 27002 の追加の手引
附属書 A (規定) PIMS 固有の参照管理目的及び管理策 (PII 管理者)
附属書 B (規定) PIMS 固有の参照管理目的及び管理策 (PII 処理者)
附属書 C (参考) ISO/IEC 29100 への対応付け
附属書 D (参考) 一般データ保護規則への対応付け
附属書 E (参考) ISO/IEC 27018 及び ISO/IEC 29151 への対応付け
附属書 F (参考) ISO/IEC 27701 を ISO/IEC 27001 及び ISO/IEC 27002 に適用する方法

引きとして27002が管理策を補足するという構成になっている。いわば、27001と27002の橋渡しとして、27001の附属書Aは重要な役割を果たしている。

27701においては、27001の要求事項に対するPIMSの追加事項を箇条5で規定し、27002の実施手引きに対するPIMSの追加事項を箇条6で規定している。そのため、箇条5は、shall（しなければならない）で書かれ、箇条6は、should（することが望ましい）で書かれた規定が一つの規格内で混在しているのに違和感があるかもしれない。これについては、それぞれ27001と27002の関係に対応しているものと考えればよい。すなわち、27701の箇条5は27001を引用しており、その中で27001附属書Aが参照されることで、27002が紐付けられ、それを拡張した27701の箇条6は、また27001附属書Aから紐付けられているという構造をなしている。したがって、27701の箇条5は、27001の附属書Aを介して、箇条6を従属させている。

以上に引き続いて、27701では、いわば本体となるPIMS固有の管理目的と管理策を附属書A、Bで規定し、それらのガイダンスを箇条7と箇条8で規定している。

附属書C、D、Eは、他の規格・規則への対応表を、附属書Fは、27001と27002への適用方法についての参考情報を提供している。

次に、27701の本文の内容であるが、27701の適用範囲は、**図表3**のように書かれている。

PIMSという表現については、既に説明したとおりである。ここでは、「privacy managementって何？」と思われるだろうが、この箇所にしか出てこない表現で、規格本文では使われていない。これもPIMSと同じで、PII protection managementと考えればよい。

3. 27001/27002に関する固有要求事項とガイダンスについて

「箇条6 ISO/IEC 27002に関連するPIMS固有の手引」は、「ISO/IEC 27009 Sector-specific application of ISO/IEC 27001」（以下、「27009」）に基づくISMS

図表3　27701の「1 Scope」

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

仮訳：
この規格は，組織の状況の下で，プライバシーマネジメントに関するISO/IEC 27001及びISO/IEC 27002の拡張という形で，プライバシー情報マネジメントシステム(PIMS)を確立し，実施し，維持し，継続的に改善するための要求事項について規定し，手引を提供する。

図表4　27701の「5.1 General」

The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.
NOTE　In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy" applies instead (see Annex F).

仮訳：
“情報セキュリティ”に言及しているISO/IEC 27001:2013の要求事項を，PIIの処理により影響を受ける可能性があるプライバシーの保護へ拡張しなければならない。
注記　実際には，ISO/IEC 27001:2013で“情報セキュリティ”が使用されている場合，その代わりに“情報セキュリティ及びプライバシー”を適用する（附属書F参照）。

図表5　27701 附属書 F : How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

Table F.1 — Mapping of the extension of the term information security by privacy

ISO/IEC 27001	This document (extension)
information security	information security and privacy
information security policy	information security and privacy policy
information security management	information security and privacy information management
information security management system (ISMS)	privacy information management system (PIMS)
information security objectives	information security and privacy objectives
Information security performance	information security and privacy performance
Information security requirements	information security and privacy requirements
information security risk	information security and privacy risk
information security risk assessment	information security and privacy risk assessment
information security risk treatment	information security and privacy risk treatment

セクター規格として開発されている。すなわち、27002の構成を引用した上で、PIMS固有の事項がある箇所にだけ、追加や改定（refine）の実施の手引を規定している。

「箇条5 ISO/IEC 27001に関連するPIMS固有の要求」は、27000シリーズ規格において、27001を拡張した初めてのものとなる。規定の方法は、27009に準じるものとして、27002への拡張と同じ体裁を使い、追加や改定事項がある箇所に、追加や改定の要求事項を規定している。

27001に対する固有要求事項で、最初に必要なことは、PIMSをISMSに組み込むことである。

箇条5と箇条6は、27001の附属書Aを介して紐付けられていることを前節で説明したが、それだけでは、認証規格である27001から見ると、情報セキュリティマネジメントの範囲を超えることができないため、27701の5.1 Generalにおいて、**図表4**のように規定している。

そして、5.1にあるとおり、附属書Fにおいて、**図表5**のような読み替え表を示している。

つまり、27001における information securityをすべて、information security and privacyと読み替えよという規定である。

このような読み替えを認証基準規格で行うことは稀であり、これを実際の認証でどのように行うかについては、図表1の「プライバシー関連で規格を開発する投票が行われている案件」にある「Requirements for bodies providing audit and certification of PIMS according to 27701 in combination with 27001」という審議案件で、2020年4月から検討が始まる予定である。基本的には、「ISO/IEC 27006 Requirements for bodies providing audit and certification of ISMS」に組み込むか拡張して対応することが予想される。

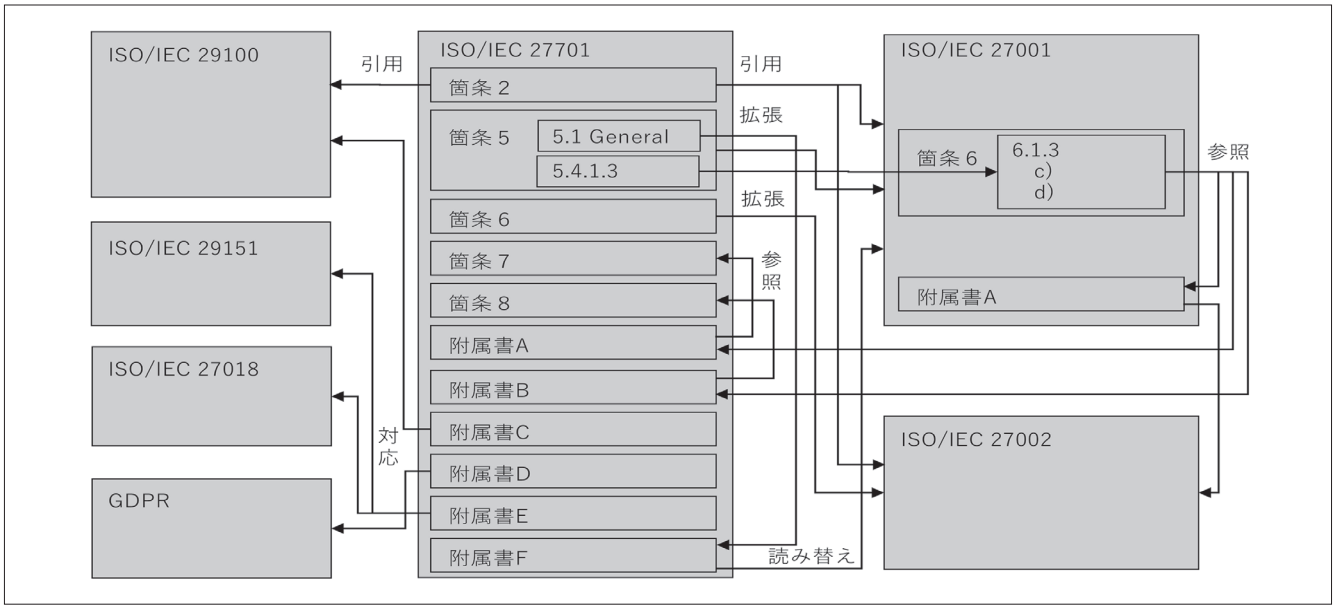
次に必要なことは、PIMS固有の管理策をISMSに従属させることである。

それをするために、27701の「5.4.1.3 情報セキュリティリスク対応」は、27001の「6.1.3 情報セキュリティリスク対応のc)及びd)」による27001附属書Aを使った管理策の確認について、27701の附属書AとBをそれに加えるように改定している。この改定によって、27701の附属書Aが箇条7を、附属書Bが箇条8を活性化している。

箇条6における27002の拡張は、基本的に29151による27002の拡張内容を継承し、さらに新たに検討された内容を追加している。

以上の関係を、**次頁図表6**に示す。

図表6　27701 と関連規格の関係



図表7　27701 の「 1 Scope 」（図表3の続き）

This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

仮訳：
この規格は，PIMS 関連の要求事項について規定し，PII 処理の責任及びアカウンタビリティ をもつ PII 管理者及び PII 処理者のための手引を提供する。

図表8　JIS X 9250「 2 用語定義 」

2.10 PII 管理者（PII controller）
私的な目的でデータを使う個人を除く，PII を処理するための目的及び手段を決定するプライバシー利害関係者。
注記 PII 管理者は，PII の処理を代行するよう他の者［例 PII 処理者（2.12）］に指示することがある。この処理の責任は，依然として PII 管理者にある。

2.12 PII 処理者（PII processor）
PII 管理者に代わり，かつ，その指示に従って PII を処理するプライバシー利害関係者。

4. 27002に付加されたPII管理者・PII処理者向けのガイダンスについて

27701の適用範囲には、図表3の文に続いて、**図表7**のように書かれている。

27701におけるPIMS固有の事項を理解するための基本となるのは、「PII controller（PII管理者）」と「PII processor（PII処理者）」というアクターの区別である。これらは、29100で定義されており、JIS X 9250では**図表8**のとおりに書かれている。

日本の個人情報保護法であれば、PIIは個人情報に、PII管理者は個人情報取扱事業者に、PII処理者は個人情報取扱事業者からの委託先に、それぞれ概ね対応することになる。

例えば、A社がセミナー開催にあたって受講者を募集する場合に、受講申込者の氏名や連絡先などの個

人情報を取得する場合には、A社が個人情報の利用目的を決定するので、PII管理者となる。この時、受講申し込みを受け付けるために、B社が運営する受講者管理サービスを利用する場合には、B社はA社に代わって個人情報を取得し、A社の指示に従って受講申込者名簿などをA社がアクセスできるように処理するので、PII処理者となる。27701の箇条8は、B社がA社のために取得する個人情報の保護について規定するものとなる。仮に、B社が自社のためのセミナー開催をする場合は、それに関連する個人情報の取扱いについてB社は、PII処理者ではなくPII管理者となる。PII管理者として取り扱う個人情報の保護については、箇条8ではなく、箇条7で規定されている。

日本の個人情報保護法では、委託先の安全管理措置（情報セキュリティ対策と同義）については、委託元が監督することになっているが、委託先が講じる対策を限定的には定めていない。しかし、上記の例のとおり、B社は、A社との関係においては委託先であるが、B社はもともと個人情報取扱事業者でもあるはずである。なぜなら、B社は、B社自身の利用目的で取り扱う個人情報をA社とは無関係に保有しているはずだからである。そのため、B社において安全管理措置の内容は、もとからあると想定することができる。その上で、A社はB社に対して善管義務を求める（B社自身の個人情報に対する安全管理措置を、A社から委託する個人情報にも準用させる）ことがあり得るが、ISMSの観点からすると、それはA社が管理すべき個人情報をB社のリスクマネジメントに委ねることになってしまう。これらの関係をPII管理者とPII処理者に分けた上で、PII処理者としてなすべきことを箇条7で規定することにより、A社のリスクマネジメントの下で、B社におけるA社の個人情報の保護を求めやすくなる。

上記の例では、委託先が実施すべき事項を規定すれば、PII処理者としての規定が示されていることと同等の効果があるように思われるかもしれない。しかし、このことは実施すべき事項を怠ることがないようにする対策として有効であるが、実施してはいけないこと又は実施することを予見できなかったことが実施されてしまうことを防ぐ対策として違いが出てくる。

例えば、B社がA社のセミナー受講者に、B社のセミナー案内を配信してしまうということを考えてみる。この場合、A社がその禁止を業務委託契約で明記していればB社が契約に違反したことは明白である。それに加えて、PII処理者が、そのような違反をすることは、PIIを処理するための目的及び手段をB社が決定したことになり、B社は、直ちにPII管理者の立場になる。その結果、利用目的について事前の同意を得ることになっていれば、B社はPII管理者としての義務を怠ったことになる。つまり、事業者はPII管理者の立場かPII処理者の立場かが区別されて順守事項が定められているために、PII処理者がPII管理者の立場のことをした場合には、直ちにPII管理者としての義務が発生する。

一方で、日本の場合には、委託によるものか否かという違いにしているため、上記のような違反は日本においても委託先は個人情報取扱事業者としての義務を負うことになるが、現状の日本法では、利用目的は通知だけで同意を求めておらず、さらに直接取得の場合の通知には公表を含んでいることから、仮に利用目的が公表されていれば、違法になるとは言い切れない。もちろん、そのようなことを契約で禁止していれば契約違反であるが、個人情報保護法違反になるとは限らないということである。

つまり、A社とB社の義務を日本では、委託の範囲とその条件は何であったかという2社間の関係性で整理するしかないが、29100の下では、事業者が個人情報をどの立場で取り扱うかによって明確に区別しているために、関係性とは独立しても各社の義務が定まる点が異なる。

以上のように、PII管理者とPII処理者を区別した上で、PII管理者を対象に附属書Aと箇条7で規定し、PII処理者を対象に附属書Bと箇条8で規定している。

5. 附属書の活用方法について

附属書A及びBは、それぞれ、箇条7及び箇条8に対応するものである。

附属書C「ISO/IEC 29100への対応付け」は、WG5におけるプライバシー関連規格の中心となる

図表9　27701 附属書 C : Mapping to ISO/IEC 29100（一部）

Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
1. Consent and Choice	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.3 Determine when and how consent is to be obtained A.7.2.4 Obtain and record consent A.7.2.5 Privacy impact assessment A.7.3.4 Provide mechanism to modify or withdraw consent A.7.3.5 Provide mechanism to object to processing A.7.3.7 PII controllers' obligations and third parties
2. Purpose legitimacy and specification	A.7.2.1 Identify and document purpose A.7.2.2 Identify lawful basis A.7.2.5 Privacy impact assessment A.7.3.2 Determining information for PII principals A.7.3.3 Providing inf

29100との対応について示しており、**図表9**はその一部である。WG5では、図表1に示したとおり、様々なプライバシー関連規格を議論しているが、27701によってPIMSを構築する際に、どのような関連規格が役に立つかを知ることができる。

附属書E「ISO/IEC 27018及びISO/IEC 29151への対応付け」は、既に発行している規格の要求事項との対応を示している。29151については、本来、27701の箇条6のうちPII管理者への規定と同様の内容であるべきもので、今後の改訂によって整合がとられる予定である。「ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors」（日本語対訳は発行されていない）は、「PII処理者としてパブリッククラウド内のPIIを保護するための実践の規範」であり、タイトルにあるとおり、パブリッククラウドにおいて、PII処理者としての役割に絞って規定している。

附属書F「ISO/IEC 27701をISO/IEC 27001及びISO/IEC 27002に適用する方法」は、先述したとおり、5.1 GeneralによるISMSをPIMSに拡張するための包括的な読み替えのための表などを示している。

特筆すべきは、附属書D「一般データ保護規則への対応付け」である。これは、EUのGDPR（一般データ保護規則）への対応を示したものである。国際規格において、特定の国や地域の法令を具体的に引用することは稀であるが、GDPRはEU以外の他国にも適用を求めているため、国際的に順守する必要がある場合があることから、その対応表が作成された。

このような対応表は、自分でも作成することができるが、附属書Dの作成においては、EU規制当局の作業部会がWG5のリエゾンとしてレビューしているため、公式に認められるものではないもののEUのお墨付きがあると言えるものであり、紐付け及び網羅性の観点で、組織がGDPRに対応する取組みをする時に有用なものである。

また、27701の規格本文では、「in some jurisdictions（法域によっては）」という但し書に続けて、法令による要求事項に触れている箇所がある。これらは、GDPRに対する網羅性を高めるためのものであり、いわば、GDPRのマーカーのようになっている。組織が27701に準拠する時に、これらのマーカーをたどることによって、GDPRへの対応に役立てることができる。

（執筆者プロフィールは15頁参照）