JIS

情報技術－セキュリティ技術－
プライバシー影響評価のためのガイドライン

JIS X 9251：2021

（ISO/IEC 29134：2017）

（JIPDEC/JSA）

令和 3 年 1 月 20 日　制定

日本産業標準調査会 審議

（日本規格協会 発行）

日本産業標準調査会標準第二部会 構成表

	氏名	所属
(部会長)	大 崎 博 之	東京大学
(委員)	青 木 真 理	川崎市地域女性連絡協議会
	青 柳 恵美子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
	儀 　 敦 夫	一般社団法人日本電機工業会
	伊 藤 　 智	一般社団法人情報処理学会情報規格調査会（国立研究開発法人新エネルギー・産業技術総合開発機構）
	岩 渕 幸 吾	一般社団法人電子情報技術産業協会
	内 田 富 雄	一般財団法人日本規格協会
	岡 本 正 英	株式会社日立製作所
	住 谷 淳 吉	一般財団法人電気安全環境研究所
	橋 爪 　 弘	一般社団法人ビジネス機械・情報システム産業協会
	平 田 真 幸	IEC/CAB 日本代表委員（富士ゼロックス株式会社）
	平 本 俊 郎	東京大学
	藤 原 　 昇	一般社団法人電気学会
	山 根 香 織	主婦連合会

主　務　大　臣：経済産業大臣　　制定：令和 3.1.20
官 報 掲 載 日：令和 3.1.20
原 案 作 成 者：一般財団法人日本情報経済社会推進協会
（〒106-0032　東京都港区六本木 1-9-9 六本木ファーストビル内　TEL 03-5860-7551）
一般財団法人日本規格協会
（〒108-0073　東京都港区三田 3-13-12 三田 MT ビル　TEL 03-4231-8530）
審　議　部　会：日本産業標準調査会　標準第二部会（部会長　大崎　博之）

この規格についての意見又は質問は，上記原案作成者又は経済産業省産業技術環境局 国際電気標準課（〒100-8901 東京都千代田区霞が関 1-3-1）にご連絡ください。

なお，日本産業規格は，産業標準化法の規定によって，少なくとも 5 年を経過する日までに日本産業標準調査会の審議に付され，速やかに，確認，改正又は廃止されます。

目　次

まえがき

この規格は，産業標準化法第 12 条第 1 項の規定に基づき，一般財団法人日本情報経済社会推進協会（JIPDEC）及び一般財団法人日本規格協会（JSA）から，産業標準原案を添えて日本産業規格を制定すべきとの申出があり，日本産業標準調査会の審議を経て，経済産業大臣が制定した日本産業規格である。

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本産業標準調査会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

日本産業規格　　JIS
X 9251：2021
(ISO/IEC 29134：2017)

情報技術－セキュリティ技術－
プライバシー影響評価のためのガイドライン

Information technology—Security techniques—
Guidelines for privacy impact assessment

序文

この規格は，2017 年に第 1 版として発行された **ISO/IEC 29134** を基に，技術的内容及び構成を変更することなく作成した日本産業規格である。

なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。

プライバシー影響評価（以下，PIA という。）は，個人識別可能情報（以下，PII という。）を処理するプロセス，情報システム，プログラム，ソフトウェアモジュール，デバイス，その他の取組みにおけるプライバシーに対する潜在的な影響をアセスメントするための手段であり，利害関係者と協議してプライバシーリスクに対応するために必要な行動を起こすための手段である。PIA 報告書には，**JIS Q 27001** における情報セキュリティマネジメントシステム（以下，ISMS という。）の使用による措置など，リスク対応のための措置に関する文書が含まれている場合がある。PIA は単なるツール以上のものである。取組みの可能な限り早い段階から始まるプロセスであり，取組みの結果に影響を及ぼす機会がまだあることから，プライバシーバイデザインを確実にするものである。PIA は，プロジェクトが展開されるまで，さらに，その後も継続するプロセスである。

取組みは，規模及び影響において大きく異なる。“プライバシー”の下に置かれる目標は，文化，社会的期待，及び法域に依存する。この規格は，全ての取組みに適用できる拡張性のあるガイダンスを提供することを目的としている。全ての状況に対応するガイダンスは規範的なものではないため，この規格のガイダンスは個々の状況を尊重し解釈するのがよい。

PII 管理者は，PIA を実施する責任を負うことがあるが，PII 管理者の代行である PII 処理者にこれを支援するよう求める場合もある。PII 処理者又はデジタルデバイスの利用者向け提供者は，自ら PIA を実施することもある。

供給者の PIA 情報は，デジタル接続されたデバイスが，アセスメント対象の情報システム，アプリケーション，又はプロセスの一部である場合に特に関係する。そのようなデバイスの供給者は，PIA を実施する者にプライバシー関連の設計情報を提供することが必要になる場合がある。デジタルデバイスの利用者向け提供者が，PIA に熟練しておらず，PIA のためにリソースをもたない場合がある。

例えば，次のような組織が，通常の事業運営にデジタル接続されたデバイスを使用する。

－　小規模な小売事業者
－　中小企業（SME）

これらの組織が，最低限の PIA 活動を行うことができるように，デバイス供給者は，供給する機器について予想される PII 主体及び／又は中小企業の状況に関して，多くのプライバシーに関する情報を提供，