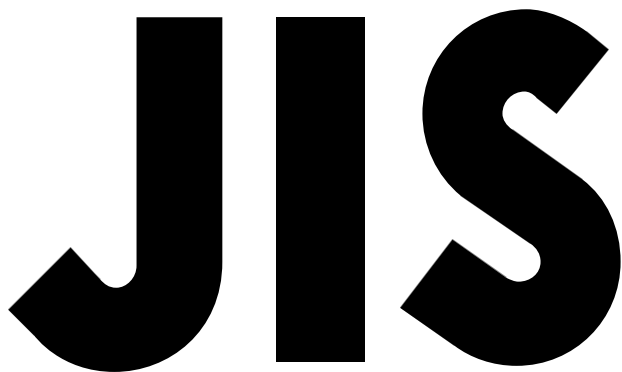




長期署名プロファイル
第 1 部：CAdES デジタル署名

JIS X 14533-1 : 2025
(ISO 14533-1 : 2022)
(JNSA/JSA)

令和 7 年 9 月 22 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)	古 関 隆 章	東京大学
(委員)	青 木 真 理	川崎市地域女性連絡協議会
	岡 本 正 英	IEC/SMB 委員 (株式会社日立製作所)
	上参郷 龍 哉	一般財団法人電気安全環境研究所
	河 合 和 哉	国立研究開発法人産業技術総合研究所
	熊 田 亜紀子	東京大学
	黒 田 健 一	一般社団法人日本電機工業会
	高 橋 弘	IEC/CAB 委員 (富士電機株式会社)
	田 中 宏 和	広島市立大学
	田 辺 恵 子	主婦連合会
	野 田 耕 一	一般財団法人日本規格協会
	林 祥一郎	一般社団法人ビジネス機械・情報システム産業協会
	平 本 俊 郎	東京大学
	本 吉 高 行	一般社団法人電気学会
	山 地 理 恵	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
	横 倉 里 美	一般社団法人電子情報技術産業協会

主 務 大 臣：経済産業大臣 制定：令和 7.9.22

官 報 掲 載 日：令和 7.9.22

原 案 作 成 者：特定非営利活動法人日本ネットワークセキュリティ協会

(〒105-0004 東京都港区新橋 5-7-12 ひのき屋ビル TEL 03-6435-6540)

一般財団法人日本規格協会

(〒108-0073 東京都港区三田 3-11-28 三田 Avanti TEL 050-1742-6017)

審 議 部 会：日本産業標準調査会 標準第二部会 (部会長 古関 隆章)

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イノベーション・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

	ページ
序文	1
1 適用範囲	1
2 引用規格	1
3 用語及び定義	2
4 記号	4
5 要求事項	4
6 長期署名プロファイル	5
6.1 定義されたプロファイル	5
6.2 要求レベルの表現	5
6.3 要求レベルの設定基準	6
6.4 任意選択要素が未実装のときに実行する処置	6
6.5 CAdES-T プロファイル	6
6.6 CAdES-A プロファイル	9
6.7 タイムスタンプ検証情報	11
附属書 A（参考）供給者適合宣言書及びその別紙	13
附属書 B（規定）タイムスタンプトークンの構造	18
参考文献	20
解 説	21

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、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）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。これによって、**JIS X 5092:2008** は廃止され、この規格に置き換えられた。

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。

JIS X 14533 規格群（長期署名プロファイル）は、次に示す部で構成する。

JIS X 14533-1 第 1 部：CAAdES デジタル署名

JIS X 14533-2 第 2 部：XAdES デジタル署名

JIS X 14533-3 第 3 部：PAAdES デジタル署名

長期署名プロファイル

第 1 部 : CAdES デジタル署名

Processes, data elements and documents in commerce, industry and administration—Long term signature—Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)

序文

この規格は、2022 年に第 3 版として発行された **ISO 14533-1** 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。

また、対応国際規格の語句の中で特定の情報を示す識別名称、又は略称として他の規格等で定義されているものは翻訳することなく英語語句のまま記載している。

1 適用範囲

この規格は、長期間にわたってデジタル署名の検証を可能にするための CMS デジタル署名及び CAdES デジタル署名で定義されている要素について規定する。この規格は、デジタル署名自体についての新しい技術仕様書を与えるものではなく、既に存在しているデジタル署名についての技術仕様書の新たな利用制限をもたらさない。

注記 この規格の対応国際規格及びその対応の程度を表す記号を、次に示す。

ISO 14533-1:2022, Processes, data elements and documents in commerce, industry and administration—Long term signature—Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES) (IDT)

なお、対応の程度を表す記号“IDT”は、**ISO/IEC Guide 21-1** に基づき、“一致している”ことを示す。

2 引用規格

次に掲げる引用規格は、この規格に引用されることによって、その一部又は全部がこの規格の要求事項を構成している。この引用規格は、その最新版（追補を含む。）を適用する。

ISO 14533-4, Processes, data elements and documents in commerce, industry and administration—Long term signature profiles—Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)