JIS

CMS 利用電子署名（CAdES）の長期署名プロファイル

JIS X 5092：2008

（ECOM）

平成 20 年 3 月 20 日　制定

日本工業標準調査会 審議

（日本規格協会 発行）

日本工業標準調査会標準部会 情報技術専門委員会 構成表

	氏名	所属
（委員会長）	石 崎　　俊	慶應義塾大学
（委員）	浅 野 正一郎	国立情報学研究所
	大 石 奈津子	財団法人日本消費者協会
	大久保 彰 徳	社団法人ビジネス機械・情報システム産業協会
	筧　　捷 彦	早稲田大学
	加 藤 泰 久	日本電信電話株式会社
	岸　　淳 一	日本銀行金融研究所
	木 戸 彰 夫	日本アイ・ビー・エム株式会社
	後 藤 志津雄	株式会社日立製作所
	塩 沢 文 朗	財団法人日本規格協会
	設 楽　　哲	社団法人電子情報技術産業協会
	関 根 千 佳	株式会社ユーディット
	高 橋 真理子	財団法人日本情報処理開発協会
	田 中　　宏	総務省
	中井川 禎 彦	総務省
	中 山 康 子	株式会社東芝
	平 野 芳 行	日本電気株式会社
	伏 見　　諭	社団法人情報サービス産業協会
	藤 村 是 明	独立行政法人産業技術総合研究所
	宮 澤　　彰	国立情報学研究所
	山 本 喜 一	慶應義塾大学
	渡 辺　　裕	早稲田大学
（専門委員）	安 藤 栄 倫	財団法人日本規格協会

主　務　大　臣：経済産業大臣　　制定：平成 20.3.20
官　報　公　示：平成 20.3.21
原 案 作 成 者：次世代電子商取引推進協議会
（〒105-0011　東京都港区芝公園 3-5-8 機械振興会館　TEL 03-3436-7500）
審　議　部　会：日本工業標準調査会　標準部会（部会長　二瓶 好正）
審議専門委員会：情報技術専門委員会（委員会長　石崎 俊）

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 基準認証ユニット情報電子標準化推進室（〒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，日本工業規格は，工業標準化法第 15 条の規定によって，少なくとも 5 年を経過する日までに日本工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，工業標準化法第 12 条第 1 項の規定に基づき，次世代電子商取引推進協議会(ECOM)から，工業標準原案を具して日本工業規格を制定すべきとの申出があり，日本工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工業規格である。

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，実用新案権又は出願公開後の実用新案登録出願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工業標準調査会は，このような特許権，出願公開後の特許出願，実用新案権又は出願公開後の実用新案登録出願に係る確認について，責任はもたない。

日本工業規格　　JIS
X 5092：2008

CMS 利用電子署名（CAdES）の長期署名プロファイル

Long term signature profiles
for CMS advanced electronic signatures (CAdES)

序文

この規格は，電子署名を長期にわたって検証可能にする長期署名に関して，実装間の相互運用性を確保することを目的とする。各々の実装が参照する長期署名の仕様は，欧州通信規格協会（ETSI）によって策定された CMS 利用電子署名（CAdES）が対象である。

1　適用範囲

この規格は，長期署名プロファイルのうち，CMS 利用電子署名（CAdES）に関するプロファイルについて規定する。

2　引用規格

次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの引用規格は，その最新版（追補を含む。）を適用する。

JIS X 0001　情報処理用語－基本用語

JIS X 0008　情報処理用語－セキュリティ

ETSI TS 101 733　CMS Advanced Electronic Signatures (CAdES)　v1.7.3

注記　http://pda.etsi.org/pda/queryform.asp から入手可能。

3　用語及び定義

この規格で用いる主な用語及び定義は，**JIS X 0001** 及び **JIS X 0008** によるほか，次による。

3.1

長期署名（long term signature）

署名時刻の特定を可能とし，かつ，署名対象及び検証情報を含む署名に関する情報の改ざん（竄）検知を可能とする措置を実施し，署名を長期にわたって検証可能にした署名。

3.2

プロファイル（profile）

参照する仕様の選択要素，値の範囲などに関する相互運用性を満たすための規約。

3.3

要求レベル（required level）

プロファイルを構成する各要素の実装に対する要求の程度。