JIS

タイムスタンピングサービス－
第 1 部：枠組み

JIS X 5063-1：2005

（ISO/IEC 18014-1：2002）

平成 17 年 1 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
	伊 藤 章	財団法人日本規格協会
	伊 藤 文 一	財団法人日本消費者協会
	岩 下 直 行	日本銀行
	岩 田 秀 行	日本電信電話株式会社
	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
	小 川 義 久	財団法人日本情報処理開発協会
	筧 捷 彦	早稲田大学
	河 内 浩 明	社団法人電子情報技術産業協会
	後 藤 志津雄	株式会社日立製作所
	小 町 祐 史	パナソニック コミュニケーションズ株式会社
	関 根 千 佳	株式会社ユーディット
	田 中 謙 治	総務省
	中井川 禎 彦	総務省
	成 田 博 和	富士通株式会社
	平 野 芳 行	日本電気株式会社
	伏 見 論	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 泰	日本アイ・ビー・エム株式会社
	山 本 喜 一	慶應義塾大学
	渡 辺 裕	早稲田大学

主 務 大 臣：経済産業大臣　　制定：平成 17.1.20
官 報 公 示：平成 17.1.20
原案作成協力者：財団法人日本規格協会
（〒107-8440　東京都港区赤坂 4 丁目 1-24　TEL 03-5770-1573）
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，上記原案作成協力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気標準化推進室（〒100-8901　東京都千代田区霞が関 1 丁目 3-1　E-mail:qqgcbd@meti.go.jp 又は FAX 03-3580-8625）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。

まえがき

この規格は，工業標準化法に基づいて，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。

制定に当たっては，日本工業規格と国際規格との対比，国際規格に一致した日本工業規格の作成及び日本工業規格を基礎にした国際規格原案の提案を容易にするために，**ISO/IEC 18014-1**:2002，Information technology－Security techniques－Time-stamping services－Part1:Framework を基礎として用いた。

この規格の一部が，技術的性質をもつ特許権，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，このような技術的性質をもつ特許権，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かかわる確認について，責任はもたない。

JIS X 5063-1 には，次に示す附属書がある。

附属書 A（規定）タイムスタンピングのための ASN.1 モジュール

附属書 B（規定）暗号メッセージ構文抜粋

JIS X 5063 の原国際規格である **ISO/IEC 18014** には，次に示す部編成がある。

ISO/IEC 18014-1 Information technology－Security techniques－Time-stamping services－Part1:Framework

参考：この規格 **JIS X 5063-1** は，**ISO/IEC 18014-1** の一致規格である。

ISO/IEC 18014-2 Information technology－Security techniques－Time-stamping services－Part2:Mechanisms producing independent tokens

ISO/IEC 18014-3 Information technology－Security techniques－Time-stamping services－Part3:Mechanisms producing linked tokens

目　次

日本工業規格　　JIS

X 5063-1：2005

(ISO/IEC 18014-1：2002)

タイムスタンピングサービス－第 1 部：枠組み

Information technology－Security techniques－Time-stamping services－Part1:Framework

序文　この規格は，2002 年に第 1 版として発行された **ISO/IEC 18014-1**:2002，Information technology－Security techniques－Time-stamping services－Part1:Framework を翻訳し，技術的内容及び規格票の様式を変更することなく作成した日本工業規格である。

なお，この規格で点線の下線を施してある“参考”は，原国際規格にはない事項である。

1.　適用範囲　この規格は，次のことを規定する。

1）タイムスタンピング機関の目的を明確にする。

2）タイムスタンピングサービスが基礎とする一般モデルを記述する。

3）タイムスタンピングサービスを定義する。

4）タイムスタンピングの基本プロトコルを定義する。

5）関連するエンティティ間のプロトコルを規定する。

備考　この規格の対応国際規格を，次に示す。

なお，対応の程度を表す記号は，**ISO/IEC Guide 21** に基づき，IDT（一致している），MOD（修正している），NEQ（同等でない）とする。

ISO/IEC 18014-1:2002，Information technology－Security techniques－Time-stamping services－Part 1: Framework (IDT)

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，発効年又は発行年を付記してあるものは，記載の年の版だけがこの規格の規定を構成するものであって，その後の改正版・追補には適用しない。発効年又は発行年を付記していない引用規格は，その最新版（追補を含む。）を適用する。

JIS X 0301:2002　情報交換のためのデータ要素及び交換形式－日付及び時刻の表記

備考　**ISO 8601**:2000, Data elements and interchange formats－Information interchange－Representation of dates and times　からの引用事項は，この規格の該当事項と同等である。

JIS X 5056-1:2002　セキュリティ技術－エンティティ認証－第 1 部：総論

備考　**ISO/IEC 9798-1**: 1997, Information technology－Security techniques－Entity authentication－Part 1: General が，この規格と一致している。

JIS X 5057-1:2003　セキュリティ技術－ハッシュ関数－第 1 部：総論

備考　**ISO/IEC 10118-1**:2000, Information technology－Security techniques－Hash-functions－Part 1: General