JIS

セキュリティ技術—否認防止—
第1部：総論

JIS X 5059-1：1999

(ISO/IEC 13888-1：1997)

(2004 確認)

平成11年11月20日　制定

日本工業標準調査会 審議

（日本規格協会 発行）

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，通商産業大臣が制定した日本工業規格である。

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，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。通商産業大臣及び工業標準調査会は，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，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をもたない。

JIS X 5059-1には，次に示す附属書がある。

附属書A（参考） 参考文献

附属書1（参考） **ISO/IEC 13888-1**：1997 Information technology—Security techniques—Non-repudiation—Part 1：General

主務大臣：通商産業大臣　　制定：平成11.11.20
官報公示：平成11.11.22
原案作成協力者：財団法人 日本規格協会
審議部会：日本工業標準調査会 情報部会（部会長　棟上 昭男）

この規格についての意見又は質問は，工業技術院標準部標準業務課 情報電気標準化推進室（〒100-8921 東京都千代田区霞が関1丁目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。

注）審議専門委員会の欄は，31条但し書きで行った時は省略できる。

日本工業規格 JIS

セキュリティ技術—否認防止— 第1部：総論

X 5059-1：1999
(ISO/IEC 13888-1：1997)

Information technology—Security techniques—Non-repudiation—Part 1：General

序文 この規格は，1997年に第1版として発行された**ISO/IEC 13888-1**，Information technology—Security techniques—Non-repudiation—Part 1：General について，技術的内容を変更することなく日本工業規格として採用するために作成したものであり，**1.**については原国際規格の同項目を全文翻訳し，**2.**以降については，原国際規格の同項目の内容を引用するものとした。

1. 適用範囲 否認防止サービスの目的は，主張された行動又は事象が発生したか否かの紛争を解決するために，その事象又は行動に関する証拠を生成し，収集し，管理し，利用可能にし，有効性を確認することである。この規格（第1部）は，暗号技術に基づく証拠を提供する否認防止機構のためのモデルを規定する。最初に，様々な否認防止サービスに汎用的な否認防止機構を規定し，次に，それらを次のような特定の否認防止サービスに適用する。

— 発信元の否認防止
— 配達の否認防止
— 差出しの否認防止
— 輸送の否認防止

否認防止サービスは，証拠を確立する：証拠は，特定の行動又は事象に関する責任追跡性を確立する。その行動に責任がある場合，又はその事象に関与している場合，エンティティは，それらの証拠が生成されることから，証拠対象者として知られている。

証拠には，次の二つの主要な形式があるが，その本質は，使用される暗号技術に依存する。

— 証拠生成機関によって対称暗号技術を用いて生成される安全な封筒
— 証拠生成者又は証拠生成機関によって非対称暗号技術を用いて生成されるディジタル署名

否認防止機構は，個々の否認防止サービス固有の否認防止トークンを交換するためのプロトコルを提供する。否認防止トークンは，安全な封筒及び/又はディジタル署名と，必要に応じて追加のデータとからなる。否認防止トークンは，紛争当事者又は紛争の仲裁を行う裁定者によって後で用いられることがあるので，否認防止情報として保管されなければならない。

特定の適用業務に対して有効な否認防止方針と，その適用業務が動作する法的環境とに依存して，否認防止情報を完成するために，例えば，次のような追加の情報が必要になる場合がある。

— タイムスタンプ機関が提供する，信頼できるタイムスタンプを含む証拠
— 単一又は複数のエンティティが作成するデータ，実行する行動，又は事象について保証するための，公証者が提供する証拠

否認防止は，特定の適用業務及びその法的環境に対して，明確に定義されたセキュリティ方針の中だけに提供される。否認防止方針は，**ISO/IEC 10181-4**による。