JIS

セキュリティ技術—否認防止—
第2部：対称暗号技術を用いる機構

JIS X 5059-2：1999

(ISO/IEC 13888-2：1998)

(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 5059-2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 13888-2**：1998 Information technology—Security techniques—Non-repudiation—Part 2：Mechanisms using symmetric techniques

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　X 5059-2：1999
—否認防止—　(ISO/IEC 13888-2：1998)
第2部：対称暗号技術を用いる機構

Information technology—
Security techniques—Non-repudiation—
Part 2：Mechanisms using symmetric techniques

序文　この規格は，1998年に第1版として発行された**ISO/IEC 13888-2**, Information technology—Security techniques—Non-repudiation—Part 2：Mechanisms using symmetric tehniques 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2部）は，否認防止サービスに使用可能な一般的な構造，発信元の否認防止（NRO）サービス，配達の否認防止（NRD）サービス，差出しの否認防止（NRS）サービス，及び輸送の否認防止（NRT）サービスを提供するために使用可能な，通信に関する幾つかの特定の機構を規定する。他の否認防止サービスは，セキュリティ方針で定義された要件を満たすように，**8.**に定義する一般的な構造を用いて構築できる。

この規格（第2部）は，偽の否認を防止するために，信頼できる第三者機関（TTP）の存在が不可欠である。通常，オンラインの信頼できる第三者機関が必要である。

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，安全な封筒及び追加のデータからなる。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。

2. 引用規格　**ISO/IEC 13888-2**：1998の2 Normative references による。

3. 定義　**ISO/IEC 13888-2**：1998の3 Definitions による。

4. 表記法及び略語　**ISO/IEC 13888-2**：1998の4 Notation and Abbreviations による。