JIS

セキュリティ技術—かぎ管理—
第1部：枠組み

JIS X 5058-1：1998

(ISO/IEC 11770-1：1996)

(2004 確認)

平成 10 年 10 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，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 5058-1には，次に示す附属書がある。

附属書A(参考)　かぎ管理の脅威

附属書B(参考)　かぎ管理情報オブジェクト

附属書C(参考)　暗号アプリケーションのクラス

附属書D(参考)　証明証のライフサイクル管理

附属書E(参考)　参考文献

附属書1(参考)　**ISO/IEC 11770-1**：1996(Information technology—Security techniques—Key management—Part 1：Framework)

主務大臣：通商産業大臣　　制定：平成 10. 10. 20

官報公示：平成 10. 10. 20

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，工業技術院標準部情報電気規格課（〒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。

日本工業規格 JIS

セキュリティ技術—かぎ管理— X 5058-1：1998
第1部：枠組み (ISO/IEC 11770-1：1996)

Information technology—
Security techniques—Key management—
Part 1：Framework

序文 この規格は，1996年に第1版として発行された**ISO/IEC 11770-1**，Information technology—Security techniques—Key management—Part 1：Framework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，それぞれ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 この規格(第1部)は，以下を記述する。

1. かぎ管理の目的
2. かぎ管理機構の基礎となる一般的なモデル
3. この規格の各部全体に共通なかぎ管理の基本概念
4. かぎ管理サービス
5. かぎ管理機構の特徴
6. ライフサイクル中のかぎ関連情報の管理の要件
7. ライフサイクル中のかぎ関連情報の管理の枠組み

この枠組みは，特定の暗号アルゴリズムの使用から独立した，かぎ管理の一般的なモデルを定義する。ただし，特定のかぎ配送機構は，例えば，非対称アルゴリズムのような，特定のアルゴリズムの特性に依存する場合がある。

かぎ管理機構の詳細は，第2部以後で言及する。対称機構は，第2部[**JIS X 5058-2**(**ISO/IEC 11770-2**) セキュリティ技術—かぎ管理—第2部：対称暗号技術を用いるかぎ確立機構]で言及する。非対称機構は第3部[**JIS X 5058-3**(制定予定)(**ISO/IEC 11770-3**) セキュリティ技術—かぎ管理—第3部：非対称型暗号技術を用いるかぎ確立機構]で言及する。

この第1部は，第2部と第3部を理解するために必要な基本的事項を記述する。かぎ管理機構の使用例は，**ISO 8732**と**ISO 11166**に記載する。否認防止がかぎ管理で必要な場合は，**ISO/IEC 13888**を使用すべきである。

この規格(第1部)は，かぎ管理サービスに用いられるデータ要素の概略と一連の操作を含む，自動及び手動の両方のかぎ管理を記述する。ただし，プロトコルの詳細は規定しない。

かぎ管理は，ほかのセキュリティサービスと同様に，設定されたセキュリティ方針の範囲内でだけ提供可能である。セキュリティ方針の設定は，この規格の適用範囲ではない。

2. 引用規格 **ISO/IEC 11770-1**：1996の**2.**Normative Referencesによる。

3. 定義 **ISO/IEC 11770-1**：1996の**3.**Definitionsによる。