JIS

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

JIS X 5058-2：1998

(ISO/IEC 11770-2：1996)

(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 5058-2には，次に示す附属書がある。

附属書A（参考） かぎ確立機構の特性

附属書B（参考） 補助的技術

附属書C（参考） 参考文献

附属書1（参考） **ISO/IEC 11770-2**：1996（Information technology—Security techniques—Key management—Part 2：Mechanisms using symmetric techniques）

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— 第2部：対称暗号技術を用いるかぎ確立機構

X 5058-2：1998
(ISO/IEC 11770-2：1996)

Information technology— Security techniques—Key management— Part 2：Mechanisms using symmetric techniques

序文 この規格は，1996年に第1版として発行された**ISO/IEC 11770-2**, Information technology—Security techniques—Key management—Part 2：Mechanisms using symmetric techniques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2部)は，有効なセキュリティ方針に従って，対称型又は非対称型の暗号アルゴリズムで使用する，暗号かぎ関連情報の取扱い手順のうち，対称暗号技術を使用するかぎ確立機構を規定する。

この対称暗号技術を使用するかぎ確立機構は，**JIS X 5056-2**(**ISO/IEC 9798-2**)及び**JIS X 5056-4**(**ISO/IEC 9798-4**)のエンティティ認証機構における，テキスト領域の使用方法を特定することによって導き出せる。この規格以外にも，例えば**ISO 8732**のような特定分野向けのかぎ確立機構の規格が存在する。このような機構の目的には，かぎ確立以外に，通信しているエンティティ間の一方向又は双方向の認証が含まれるかもしれない。さらに，確立したかぎの完全性の検証又はかぎ確認も目的になるかもしれない。

この規格(第2部)は，かぎ確立の3種類の環境について言及する。それらは，ポイントツーポイント，かぎ配送センター(KDC)，及びかぎ変換センター(KTC)である。この規格(第2部)は，かぎ関連情報を運ぶメッセージの内容及びかぎ確立に必要なメッセージの内容について記述する。この規格は，メッセージに含まれるかぎ確立以外の情報又はエラーメッセージなどは規定しない。メッセージのフォーマットは，この規格の適用範囲ではない。

この規格(第2部)は，領域をまたがるかぎ管理の方法については，明確には言及しない。さらに，この規格(第2部)は，かぎ管理機構の導入実施方法については規定しないので，この規格(第2部)に適合していても，互換性のない種々の製品が存在するかもしれない。

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

3. 定義と表記法 **ISO/IEC 11770-2**：1996の**3.**Definitions and Notationによる。

4. 要件 **ISO/IEC 11770-2**：1996の**4.**Requirementsによる。

5. ポイントツーポイントかぎ確立 **ISO/IEC 11770-2**：1996の**5.**Point-to-Point Key Establishmentによる。

6. かぎ配送センター **ISO/IEC 11770-2**：1996の**6.**Key Distribution Centreによる。