JIS

セキュリティ技術—
*n*ビットブロック暗号の利用モード

JIS X 5053：1998

(ISO/IEC 10116：1997)

(2004 確認)

平成 10 年 10 月 20 日　改正

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，通商産業大臣が改正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 5053には，次に示す附属書がある。

附属書A（参考） 利用モードの特性

附属書B（参考） 特許に関する情報

附属書C（参考） 利用モードの例

附属書D（参考） 参考文献

附属書1（参考） **ISO/IEC 10116**：1997（Information technology—Security techniques—Modes of operation for an n-bit block cipher）

主務大臣：通商産業大臣　　制定：平成8.11.20　　改正：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—*n*ビットブロック暗号の利用モード

X 5053：1998

(ISO/IEC 10116：1997)

Information technology—Security techniques—Modes of operation for an *n*-bit block cipher

序文　この規格は，1997年に第2版として発行された**ISO/IEC 10116**, Information technology—Security techniques—Modes of operation for an *n*-bit block cipher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　この規格は，*n*ビットブロック暗号のための四つの利用モードを規定する。

備考　**附属書A(参考)**は，各モードの特性に関する解説である。

この規格は，四つの利用モードを規定し，*n*ビットブロック暗号の応用(例えば，伝送データの保護，格納データの保護，認証など)において，各利用モードの仕様及びパラメタの値などの有用な参考を提供する。

2.　定義　**ISO/IEC 10116**：1997の**2.**Definitionsによる。

3.　表記法　**ISO/IEC 10116**：1997の**3.**Notationによる。

4.　要件　**ISO/IEC 10116**：1997の**4.**Requirementsによる。

5.　電子コードブック(ECB)モード　**ISO/IEC 10116**：1997の**5.**Electronic Codebook (ECB) Modeによる。

6.　暗号ブロック連鎖(CBC)モード　**ISO/IEC 10116**：1997の**6.**Cipher Block Chaining (CBC) Modeによる。

7.　暗号フィードバック(CFB)モード　**ISO/IEC 10116**：1997の**7.**Cipher Feedback (CFB) Modeによる。

8.　出力フィードバック(OFB)モード　**ISO/IEC 10116**：1997の**8.**Output Feedback (OFB) Modeによる。

附属書A(参考)　利用モードの特性　**ISO/IEC 10116**：1997の**Annex A**—Properties of the modes of operationによる。

附属書B(参考)　特許に関する情報　**ISO/IEC 10116**：1997の**Annex B**—Information about patentsによる。

附属書C(参考)　利用モードの例　**ISO/IEC 10116**：1997の**Annex C**—Examples for the modes of operationによる。

附属書D(参考)　参考文献　**ISO/IEC 10116**：1997の**Annex D**—Bibliographyによる。