JIS

開放型システム間相互接続―ディレクトリ―第8部　認証の枠組み

JIS X 5731-8：2003

（ISO/IEC 9594-8：2001）

（IPSJ・ITSCJ/JSA）

（2008 確認）

平成 15 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）

日本工業標準調査会標準部会 情報技術専門委員会 構成表

	氏名	所属
（委員会長）	石　崎　　俊	慶應義塾大学
（委員）	浅　野　正一郎	国立情報学研究所
	伊　藤　文　一	財団法人日本消費者協会
	岩　下　直　行	日本銀行金融研究所
	大久保　彰　徳	社団法人日本事務機械工業会
	筧　　捷　彦	早稲田大学
	金　谷　　学	総務省
	小　町　祐　史	パナソニックコミュニケーションズ株式会社
	後　藤　志津雄	株式会社日立製作所
	関　口　　裕	社団法人電子情報技術産業協会
	高　森　國　臣	総務省
	成　田　博　和	富士通株式会社
	八　田　　勲	財団法人日本規格協会
	平　野　芳　行	日本電気株式会社
	関　　俊　司	NTT
	伏　見　　諭	社団法人情報サービス産業協会
	藤　村　是　明	独立行政法人産業技術総合研究所
	宮　川　秀　眞	財団法人日本情報処理開発協会
	宮　澤　　彰	国立情報学研究所
	山　本　　泰	日本アイ・ビー・エム株式会社
	山　本　喜　一	慶應義塾大学
	渡　辺　　裕	早稲田大学

主　務　大　臣：経済産業大臣　　制定：平成 9.10.20　　改正：平成 15.10.20
官　報　公　示：平成 15.10.20
原 案 作 成 者：社団法人情報処理学会
（〒105-0011　東京都港区芝公園 3 丁目 5-8　機械振興会館　TEL 03-3431-2808）
財団法人日本規格協会
（〒107-8440　東京都港区赤坂 4 丁目 1-24　TEL 03-5770-1573）
審　議　部　会：日本工業標準調査会　標準部会（部会長代理　二瓶　好正）
審議専門委員会：情報技術専門委員会（委員会長　石崎　俊）

この規格についての意見又は質問は，上記原案作成者又は経済産業省産業技術環境局 標準課情報電気標準化推進室（〒100-8901　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。

まえがき

この規格は，工業標準化法第 14 条によって準用する第 12 条第 1 項の規定に基づき，社団法人情報処理学会情報規格調査会(IPSJ・ITSCJ)／財団法人日本規格協会(JSA)から，工業標準原案を具して日本工業規格を改正すべきとの申出があり，日本工業標準調査会の審議を経て，経済産業大臣が改正した日本工業規格である。これによって，**JIS X 5731-8**：1997 は改正され，この規格に置き換えられる。

改正に当たっては，日本工業規格と国際規格との対比，国際規格に一致した日本工業規格の作成及び日本工業規格を基礎にした国際規格原案の提案を容易にするために，**ISO/IEC 9594-8**：2001，Information technology―Open Systems Interconnection―The Directory：Public-key and attribute certificate frameworks を基礎として用いた。

JIS X 5731-8 には，次に示す附属書がある。

附属書 A（規定） 公開かぎ証明書及び属性証明書の枠組みの ASN.1 表記

附属書 B（規定） CRL の生成及び処理規則

附属書 C（参考） デルタ CRL の発行例

附属書 D（参考） 権限方針及び権限属性の定義例

附属書 E（参考） 公開かぎ暗号法

附属書 F（規定） アルゴリズムオブジェクト識別子の参照定義

附属書 G（参考） 証明経路制約の使用例

附属書 H（参考） 情報項目定義のアルファベット順索引

附属書 I（参考） 旧版に対する追補及び技術に関する正誤票

附属書 1（参考） **ISO/IEC 9594-8**：2001，Information technology―Open Systems Interconnection―The Directory：Public-key and attribute certificate frameworks

JIS X 5731 の規格群には，次に示す部編成がある。

JIS X 5731-1 第 1 部　概念，モデル及びサービスの概要

JIS X 5731-2 第 2 部　モデル

JIS X 5731-3 第 3 部　抽象サービス定義

JIS X 5731-4 第 4 部　分散操作の手順

JIS X 5731-5 第 5 部　プロトコル仕様

JIS X 5731-6 第 6 部　代表的な属性型

JIS X 5731-7 第 7 部　代表的なオブジェクトクラス

JIS X 5731-8 第 8 部　認証の枠組み

JIS X 5731-9 第 9 部　複製

JIS X 5731-10 第 10 部　システム管理を利用したディレクトリの管理

目　次

日本工業規格　　JIS
X 5731-8：2003
(ISO/IEC 9594-8：2001)

開放型システム間相互接続―ディレクトリ―第8部　認証の枠組み

Information technology―
Open Systems Interconnection―The Directory：
Public-key and attribute certificate frameworks

序文　この規格は，2001年に第4版として発行された**ISO/IEC 9594-8**：2001，Information technology―Open Systems Interconnection―The Directory：Public-key and attribute certificate frameworks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されたものであり，**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，認証及びその他のセキュリティサービスの領域におけるセキュリティ要件を，十分なサービスの基礎である枠組み一式の提供を通して取り扱う。特に，この規格は，次に示す枠組みを規定する。

a)　公開かぎ証明書の枠組み

b)　属性証明書の枠組み

c)　認証サービスの枠組み

この規格で定義する公開かぎ証明書の枠組みは，公開かぎ証明書及び証明書失効リスト（CRL）を含む，公開かぎ基盤（PKI）のための情報オブジェクトを規定する。属性証明書の枠組みは，属性証明書及び属性証明書失効リスト（ACRL）を含む，権限管理基盤（PMI）のための情報オブジェクトを規定する。また，この仕様は，証明書の発行，管理，利用及び失効を行うための枠組みを提供する。両方の型の証明書及びすべての失効リストのスキームに対応した形式定義の形で，証明書及び失効リストの拡張機構を規定する。さらに，この規格は，多くのPKI及びPMIのアプリケーションに対して一般的に有益と期待される，証明書及びCRL用の標準拡張一式を規定する。この規格は，PKI及びPMIのオブジェクトをディレクトリ上に格納するための，オブジェクトクラス，属性型及び照合規則を含むスキーマ要素を規定する。この枠組みを超えたPKI及びPMIの他の要素，例えば，かぎ管理プロトコル，証明書管理プロトコル，操作プロトコル，追加の証明書拡張及びCRL拡張などは，他の標準化団体（**ISO TC68**，IETFなど）によって規定されることを期待している。

この規格で定義する認証スキームは，一般的であり，様々な応用及び環境に適用し得る。

ディレクトリは，公開かぎ証明書及び属性証明書を使用する。この規格は，ディレクトリにおけるこれらの証明書の利用についての枠組みも規定する。証明書を含む公開かぎ暗号技術は，ディレクトリにおいて，厳密認証，署名付き操作及び暗号化操作，署名付きデータ及び暗号化データのディレクトリ上での格