国際標準化の立場から見たCryptrecの意義と課題

2009-02-18

ISO/IEC JTC1/SC27/WG2コンビーナ
苗村 憲司 (naemura@iisec.ac.jp)

国際標準化の立場から見たCryptrecの意義と課題

1. 暗号技術に関する国際標準化の背景

2. 暗号技術の国際標準化の経緯と現状

3. Cryptrecの意義と課題

1. 暗号技術に関する国際標準化の背景

1.1 WTO技術的障壁(TBT)協定（1995年）

http://www.jisc.go.jp/cooperation/wto-tbt-guide.html

http://www.wto.org/English/docs_e/legal_e/17-tbt_e.htm

Article 2. With respect to the Central Government Bodies, Members shall use relevant international standards as a basis for their Technical Regulations.

Article 4. Members shall ensure that their Central Government Standardizing Bodies accept and comply with the Code of Good Practice for the Preparation, Adoption and Application of Standards.

1. 暗号技術に関する国際標準化の背景

1.1 WTO技術的障壁(TBT)協定（1995年）

Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards

D. In respect of standards, the standardizing body shall accord treatment to products originating in the territory of any other Member of the WTO no less favourable than that accorded to like products of national origin and to like products originating in any other country.

E. The standardizing body shall ensure that standards are not prepared, adopted or applied with a view to, or with the effect of, creating unnecessary obstacles to international trade.

1. 暗号技術に関する国際標準化の背景

1.1 WTO技術的障壁(TBT)協定（1995年）

Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards

F. Where international standards exist or their completion is imminent, the standardizing body shall use them, or the relevant parts of them, as a basis for the standards it develops, except where such international standards or relevant parts would be ineffective or inappropriate, for instance, because of an insufficient level of protection or fundamental climatic or geographical factors or fundamental technological problems.

1. 暗号技術に関する国際標準化の背景
1.2 OECDの暗号政策ガイドライン（1997年）

- 原則
  1) 暗号機能の信頼性(trust in cryptographic methods)
  2) 暗号機能の自由選択(choice of cryptographic methods)
  3) 市場の要求に基づく暗号機能の開発(market driven development of cryptographic methods)
  4) 暗号機能の標準(standards for cryptographic methods)
  5) プライバシーおよび個人情報の保護(protection of privacy and personal data)
  6) 法執行のためのアクセス(lawful access)
  7) 責務(liability)
  8) 国際協力(international co-operation)

http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html

2. 暗号技術の国際標準化の経緯と現状
2.1 米国規格DESの国際標準化の開始と中断

- 米国政府標準暗号Data Encryption Standard を公募
  ⇒ IBM提案のアルゴリズムを採用
  ⇒ 1977年に政府標準(FIPS 46)として出版
  ⇒ ANSI標準(DEA1)として出版

- 1980年英国がISO/TC97に対して、暗号アルゴリズムの国際標準化提案
  ⇒ ISO/TC97/WG1
  ⇒ ISO/TC97/SC20(1984年):DEA1国際標準化作業

2. 暗号技術の国際標準化の経緯と現状
2.1 米国規格DESの国際標準化の開始と中断

- 米国商務省長官による反対声明

  理由：(1)暗号アルゴリズムは強度の評価が重要で困難

  (2)暗号関連装置は武器等輸出規制の範囲にある

  ∴ISOにおける標準化には適さない

  対案：暗号アルゴリズム登録制度

- 1987年：ISO/IEC JTC1(Information Technology)発足
⇒SC 27(Security Techniques)
- SC27の担当分野と範囲の特異性：

  (1)適用分野毎のメカニズムの組み込みは除く

  (2)暗号アルゴリズムの標準化はしない ⇒ 1997年、制約解除

2. 暗号技術の国際標準化の経緯と現状
2.2 暗号アルゴリズム登録制度の開始と中断

- 暗号アルゴリズム登録制度(ISO 9979:1991
⇒ JIS X5060:1994、IPAが国内の登録窓口)
  - 公開アルゴリズムも秘密アルゴリズムも受け入れる
  - 登録機関(英国)はその安全性についての責任を負わない
  - 2001年時点で24件（13件は日本の企業等の提案）

  （http://www.ipa.go.jp/security/enc/regist-3.htm）

- ISO/IEC 9979は2005年に廃止
  ⇒ JIS X5060は2008年に廃止

2. 暗号技術の国際標準化の経緯と現状
2.3 AESの成立と暗号アルゴリズム標準化の再開

- DESアルゴリズムの強度低下
  ⇒ Tripple DES（TDEA)の標準化(FIPS 46-3)

- 1997年よりAdvanced Encryption Standard の公募開始
  1999年に最終候補を8つに絞り込み
  2000年、ベルギーのDaemonとRijmen提案のRijndaelを選択
  2001年、FIPS 197として出版

(http://csrc.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf)

- ISO/IEC JTC1/SC27/WG2：2000年より暗号アルゴリズムの標準化を再開

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- SC27 (Security Techniques)
  - WG 1: 情報セキュリティマネジメントシステム（ISMS）
  - WG 2: 暗号とセキュリティメカニズム
  - WG 3: セキュリティ評価技術
  - WG 4: セキュリティコントロールとサービス
  - WG 5: アイデンティティ管理とプライバシー技術

2. 暗号技術の国際標準化の経緯と現状

2.4 ISO/IEC JTC1/SC27における標準化状況

- SC27/WG2の作成した国際規格(例)
  - 暗号アルゴリズム：ISO/IEC 18033
  - ディジタル署名：ISO/IEC 14888(添付型), 9796(復元型)
  - ハッシュ関数：ISO/IEC 10118
  - メッセージ認証コード：ISO/IEC 9797
  - エンティティ認証：ISO/IEC 9798
  - 認証付き暗号：ISO/IEC 19772
  - 鍵管理：ISO/IEC 11770
  - 暗号利用モード：ISO/IEC 10116
  - 乱ビット生成：ISO/IEC 18031
  - 素数生成：ISO/IEC 18032
  - 楕円曲線ベース暗号技術：ISO/IEC 15946

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- ISO/IEC 18033（暗号アルゴリズム）
  - 第1部：総論
  - 第2部：非対称暗号（公開鍵暗号）
  - 第3部：ブロック暗号
  - 第4部：ストリーム暗号
- ISO/IEC 14888（添付型ディジタル署名）
  - 第1部：総論
  - 第2部：整数分解ベースメカニズム
  - 第3部：離散対数ベースメカニズム

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- 18033-2に採用された公開鍵暗号アルゴリズム

  (1)秘密鍵共有方式（Key Encapsulation Mechanism）

  RSA-KEM(米)

  ECIES-KEM(米)

  PSEC-KEM(NTT)

  ACE-KEM(スイス)

  (2)データ秘匿のために暗号化する方式

  RSAES(米)

  HIME(R)(日立)

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- 18033-3に採用されたブロック暗号アルゴリズム
  (1)64ビット長のブロックを対象とするもの
    TDEA(米)
    MISTY1(三菱電機)
    CAST-128(加)
  (2)128ビット長のブロックを対象とするもの
    AES(米)
    Camellia(三菱電機＋NTT)
    SEED(韓)

進行中の作業:韓国等の提案によるアルゴリズムの追加

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- 18033-4に採用されたストリーム暗号アルゴリズム

(1)鍵ストリーム生成

MUGI(日立)

SNOW 2.0(スウェーデン)

(2)出力関数

Exclusive-OR

MULTI-S01(日立)

進行中の作業:欧州提案のアルゴリズムの追加

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- 14888-2に採用されたディジタル署名アルゴリズム
  - Rabin-Williams（米）
  - RSA-PSS（米）
  - GQ1, GQ2(仏）
  - GPS1, GPS2（仏）
  - ESIGN(NTT)

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

- 14888-3に採用されたディジタル署名アルゴリズム
  (1)狭義の離散対数方式
    DSA(米), KCDSA(韓),
  (2)楕円曲線方式
    EC-DSA(米), EC-KDSA(韓), EC-GDSA(独)
  (3)IDベース方式
    Hess（英）, Cha-Cheon（韓）

進行中の作業：ロシア国内規格（EC-RDSA）等の追加

2. 暗号技術の国際標準化の経緯と現状
2.4 ISO/IEC JTC1/SC27における標準化状況

ロシアが国内規格（EC-RDSA）を国際標準に提案した背景

- Proposed standard describes mechanisms that are widely used in the big geographical area – Russia and CIS countries.
- EC-RDSA was developed and described in GOST R 34.10-2001 “Information technology – Cryptographic data security – Electronic digital signature generation and verification processes” by Federal Agency for Government Communication and Information at President of Russian Federation with participation of All-Russian Scientific and Research Institute of Standardization (VNIIstandart).
- GOST 34.10-2001 was adopted and came into effect by Gosstandart of Russia (GOST R) in 2002.
- In 2004 EC-RDSA was adopted as regional standard GOST 340.10-2004 which was destined for inter-state usage in Commonwealth of Independent States (CIS).

3. Cryptrecの意義と課題

- 国際標準化の立場から見たCryptrecの意義
  - 日本の国内規格作成における官と民の役割分担モデル
  - 暗号アルゴリズム登録制度に関する経験からの教訓
  - 暗号評価に関するアジアのリーダ的貢献

- 国際標準化の立場から見たCryptrecの課題
  - ISO/IEC規格との整合性確保
  - 危殆化対策および導入実績評価に基づく見直し
  - 暗号評価に関する国際協調