ISO/IEC JTC1/ SC27/WG2における暗号技術標準化動向

--- 登録制から規格化へ ---

九州大学大学院
システム情報科学研究院
櫻井幸一

90年代(公開鍵)暗号の大発展 その理由は [S.Vanstone@ECC00]

- インターネットの発達
- 暗号技術に関する信用と理解
- 公開鍵インフラ(PKI)
- 法律･規約面での整備(e.g. 電子署名法)
- 応用面からの要求(e.g. 携帯電話、VPN)
- 標準化
- インターネットの発達

IS化されている主な暗号技術

- ブロック暗号利用モード
- データ完全性
- 認証
- 鍵管理
- 電子署名
- 否認不可技術

現在IS化審議中の案件(I)

- TTP・タイムスタンプサービス
- 楕円暗号技術
  - 鍵交換、電子署名(添付型、回復型)
- メッセージ回復型RSA電子署名
  - 9796解読('99) ➔ 修正中
- 機密保護暗号(Encryption)
  - 公開鍵、ブロック暗号、ストリーム暗号

現在IS化審議中の案件(II)

- 擬似乱数生成
- 素数生成
- ハッシュ関数を利用した
  認証技術(含む署名)

SC27における暗号アルゴリズムの標準化の経緯

- 従来
  - 機密保護(Confidentiality)に係わる暗号技術は、SC27では扱わない
    (ISO/IEC JTC1の決定により扱えない規制)
  - 認証、署名、鍵共有は標準化可能
    - 多くの国際標準が策定された
  - DESの国際標準化の頓挫
    - 暗号アルゴリズムの登録制(ISO 9979)の導入へ
  - トリプルDES
    - TC68で標準化

最近の情勢変化

- 数年前より、ISO/IEC JTC1が方針を変更
- IEEEp1363(公開鍵)、
  AES(次世代ブロック暗号)の規格化

→ SC27における機密保護に係わる
暗号アルゴリズムの標準化

(18033 ”Encryption algorithms”)

ー公開鍵、ブロック暗号、ストリーム暗号

SC27国際体制と活動内容

- 担当分野：セキュリティ技術（IT - Security Techniques)
  - Chairman：ドイツ　Walter Fumy(Siemens)
  - Secretariat：ドイツ（DIN） Krystyna Passia
- 下部組織：
  - WG1：情報セキュリティ要求条件と統合技術（Requirements,Security services and guidelines)
    - Convener：イギリス（BSI） Ted Humphreys
    - セキュリティ・サービス等の標準を審議
  - WG2：セキュリティ技術とメカニズム（Security Techniques and mechanisms)
    - Convener：ベルギー（EuroPay） Marijke De Soete
    - 暗号技術及びその使用方法等の標準を審議
  - WG3：セキュリティ評価基準（ Security Evaluation Criteria)
    - Convener：スウェーデン（FMV） Mats Ohlin
    - セキュリティ評価基準及び関連標準類の審議
    - セキュリティ管理ガイドライン等の標準を審議

IS化の体制･手順

- 参加国のNational bodyより構成
  - 欧州(16),アジア(3),北米(2), オセアニア(2), ｱﾌﾘｶ(2), ブラジル(1)　注:投票件のある国･ない国
- プロジェクト提案 → 研究期間 → ドラフト → コメント →国際会議 → ･･･ →投票
  - 国際会議は6ヵ月ごと、
- ドラフト:　Working → Committee → →DecisionIS → IS : IS化まで2年～4年
- 投票:一国一票　（➔欧州:有利）

ISでのプロジェクト提案

1. 新作業項目:New work item
   (a) FIPS(米国規格)のIS化,: TDES, AES
   (b) SC27独自の方式: 9796 RSA署名
   (c) IEEEp1363: 公開鍵技術
   RSA社: ハッシュ関数を利用した認証技術
2. 研究期間(Study Period):6ヶ月～一年
3. ドラフト from エディター

ISOの特徴 (vs　IETF)

- ドラフトの作成
- 投票　or ゴール
- 規格化までの時間（スピード）
- 利用対象
- 相互関係（リエゾン）
- 日本の貢献度
- 暗号技術において

日本の取り組み

- 国内委員会:ベンダー、業界、政府、大学
- 委員会事務局:規格調査会@情報処理学会
  - 苗村SC27委員長(慶応大)、中尾WG1主査(KDDI)、櫻井WG2主査(九大)、田淵WG3主査(富士通)
- (小)委員会2が月ごと、定例技術委員会
- 電子政府プロジェクト　目標2003、
  - 電子署名法　4月から

SC27WG2における日本の貢献

- **ESIGN(NTT):添付型電子署名**
  唯一の日本独自のIS暗号方式
- 国際会議への参加
  - **各WG1,2名 (最近WG2は3～5名)**
- Japanese editors
  - **宝木(日立)WG2('90当時)主査:否認不可技術(IS)**
  - **宮地(JAIST): 楕円暗号回復型署名 (CD)**
  - **櫻井(九大): ストリム暗号 (WD)**
- 国際会議(東京)ホスト
  - 90年、2000年
  - 2000年東京会議 Thanks to ITSCJ, 通産・郵政省

暗号技術における　規格化　対　評価（基準）

- 規格化過程で、評価を行う。
  - SC27ではIS化までに各国が(形式上は)評価する。
- ISO15408　ITセキュリティ評価基準
  - 15408:暗号技術に関する基準は対象外
- AES: DES後継規格の選定プロジェクト
  - デジュールのための暗号強度性能評価
- NESSIE（EU）: 暗号技術評価
- CRYPTREC00（経済省）:
  電子政府利用暗号の評価

暗号技術にかかわる ISO vs. JIS vs. IT国内新法

- 基本的にJISはISの翻訳(全訳or 要約)
  - (＋) 国内規格と国際規格の整合
  - (－)国内独自規格化の困難性
- IT国内新法の登場
  - 電子署名法
- JIS(IS)と国内法との整合性
  - 国際入札の問題 (TBT@WTO)

暗号技術標準化:今後の課題

- SC27国際
  - 登録制 vs. 規格化
    (暗号アルゴリズム)
  - 強度評価 vs.規格化
  - 他機関(IETF, IEEE)との整合性

- 国内の対国際対応
  - 登録制 vs. 規格化
  - 日本提案のIS化
  - IS 対 JIS
  - IS 対 国内IT法
  - 標準化・評価 国内体制

国内標準化と国際標準化の関連

(苗村SC27委員長@慶応大 2000年東京総会報告より)

これまでは，情報セキュリティに関する国内標準化が不明確なまま，国際標準化活動を優先して取り組んきたのが実態であった.

今後は，電子政府，電子商取引，遠隔教育，医療情報ステム等に関して日本固有の要求条件に応じた国内標準

の必要性が高まる可能性がある．その体制をどうすべきかについて本格的に検討すべき時期が来ているのではないだろうか.

今回**DIS 17799**に関して意見が分かれた背景としても，対応する国内規格の不備があった．暗号アルゴリズムについても登録が先行して国内標準化が進まない実態を反省する必要がある.

暗号標準化: 今後の課題

1. 90年代: 登録制
2. AES (98-00)
    1. アルゴリズム公募
    2. 公開評価(強度と性能)
    3. 単一規格アルゴリズム選定
3. 2000年: 標準化、評価
    1. 標準化と評価の関係
    2. 評価 (公開 vs. 非公開)
        - 自主評価
        - 第三者評価: 国 vs. 民間

ISO規格化とは？ (cf. 言語文化)

- 標準化:デファクトを正確に利用すべく。
- 国ごとの政策の優位化
  - 自国の技術･政策を優位に。
  - ガイドライン･ビジネス(認証評価)@UK
- ビジネス戦略(ベンダーにとっても)
- 最先端の研究成果の場(暗号解読)
- 情報社会学･社会政策学の実践･検証