

SC27 (セキュリティ技術) / WG2 (セキュリティ技術とメカニズム)
国際会議出席報告書

委員会名 : SC 27/WG 2 小委員会

報告者 : 宮地充子 (JAIST), 竜田敏男 (IISEC)

渡辺創 (産総研), 櫻井幸一 (九大)

1. 開催場所 : モスクワ~サンクトペテルブルグ (ロシア)
2. 開催期間 : 2007-05-4/8
(ただし, 竜田と櫻井とはその後の 2007-05-11/12 の SC27 総会にも出席)
3. 参加国数 / 出席者数 : 11 カ国 / 29 名
コンピーナ (苗村, 日本 [情報セキュリティ大学院大学]) 秘書 (近澤, 日本 [IPA])
ロシア (3), 南アフリカ (1), 英国 (2), 米国 (2) オーストラリア (1) オーストリア
(1) ドイツ (3), デンマーク (1), 中国 (2) 韓国 (2), 日本 (9: 宮崎 [日立], 田中 [KDDI],
清本 [KDDI], 市川 [アマノ], 大熊 [IPA], 宮地 [JAIST], 竜田 [IISEC], 渡辺 [産総研],
櫻井 [九大])
4. 特記事項
 - 4.1 2-key Triple DES の安全性に関する脚注見直し
TC68/SC2 から, 対称暗号技術 (18033-3) 内の 2-key Triple DES の安全性に関する NIST の方針に関する記述 (footnote) を見直すことが要求されていたが, SC27 総会において, 問題の記述を削除するための Technical Corrigendum を作成することになった. 18033-3/Cor3 のエディタと TC68/SC2 へのリエゾンとして MasterCard の Ward 氏を指名した. また, 暗号の鍵長に関する資料を作成することになり, 寄書募集をすることになった.
 - 4.2 新規の作業項目
 - (1) ロシアからデジタル署名 (14888) のアルゴリズムの追加を提案があり, 現規格 14888-3 の Amendment として着手, ロシアがエディタ担当と決まった. 2001 年に作成されたロシア国内規格であり, 内容は 14888-3 で規定済みの楕円曲線利用アルゴリズムの変形の一つとみられる.
 - (2) 中国からは, エンティティ認証に関する追加提案 (3 者間エンティティ認証プロトコル) が提出された. 簡単なスライドを利用した説明後の協議の結果, 新たな WG2 study period として検討を開始することになった.
 - (3) JTC1 から指示された低電力暗号技術については, ラポータ (櫻井 [九大]) による現状調査の報告と審議を経て, 既存のアルゴリズムの低電力性能および専用アルゴリズムに関する提案募集を WG2 study period として行うことになった. 暗号アルゴリズム標準 (18033) の見直しとも絡んで, 既存の日本提案の暗号アルゴリズムや新規提案が, どう議論されていくか, RFID への応用としても注目される.

4.3 日本からの主な提案とその結果

(1) 日本がエディタを担当している項目の進捗:

- (a) 18014-1(タイムスタンプサービスの枠組み)改版については, エディタの市川氏(アマノ)と宮地(北陸先端大)等の努力により FDIS に進展した.
- (b) 宮地が担当した楕円曲線関係規格では, 15946-1 が FDIS に, 15946-5 が CD にそれぞれ進展した.
- (c) 竜田の担当するエンティティ認証規格(9798-2)が CD に進み, 渡辺(産総研)が担当する否認防止規格(13888-3)は 2ndCD 投票にかけることになった.

(2) 日本から新たに提案された項目:

- (a) ブロック暗号を利用したハッシュ関数(10118-2)改版に当たり日本提案のアルゴリズム(DHF1)を追加することについて議論したが継続検討となった. 改版を担当するエディタには, 日本提案の通り吉田氏(日立)と近澤氏が就任することになった.
- (b) 暗号プロトコルの安全性証明に関する日本提案(日立・宮崎氏担当)は, WG3 の担当範囲に近いとの理由で, WG2 ではなく WG3 での新規作業項目候補として投票にかけられることになった.
- (c) ストリーム暗号のアルゴリズム(KCipher-2)を追加することに関して日本のエキスパート(KDDI)から提案が行われたが, 継続審議となり, ドラフト自体の改定は行われなかった.

4.5 日本からの貢献

(a) コンピナー(苗村)・秘書(近澤)をはじめ, エディタ(宮地・竜田・渡辺・近澤・市川)・レポート(櫻井)・決議集ドラフト委員(竜田)と日本が WG2 作業の大半を担当している. このため, 日本提案の IS 化をはじめ, 多くの成果が出るようになった. 続いて継続的・奉仕的に貢献しているのは英国のみ. 今後も改定や新提案で, WG2 の作業項目は増えると予想され, 日本からの更なる継続的貢献が期待される.

(b) 2008 年春に日本がホストする京都会議の紹介を, 竜田が WG 会合と総会とで行ったが, 大変好評であり効果ありとの感触を得た.

5. 今後の開催予定:

次回 : 第 35th meeting WG : October, 2007, in Lucerne (Switzerland)

次次回 : 第 36th meeting WG・総会 April, 2008, in 京都(日本)

以上.