

SC 27(セキュリティ技術) / WG 2(暗号とセキュリティメカニズム)国際会議出席報告

SC 27/WG 2 小委員会

宮地 充子(北陸先端科学技術大学院大学)

1. 開催場所: ナイロビ(ケニア)
2. 開催期間: 2011-10-09/14
3. 参加国数/出席者数: 2 か国, 2 リエゾン/40 名

Convenor: 近澤(日本, IPA), Vice-Convenor: 竜田(日本, IISEC), Belgium (1), China (1), France (1), 日本 [12: 松尾真一郎[HoD, NICT], 宮地[北陸先端大], 竇木[日立], 吉田[日立], 安田[NTT], 大塚[産総研], 櫻井[IPA], Zheng[産総研], 鈴木[NTT], 松尾俊彦[NTT データ], 上畑[SI], 小宮山[デ協]], ケニア (5), 韓 (2), 露 (5), シンガポール (2), 南ア (2), スウェーデン (1), UK (1), US (4),

Liaison 組織: ECRYPT (1, Belgium と兼任), ETSI (1)

4. 特記事項

4.1 経緯および出張目的

出張者は、2000 年 4 月の London 会議において、楕円曲線暗号の国際規格の第四部(15946-4)のエディタに選任されて以来、15946-4、メッセージ復元型署名(9796-3)、2005 年のクアラルンプールが最初の会議となる楕円曲線暗号の国際規格の第 1 部(15946-1)のエディタを務め、2006 年 11 月の南アフリカ会議から新たに楕円曲線暗号の国際規格第 5 部(15946-5)、タイムスタンプの国際規格第一部(18014-1)のエディタを務め、北京会議の 2009 年 5 月より暗号の国際規格第四部(18033-4)を務める。さらに、2010 年 10 月のベルリン会議から WG2 Study Period on Criteria for the standardization of encryption algorithms のコラポータを務め、2011 年 4 月のシンガポール会議から、鍵管理 - 非対称技術を利用する機構(11770-3)のエディター、暗号の国際規格第一部(18033-1)のコエディタを務め、今回は 21 回目の出席となる。

なお、15946-1 は 2008 年に発行され、18014-1 も 2008 年に発行された。また、2006 年の南アフリカが最初の会議になる 15946-5 も 2009 年に発行された。

本シンガポール会議は Final CD の会議となる 18033-4 のエディタ及び最初の会議である暗号標準選定の study period のラポータの立場として出席した。

4.2 2011-10-10~14 SC27/WG2 での議事内容

10/10 審議事項

(1) WG2 Plenary -近澤 Convenor

-議事次第の最新版(SC27 N10420)のプリントを配布、関連資料を USB メモリーで回覧

-全参加者の自己紹介

-前回の WG2 の Singapore 会議 Resolutions (SC27 N9848) と報告書(SC27 N9849)の確認以降各セッション内容。

(2) FCD 29192-1(軽量暗号 - 総論)

日時 10/10

議論内容 日本からの大きなコメントはなく、そのまま Accept された。FDIS に進むことになった。

(3) FCD 29192-3(軽量暗号 - ストリーム暗号)

日時 10/10

議論内容 日本からの大きなコメントはなく、そのまま Accept された。FDIS に進むことになった。

(4) CD 29192-4(軽量暗号 - 公開鍵利用)

議論内容日本からの大きなコメントはなく、そのまま Accept された。29192-1,2 については FDIS へ、29192-4 について DIS ステージへと進むこととなった。

10/11 審議事項

(5) WD 18014-4(上畑) 日時 10/11

議論内容 2nd WD にになった。

(6) Study Period: Lightweight hash functions (軽量ハッシュ関数)

座長:A. Poschmann

参加国:英国, フランス, 米国, ベルギー, 南ア, 日本

日時 10/11

エディタから本 SP に関する動機, 背景, 主旨等の説明, 特に, 軽量ハッシュ関数の動向等が説明され, 本 SP では標準化を直ちに開始するのではなく, 軽量ハッシュに関する動向チェックを行うという説明が行われた。

次に, 英国, フランス, 米国, ベルギー, 南ア, 日本から軽量ハッシュ関数は興味深い研究分野になりつつあること等の理由から, study period の開始をサポートするという意見が表明された。

日本からは, SHA-3 の動向等を踏まえ, 本 SP では候補を検討するのではなく, 速度/安全性要件, アプリケーション等を主に検討すべきという意見を述べた。

フランスからコンペを行うのが良いのではという意見があったが, 米国が SHA3 コンペ運営等の経験から, コンペはハードワークのため困難という回答が行われた。フランスから, 将来のある時点においては, Ecrypt 2 のリエゾン等を利用して, 暗号コミュニティと連携していきたいとの意見がなされた。

(7) 11770-3

参加者:韓国, 日本(宮地, 松尾他), US, UK, ロシア, 南アフリカ

フランス, ベルギー, 中国, ケニア

日時 10/11

議論内容

鍵管理 - 非対称技術を利用する機構に関する国際規格 11770-3 が 2011 年のシンガポール会議で改訂が決定し, 本ケニア会議から審議が開始した。11770-3 は第三版では, ペアリングを用いた鍵共有方式の規格化を初めて行うことが目的で始まった。なお, ペアリングを用いた鍵共有方式は, 日本で初めて開発された技術である。

このような背景の下, 韓国, US, UK, ロシア, 南アフリカ, フランス, ベルギー, 中国, ケニアの参加のもと会議が進められた。各国からのコメントを会議前に修正し, 事前に関係各位に送付していた。

このため, 会議前に, 会議不参加国とはドキュメントの修正に関してコンセンサスを得ていた。

日本のコメント 16 件, ドイツ 38 件, UK5, 南アフリカ 43 件のコメントを議論した。大きな問題はなく, 全てのコメントについての合意を得ることができた。なお, 新規方式の提案が UK と日本からあった。

UK の方式は 2007 年に発表された方法であり, IEEE に掲載されている。日本の提案は 2010 年に発表された方法である。会議では UK の方式は掲載することが決まった。日本の方式に関しては, 対称・非対称ペアリングの利用可否, 他の方式との比較などのさらなるレポートを次回までに提出することがきまった。各国コメントは問題なく対応したが, 2nd WD でとどまることにした。

なお, call for contribution は今回で打ち切りである。

(8) 18033-1 (Riaal Domingues and Miyaji)

日時 10/11

議論内容

暗号アルゴリズム－総論に関する国際規格 18033-1 が 2011 年のシンガポール会議で改訂が決定し、本ケニア会議から審議が開始した。18033-1 は第二版では、暗号アルゴリズムの規格化の基準、過程を厳密に規格化することが目的で始まった。なお、暗号アルゴリズムの規格は、日本企業からの技術も多く、日本企業の技術の規格化が推進されることが望まれる。

このような背景のもと、韓国、US、UK、ロシア、南アフリカ、フランス、ベルギー、中国、ケニアの参加のもと会議が進められた。各国からのコメントを会議前に修正し、事前に関係各位に送付していた。このため、会議前に、会議不参加国とはドキュメントの修正に関してコンセンサスを得ていた。特に、ロシアとは何度もメール審議を行った。

日本のコメント 4 件、ドイツ 7 件、UK31、ロシア 6 件、US6 件のコメントを議論した。

主なコメントに

1. 会議名の指定は現状のままにすることで合意。ただし、他の会議・ジャーナルも認めるという記載を追加。
 2. 発表後の年数は 3 年とすることで合意。
 3. 評価レポートは 3 件とし、レビューのあるジャーナル 1 件を含むトータル 3 件とした。
 4. 既存の攻撃手法の記載。(これは次のドラフトで記載)
- 全てのコメントについて合意を得たが、既存攻撃手法の記載などがあるので、2nd WD になることが決定した。

(9) WG2 SP (Riaal Domingues and Miyaji)

日時 10/11

議論内容

ラポータが提出した質問に対する各国のコメントを要約した。なお、本セッションの目的は共通認識を持つことである。

主な議論は call for

1. 会議名の指定は現状のままにすることで合意。ただし、他の会議・ジャーナルも認めるという記載を追加。
 2. 発表後の年数は 3 年とすることで合意。
 3. 評価レポートは 3 件とし、レビューのあるジャーナル 1 件を含むトータル 3 件とした。
 4. 既存の攻撃手法の記載。(これは次のドラフトで記載)
- 全てのコメントについて合意を得たが、既存攻撃手法の記載などがあるので、2nd WD になることが決定した。

10/12 審議事項

(10) 匿名電子署名、匿名エンティティ認証

(a) WD 20008-1(匿名電子署名 - 総論)

(b) WD 20008-2(匿名電子署名 - グループ公開鍵利用)

(c) WD 20009-1(匿名エンティティ認証 - 総論)

(d) WD 20009-2(匿名エンティティ認証 - グループ公開鍵による電子署名利用)

日時 10/12

匿名署名, 匿名エンティティ認証については, 日本からのコメントはおおむね Accept された. 今後議論が必要である条項のため, 修正の必要があれば次の国際会議までにオフラインで議論を行い, 次回 CD で修正することとなった. 4 規格とも CD に進むこととなった.

(11) WD 18033-5 ID ベース暗号

日時 10/12

日本エディタの案件であり, 日本から標準化の範囲に関する Contribution を行った. 標準化の範囲を暗号アルゴリズムに限定する方向で, 次回までに 1st WD を作成することとなった.

10/13 審議事項

(12) WG2 Plenary 10/13

審議内容: 10 月 12 日(水)の午後の審議結果の確認と報告を行った. 内容は以下の通り.

+ WG2 Study Period on WG2 Road Map

結果: WG2 Road Map の改訂版: SC27 N10445, 期限: 2011-12-15

+ ISO/IEC 20009-3 Anonymous entity authentication – Part 3: Mechanisms based on blind signatures

(匿名エンティティ認証 – ブラインド署名に基づく機構)

結果: 第 2 回 Editor 募集: SC27 N10453, 第 2 回寄書募集: SC27 N10454, 応募期限: 2012-03-31

+ NP Blind Signature (ブラインド署名)

Editor 候補者の Mr. Jacques Traore が欠席で議論なし

+WG2 Study Period on Password-based anonymous entity authentication

(パスワードベースの匿名エンティティ認証)

Rapporteur の Mr. Yanjiang Yang が欠席のため, WG2 Convenor が状況説明

結果: Study period を 6 か月延長

+Defect report on ISO/IEC 13888-2 Non-repudiation –Part 2: Mechanisms using symmetric techniques

(否認防止 – 対称技術を用いる機構)

+ISO/IEC 18031 Random bit generation (乱数生成)

Ms. Debby Wallner と Mr. Gen'ya Sakurai (櫻井玄弥)が担当

結果: Final corrections: SC27 N10464, コメント処理: SC27 N10465, 出版に進む.

+Amendment to 18031 Random bit generation (乱数生成)

Editor: Mr. Pascal Paillier を Editor に指名することが決まった.

+ Amendment 2 to 14888-3 Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms

(添付型デジタル署名 – 離散対数に基づく機構)

結果: 反対投票もコメントもなく FDAM に進む.

+ DCOR1 to 10118-2/3 Hash-functions Part 2: Hash-functions using an n-bit block cipher & Part 3: Dedicated hash-functions (ハッシュ関数 – n ビットブロック暗号を用いるハッシュ関数 & 専用ハッシュ関数)

結果: DCOR text の SC27 N10071 と SC27 N10045 を ITTF に送付

+Amendment 1 to 18033-3 Encryption algorithms – Part 3: Block ciphers – GOST

(暗号アルゴリズム – ブロック暗号 – GOST 暗号)

結果: “Amendment を中止すべき”が多数だったので, 中止となった.

10/14 審議事項

WG2 Final Plenary

WG2 の Liaison 及び WG2 Resolutions (SC27 N10473) の確認

4.3 今後の展開

報告者が関係する国際規格に関しては以下のスケジュールで考えている。

- ストリーム暗号-(18033-4) 2012 年 12 月に IS 発行
- 鍵管理 11770-3 2012 年春の会議で 2nd WD, 2011 年秋の会議で 1st CD.
- 暗号概要 18033-1 2012 年春の会議で 2nd WD, 2011 年秋の会議で 1st CD
- Study Period 2012 年春の会議で判定基準の方向性の議論

上記国際規格及び Study Period を遅延することなく進行させるように努力したい。なお 18033-1, Study Period に関しては多くの日本の技術が関係しており, それらを含めた進行を進めたい。さらに 11770-3 は日本発祥の双線形写像を用いた鍵共有が関係しており, それらを含めた国際規格化に努力したい。

5. 今後の開催予定:

2012-05-07~11 WG Stockholm, Sweden