

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)
国際会議出席報告書

委員会名 : SC27/WG2

報告者 : 宮地充子 (JAIST) ,
竜田敏男 (情報セキュリティ大学院大学) ,
櫻井幸一 (九大)

1. 開催場所 : レッドモンド(米)
2. 開催期間 : 2009-11-2/6
3. 参加国数/出席者数 : WG 2: 15 カ国+3 リエゾン機関/46 名
ベルギー(1), 加(1), 中国(3), 仏(1), 独(2), 日(18: 宮地, 竜田, 櫻井, 田中 [KDDI 研究所], 渡邊 [産総研], 大熊 [東芝], 安田 [NTT], 苗村 [情報セキュリティ大学院大], 吉田 [日立], 近澤 [IPA], 他 8 名), 韓(2), マレーシア(2), ポーランド(1), ロシア(1), シンガポール(2), 南アフリカ(1), スペイン(1), 英(4), 米(3), SC31(1), VISA(1), TCG(1)
4. 特記事項
 - 4.1 日本からの貢献
日本がエディタなど中心となって担当する項目が次のように進展した。
 - (1) 継続項目
 - 1.1 宮地がコエディタをつとめるストリーム暗号 18033-4 は, Decim (フランス) と K2cipher (日本 KDDI) を盛り込んで 1st CD へ進んだ.
 - 1.2 竜田がエディタをつとめる FCD1770-1 (鍵管理 第1部 枠組み) は, 2nd FCD に進むことになった. 11770-5 が CD に進む場合は, 11770-5 を Intro に入れることにした.
 - 1.3 FCD 10118-2 ブロック暗号のハッシュ関数 (日立・吉田エディタ) は FDIS に進む.
 - 1.4 軽量暗号 29192 (ソニー盛合コエディタ) については, 当初計画に沿って 4 個の part に分割することを決定し, 各 part のエディタ候補を選定して寄書募集と WD 作成に着手した.
 - 1.5 前会議で WD 段階に留まったグループ鍵管理 11770-5 (KDDI 田中コエディタ) は CD 段階に進むことになった.
 - 1.6 前会議で CD 段階に進んだサインクリプション 29150 (産総研 Zheng コエディタ) は CD 投票を行うことになった.
 - (2) 新規項目
 - 2.1 匿名性支援メカニズムについては, 「匿名署名」と「匿名認証」の 2 件について必要な説明文書を作成し, 新規作業項目 (NWI) 投票にかけることを決定した.
 - 2.2 WG2 Roadmap の検討の一環として, 日本提案の Certificateless public key cryptosystem について WG2 SP を開始し, 次会議で NWI 投票に進めることを予定することとした.
 - 4.2 その他の重要項目
ロシアから提案されたハッシュ関数とブロック暗号の追加 (10118-3/Amd1 および 18033-3/Amd1) については, 今会議の検討の結果, ハッシュ関数については安全性の問題があることから着手を見送り, ブロック暗号の安全性については WG2 study period (SP)

の対象とすることになった。

なお、WG2 SP の秘密分散メカニズムについては寄書がなかったことから終了することとした。

5. 今後の開催予定：

2010-04-19～27 (WG 2, SC27)： マラッカ (マレーシア)

2010-10-04～08 (WG 2)： ベルリン (独)

以上