社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (38)
2006／7／21

情報セキュリティの標準化動向について
－ISO/IEC JTC1/SC27/WG2 2006年5月マドリッド会議報告－

宮地 充子[I] 近澤 武[II] 竜田 敏男[III] 大塚 玲[IV] 安田 幹[V] 森 健吾[VI] 才所 敏明[VII]

[I]北陸先端科学技術大学院大学 情報科学研究科 〒923-1292 石川県能美市旭台 1-1
[II]三菱電機株式会社／情報処理推進機構 〒247-8501 神奈川県鎌倉市大船 5-1-1
[III]情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
[IV]情報処理推進機構／産業技術総合研究所 〒113-6591 東京都文京区本駒込 2-28-2
[V]日本電信電話株式会社 NTT 情報流通プラットフォーム研究所 〒239-0847 神奈川県横須賀市光の丘 1-1
[VI]NEC インターネットシステム研究所 〒211-8666 神奈川県川崎市中原区下沼部 1753
[VII]東芝ソリューション株式会社 〒183-8512 東京都府中市片町 3-22

E-mail: [I]miyaji@jaist.ac.jp [II]Chikazawa.Takeshi@bk.MitsubishiElectric.co.jp [III]tatsuta@iisec.ac.jp
[IV]a-otsuka@aist.go.jp [V]yasuda.kan@lab.ntt.co.jp [VI]ke-mori@bx.jp.nec.com [VII]Saisho.Toshiaki@toshiba-sol.co.jp

あらまし 情報社会の進展に伴い，安全な社会システムの構築が産官学において進められている．情報セキュリティ技術の国際標準化活動[I]は，安全な社会システムの構築にとって重要な役割をもつ．ISO/IEC JTC 1/SC 27/WG 2 では，情報セキュリティのアルゴリズム及びプロトコルに関する国際標準化規格の策定を進めている．本報告書は，現在，ISO/IEC JTC 1/SC 27/WG 2 で審議事項を解説すると共に，特に今年の5月に行われたマドリッド会議に関して報告する．

キーワード ISO，IEC，情報セキュリティ，マドリッド会議

On the Standardization of Information Security
－Report on the Madrid Meeting in May, 2006－

Atsuko MIYAJI[I] Takeshi CHIKAZAWA[II] Toshio TATSUTA[III]
Akira OTSUKA[IV] Kan YASUDA[V] Kengo MORI[VI] Toshiaki SAISHO[VII]

[I]JAIST 1-1 Asahidai, Nomi, Ishikawa, 923-1292 Japan
[II]Mitsubishi Electric/IPA 5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501 Japan
[III]IISEC 2-14-1 Tsuruya, Kanagawa-Ku, Yokohama, Kanagawa, 211-0835 Japan
[IV]IPA/AIST 2-28-8 Honkomagome, Bunkyou, Tokyo 113-6591 Japan
[V]NTT 1-1 Hikarinooka, Yokosuka, Kanagawa, 239-0847 Japan
[VI]NEC Corporation 1753 Shimonumabe, Nakahara-Ku, Kawasaki, 211-866, Japan
[VII]TOSHIBA Solutions Corporation 3-22 Katamachi, Futyu, Tokyo, 183-8512, Japan

E-mail: [I]miyaji@jaist.ac.jp [II]Chikazawa.Takeshi@bk.MitsubishiElectric.co.jp [III]tatsuta@iisec.ac.jp
[IV]a-otsuka@aist.go.jp [V]yasuda.kan@lab.ntt.co.jp [VI]ke-mori@bx.jp.nec.com [VII]Saisho.Toshiaki@toshiba-sol.co.jp

Abstract Secure information systems are absolutely required in the various situations. The international standardization is one of the important factors for the spread of secure systems. The purpose of the ISO/IEC JTC 1/SC 27/WG 2 is giving the international standardization for the technology of information security such as algorithms and protocols. In this report, we explain the present issues of ISO/IEC JTC 1/SC 27/WG 2 and report the recent meeting results held at the Madrid in May, 2006.

Keyword ISO, IEC, Information Security, Madrid meeting

1. はじめに

情報セキュリティ技術の普及には標準化活動が不可欠である．情報セキュリティ技術のアルゴリズム及びプロトコルに関する国際標準化規格の策定を進めているのが ISO / IEC JTC1 / SC27 / WG2である．ここで，ISO は International Organization for Standardization（国際標準化機構），IEC は International Electrotechnical Commission（国際電気標準会議），JTC1 は，ISO とIEC が共同で設置した情報処理関連技術の国際規格の作成を担当する技術委員会，その下部組織であるSC27は，情報

[I] 本標準化活動を進めるWG2国内委員会は，社団法人情報処理学会・情報規格調査会・技術委員会の傘下にある．

セキュリティ技術全般の国際標準を決定する委員会である. SC27 には本報告書で取り扱うWG2の他, WG1, WG3の合計3つの作業グループが存在する. WG1は情報システムにおけるセキュリティ要求条件, 必要とされるセキュリティサービス, セキュリティを確保するために必要なガイドラインなどの国際規格の策定を担当する. セキュリティマネジメントなどがその代表例である. WG3は, セキュリティ評価及びその評価手法に関わる要求事項, プロテクションプロファイルの登録手続, セキュリティ保証に関わるガイドラインの国際規格の策定を担当する. 各国際組織に対する日本の対応を審議する国内審議委員会が社団法人情報処理学会・情報規格調査会・技術委員会の傘下に, WG1, WG2,WG3国内委員会として設けられている.

SC27 は毎年春と秋に国際標準化会議を行う. 2005 年は 4 月にウィーン会議, 11 月にクアラルンプール会議を行った. 本報告書は, 昨年のウィーン会議の報告[1]に続き, 2006 年 5 月に行われたマドリッド会議の速報と現在 WG2 で策定中の国際規格について解説する. なお, 本会議で SC27 の WG の構成の再編が決定し, 現在の 3WG での会議は本会議が最後となる. 会議の日程, 場所, 日本からの参加者は以下のとおりである.

日程:2006 年 5 月 8 日(月)〜12 日(金)
場所:マドリッド(スペイン)
WG2 の参加国(人数):豪(1), ベルギー(2), 加(2), 中国(4), デンマーク(1), 仏(2), 独(1), 日本(14), 韓(2), シンガポール(1), 南アフリカ(1), スペイン(1), 英(2), 米(2), TC/68/SC2(1), マスターカード(兼務)
WG2 の日本からの参加者(順不同, 敬称略):苗村(IISEC, WG2 コンビーナ), 近澤[2] (IPA, WG2 国際幹事), 大熊, 大塚(IPA), 才所, 山田(東芝ソリューション), 櫻井(九州大), 空本, 市川(アマノ), 竜田(IISEC), 藤岡, 安田(NTT), 森(NEC), 渡辺 (産総研), 三村(日立), 宮地(JAIST)

なお, WG1, WG2, WG3 は同じ会議場で独立して行われ, さらに各 WG を横断する WG として女性委員から構成される非公式の会議も開催される.

本会議でも前回報告のウィーン会議に引き続き, 日本人の参加人数が目立つが, ウィーン会議よりは参加者は減少した. 着実に参加者が増えているのが中国である. 本会議は現在策定中の規格のドラフト会議, 現国際規格の見直し, 新しい標準化審議に関する議論がなされた.

以降, 2 章では, 現在策定中の規格のドラフト及び現国際規格の見直しに関する会議報告をそれぞれ規格番号順に記載する. 3 章では新しい標準化提案に関する会議報告を記述する. 4 章では SC27 の再編について報告する.

2. 国際標準化審議事項

2.1. メッセージ復元型ディジタル署名 (9796)

メッセージ復元型ディジタル署名の国際規格を定める 9796 は, Integer factorization based mechanisms (因数分解に基づく機構)の規格(9796-2), Discrete logarithm based mechanisms(離散対数に基づく機構)の規格(9796-3)の 2 部から構成される. 14888 と 9796 の二つの規格によりディジタル署名全体の規格が行われる. メッセージ復元型署名とは, 署名の中にメッセージの情報の一部もしくは全部を含み, 署名検証時にそのメッセージが復元されることを特徴とする署名である. なお以前, 規格化された 9796-1 は安全性の理由により 2000 年に廃止された. 2 部は 2002 年に継続使用が認められ, 3 部は 2003 年より改訂が進められている.

2.1.1 第 3 部 離散対数に基づく機構 (9796-3)

9796-3 は離散対数問題に基づくメッセージ復元型署名を扱う国際規格である. 現在の IS9796-3 と楕円曲線暗号のメッセージ復元型署名の規格 IS15046-4 を包含する目的で 2003 年より改訂が始まった. ECNR, NR (フィンランド), ECMR (日本, 松下電器), ECAO(日本, NTT), ECPV(米国), ECKNR(韓国)が含まれる. 本規格の編集者は宮地氏が務める. 現在, FDIS 投票を実施している.

2.2. メッセージ認証コード (9797)

9797 はメッセージ認証コード(MAC)の国際規格を定めている. Mechanisms using a block cipher(ブロック暗号を用いる機構)の規格 (9797-1), Mechanisms using a dedicated hash-function(専用ハッシュ関数を用いる機構)の規格(9797-2)と, 2005 年春のウィーン会議で新規に提案された Mechanisms using a universal hash-function(ユニバーサルハッシュ関数を用いる機構)の規格(9797-3)の 3 つから構成される.

2.2.1. 第 1 部 ブロック暗号を用いる機構 (9797-1)

ブロック暗号を用いたメッセージ認証コードに関する規格である. 現在, 1999 年に IS 化された 9797-1 の改訂作業を行っており, 1st CD の段階である.

旧規格に掲載されている 6 つのアルゴリズムのうち, 鍵の異なる 2 つの MAC を並行して計算する形をしたアルゴリズム 5 と 6 の 2 つを削除し, 新たに OMAC と CMAC を追加する方向で改訂が進められている. ただし新しい MAC アルゴリズム 5 は ANSI X9.24 に書かれた一部の使い方をすると問題があるので, NOTE に warning が記述されている.

編集者の Bart Preneel 氏が欠席し, ドラフトも未着だったため, 依然 1st CD の状態に留まっている.

[2] 本マドリッド会議より大塚氏に代わり近澤氏が WG2 国際幹事に就任した.

2.2.2 第 2 部 専用ハッシュ関数を用いる機構 (9797-2)

専用ハッシュ関数を用いたメッセージ認証コードを定めた規格である. 旧規格にはMDx-MAC (RIPEMD-160-MAC, RIPEMD-128-MAC, SHA-1-MAC), HMAC および256bit 以下のメッセージ向けに高速化されたMDx-MACの変形版が掲載されている. 2005 年のウィーン会議で定期見直しが行われ, 改訂することで合意されている. Bart Preneel 氏が編集者を務めているが, 現在のところまだ 1st WD が出ていない.

2.2.3 第 3 部 ユニバーサルハッシュ関数を用いる機構 (9797-3)

2005 年のウィーン会議にて決定した新規格である. 9797-3 に掲載するメカニズムの候補としては, Poly1305-AES, Universal hash function proposed in GCM, UMAC が挙げられている. Bart Preneel 氏が編集者を務めているが, 現在のところまだ 1st WD が出ていない.

2.3. エンティティ認証 (9798)

9798 はエンティティ認証に関する国際規格で, 第 1 部から第 6 部まである. 各部はそれぞれ総論, 対称暗号アルゴリズムを用いる機構, ディジタル署名技術を用いる機構, 暗号検査関数を用いる機構, ゼロ知識技術を用いる機構, 手動データ移動を用いる機構, となっている.

2.3.1 第 2 部 対称暗号アルゴリズムを用いる機構 (IS 9798-2)

第 2 部(対称暗号アルゴリズムを用いる機構, IS 1999 年版)は 2005 年春のウィーン会議で改訂が決定している. その後, 2 回に亘って寄書と編集者の募集が行われたが, 応募が皆無という状況になっていた. 今回の会議では, 旧規格において問題が顕在化している ASN.1 に関して, (旧規格に対する)追補を作成するという作業を, 規格の改訂作業とは独立並行して進めるということが合意された. 追補の編集者を Hans Sommerfield 氏, 改訂作業の編集者として竜田氏を申請中である.

2.3.2 第 4 部 暗号検査関数を用いる機構

5 年見直しの時期を迎えたため, 今回の会議にて審議された結果, 継続使用(confirmation)となった.

2.4. ハッシュ関数 (10118)

ハッシュ関数の国際規格を定める 10118 は, 総論(10118-1), n ビットブロック暗号アルゴリズムを用いるハッシュ関数(10118-2), 専用ハッシュ関数(10118-3), 剰余演算を利用したハッシュ関数(10118-4)の 4 つから構成されるマドリッド会議ではすべてのパートについて審議が行われた.

2.4.1. 第 1 部 総論 (IS 10118-1)

10118-1 はハッシュ関数の総論についての規格であり, ハッシュ関数の規格全体で使われる用語や記号などを定義している. 現在定期見直しの時期であり, マドリッド会議では改訂を行うかどうかと, ドイツより提出された欠陥報告の扱いについて審議を行った.

ドイツの欠陥報告は規格で定義されている round-function という用語がハッシュ関数での文脈とブロック暗号での文脈とで別の意味になり紛らわしいため変更せよというもの. ややエディトリアルな問題でもあり, ドイツも積極的に編集者を務める意思を示さなかったため, 議論の結果, 今後改訂が行われる際には用語の変更を検討することを条件に, 本規格を継続使用することで合意した.

2.4.2. 第 2 部 n ビットブロック暗号アルゴリズムを用いるハッシュ関数 (IS 10118-2)

10118-2 は n ビットブロック暗号アルゴリズムを用いるハッシュ関数に関する規格であり, 3 つの方式が掲載されている. 10118-1 同様に定期見直しの時期であり, マドリッド会議では改訂を行うかどうかと, ドイツと米国から提出された欠陥報告の扱いを審議した.

ドイツの欠陥報告は 10118-1 に対するものと同じ内容であり, 米国の欠陥報告は Annex で例として挙げられている DES がすでに廃止されているため AES におきかるべきだというものである. 議論の結果, 本規格を改訂することが決定された.

なお米国の欠陥報告については本文の改訂作業を待たずに早急に訂正文書を発行することとし, 米国の Debby Wallner 氏が訂正文書の編集者を務めることで合意した.

2.4.3. 第 3 部 専用ハッシュ関数 (IS 10118-3)

10118-3 は, 専用ハッシュ関数に関する規格であり, RIPEMD-160, RIPEMD-128, SHA-1, SHA-256, SHA-384, SHA-512, WHIRLPOOL の 7 つのアルゴリズムが掲載されて国際標準になっている. また, SHA-224 と動作確認用のテストベクタを追加する追補(10118-3 Amendment 1)が発行されている.

マドリッド会議では, 米国の Debby Wallner 氏より提出された SHA-1 に対する米国 NIST の動向についての rapporteur report に従い, SHA-1 の安全性に関して SC27 から出しているステートメントを更新することが確認された.

2.4.4. 第 4 部 剰余演算を用いるハッシュ関数(IS 10118-4)

10118-4 は剰余演算を用いるハッシュ関数に関する規格であり, MASH-1, MASH-2 と呼ばれる RSA 剰余を用いた 2 つの方式が掲載されている.

本規格は 2005 年のウィーン会議において改訂されることが決まったが, その後の編集者募集, 寄書募集に対して何ら提案がなく改訂作業が進んでおらず, 対応を協議した. 規格の廃止と継続使用とで会議に参加した各国の意見は分かれたが, 最終的に改訂を中止して現在の規格のまま継続使用することが決定した.

2.5 かぎ管理 (11770)

鍵管理の国際規格を定める 11770 は，鍵管理枠組みの規格 (11770-1)，対称暗号技術を用いる機構の規格 (11770-2)，非対称暗号技術を用いる機構の規格 (11770-3)，弱い秘密(weak secrets)に基づく機構の規格 (11770-4)の 4 つから構成される．

11770-1 は 1996 年に IS 規格化され，2005 年春のウィーン会議にて継続使用が決定している．11770-2 と 11770-3 は，それぞれ 1996 年版と 1999 年版の旧規格の改訂作業が進められている．11770-4 は 2006 年に IS が出版されている．

2.5.1 第 2 部 対称暗号技術を用いるかぎ確立機構 (11770-2)

11770-2 は対称暗号技術を用いた鍵管理の規格で，ポイントツーポイントの鍵確立機構，鍵配送センタを用いた鍵確立機構，鍵変換センタを用いた鍵確立機構を，それぞれ幾つか規定している．鍵変換センタを用いた鍵確立機構の一つ(方式 12)に対し，セキュリティの問題が指摘されているため，この方式 12 を削除する方向で改訂作業が進められている．Chris Mitchel 氏が編集者を務めているが，公式ドラフトの準備が間に合わなかったため，今回の会議では，現地にて配布された非公式なドラフトに対する非公式なセッションが設けられた．この結果を受けた公式ドラフトが登録されることになる．

2.5.2 第 3 部 非対称暗号技術を用いるかぎ確立機構 (11770-3)

11770-3 は非対称暗号技術を用いた鍵管理の規格で，対称暗号に使用する秘密鍵の共有方式，および配送方式，公開鍵の配送方式をそれぞれ幾つか規定している．2005 年春のウィーン会議にて改訂が決定し，ペアリング技術を加味する方向で現在改訂作業が進められている．カナダの Savard 氏が編集者を務める．本会議では特に大きな議論も無く，CD に進むことになった．

2.6 否認防止 (13888)

否認防止技術の国際規格を定める13888は，General(総論)の規格 (13888-1)，Mechanisms using symmetric techniques(対称暗号技術を用いる機構)の規格 (13888-2)，Mechanisms using asymmetric techniques(非対称暗号技術を用いる機構)の規格 (13888-3)の3部から構成される．

本会議では，第2部と第3部の規格が定期見直しとなったのでその報告を行う．

2.6.1. 第 2 部 対称暗号技術を用いる機構 (IS 13888-2)

13888-2 は対称暗号技術を用いる否認防止機構の規格である．否認防止サービスに適用できる一般的な方式と，発信元の否認防止サービス，配達の否認防止サービス，差出しの否認防止サービス，輸送の否認防止サービスのそれぞれについて方式が規格化されている．

カナダ，米国，英国が改訂を提案し，そのうち，否認防止トークンに含まれる送信者IDを確認する処理を明記する必要があるという英国の意見に基づいて改訂が決定された．現在，編集者募集と寄書募集が行われている．

2.6.2. 第 3 部 非対称暗号技術を用いる機構 (IS 13888-3)

13888-3 は非対称暗号技術を用いる否認防止機構の規格である．発信元の否認防止サービス，配達の否認防止サービス，差出しの否認防止サービス，輸送の否認防止サービスのそれぞれについて方式が規格化されている．

カナダと英国が改訂を提案した．英国からは 13888-2 と同じ意見が提出されており，改訂が決まった．渡辺氏(産総研)を編集者に申請中である．

2.7 添付型ディジタル署名 (14888)

14888 は添付型ディジタル署名の国際規格を定めている．General (14888-1) , Integer factorization based mechanisms(因数分解に基づく機構)の規格(14888-2)，Discrete logarithm based mechanisms(離散対数に基づく機構)の規格(14888-3)の 3 つから構成される．

2.7.1 第 1 部 総論 (14888-1)

14888-1 は添付型ディジタル署名規格全体のフレームワークを定義しており，大塚氏が編集者を担当している．本会議ではディジタル署名規格の再編成の方針について 14888-2 および 14888-3 の修正も含めた合意が得られており，現在，Final CD の投票を実施している．

2.7.2 第 2 部 因数分解に基づく機構(14888-2)

14888-2 は因数分解問題に基づくディジタル署名を扱う規格である．審議中の草案には RW(Rabin-Williams)(米)，RSA(RSA-PSS)(米)，GQ1(仏)，GQ2(仏)，GPS1(仏)，GPS2(仏)，ESIGN(日)の 7 つのアルゴリズムが掲載されている．各国から大量のコメントが寄せられ，Final CD に留まることで合意した．Louis Guillou 氏が編集者を務める．

2.7.3 第 3 部 離散対数に基づく機構(14888-3)

14888-3 は離散対数問題に基づくディジタル署名を扱い，規格は証明書に基づく方式とIDベース方式に別れている．審議中の草案には，証明書に基づく方式として DSA，KCDSA，EC-DSA，EC-KDSA，EC-GDSA の 5 つが掲載され，ID ベース方式として Hess[*2]と Cha-Cheon[*1]の 2 つが掲載されている．Liqun Chen 氏と Pil John Lee 氏が編集者を務める．14888-3 は FDIS 投票を実施している．

[*1] J. C. Cha and J. H. Cheon, An identity-based signature from gap Diffie-Hellman groups, Proceedings of PKC 2002, LNCS 2567, pp. 18-30, Springer-Verlag, 2002.

[*2] F. Hess, Efficient identity based signature schemes based on pairings, Proceedings of SAC 2002, LNCS 2369, pp. 324-337, Springer-Verlag, 2001.

2.8 楕円曲線に基づく暗号技術 (15946)

楕円曲線に基づく暗号技術の国際規格を定める15946は，General(楕円曲線全般)の規格(15946-1)，Digital signatures(ディジタル署名)の規格(15946-2)，Key establishment(かぎ確立)の規格(15946-3)，Digital signatures giving message recovery(メッセージ復元型署名)の規格(15946-4)の4部から構成される．15946-1，2，3 は1998年から審議が始まり2002年に国際規格に，15946-4 は2000年から審議が始まり2003年に国際規格となった．2005年のウィーン会議で1-3部の定期見直しの議論があり，1部のみ改訂し，2，3部に関しては継続使用が決定した．

本会議では，改訂が始まった第1部の報告を行う．

2.8.1. 第 1 部 総論 (15946-1)

15946-1 は楕円曲線に基づく暗号技術の実現に必要になる要素，楕円曲線のパラメータの生成手順やその検証方法，楕円曲線の元を整数に変換する方法等の規格で，昨年の 11 月のマレーシア会議から審議が始まった．付録として，楕円曲線の各種加算公式も記載されている．

本規格には，UK，US，南アフリカ，韓国，オランダ，ドイツなどからコメント寄与があった．大きな議論として，双線形写像のアルゴリズムを新規格に移行するか否かの議論があったが，現状のまま第 1 部に記載することが決定した．

2.9 タイムスタンプサービス (18014)

18014はタイムスタンプサービスの規格であり，第1部は枠組み，第2部は独立トークンを生成する機構，第3部はリンク付きトークンを生成する機構となっている．2005年のウィーン会議で1，2 部の定期見直しの議論で両部とも改訂をすることが決定した．

本会議では，改訂が始まった第 1，2 部の報告を行う．

2.9.1 第 1 部 枠組み (18014-1)

18014-1 は 1stCD の議論を行う予定であったが，ドラフトが締切りに間に合わなかったため，各国の投票結果の締切りが本会議に間に合わなかった．このため，本会議では大きな進展はなかった．特に，次の段階である FCD 投票に進むかどうかは次回 11 月の南アフリカ会議で議論する予定である．

2.9.2 第 2 部 独立トークンを生成する機構 (18014-2)

18014-2も18014-1と同様にドラフトが大幅に遅れ，各国からのコメントが間に合わなかった．しかし，18014-2 は現在，WD の段階であり各国の投票が不要なため，次の段階である CD に進む審議をすることが可能である．しかしながら，US 及び編集者自身が早期 CD を望まないことから，CD に進むかどうかは次回 11 月の南アフリカ会議で議論する予定である．

2.10 暗号アルゴリズム (18033)

18033 は暗号アルゴリズムの国際規格を扱う．18033 には第 1 部から第 4 部まであり，それぞれ総論，非対称暗号，ブロック暗号，ストリーム暗号となっている．

2.10.1 第 2 部 非対称暗号 (18033-2)

第 2 部(非対称暗号)が 2006 年 5 月に出版された．

2.10.2 第 3 部 ブロック暗号 (18033-3)

第 3 部(ブロック暗号)は 2005 年 7 月に発行されているが，規格文書に通常使用されないフォントが最終編集段階で挿入され，表示/印刷が正しくされない恐れが生じたため，訂正文書案を作成した．投票の結果，賛成多数で訂正文書を発行することが決まった．

2.10.3 第 4 部 ストリーム暗号 (18033-4)

第 4 部(ストリーム暗号)は同じく 2005 年 7 月に発行されているが，デンマークから新たなストリーム暗号アルゴリズム Rabbit を追加する提案があったため，さらに各国に追加のストリーム暗号アルゴリズムを募集した．

フランスよりストリーム暗号 DECIM v2 が提案された一方，日本や英国からは ECRYPT の eStream プロジェクト[3]の結果を待つべきとの意見が出された．マドリッド会合では，eStream と本プロジェクトの関係をどうするか審議し，eStream の終了を待つのではなく，並行して追補作成を進めることが決まった．各国提案を調整すべく，新たに寄書提案を募集することになった．それと並行して編集者の Erik Zenner 氏が追補の前段階である WD を用意し，その中に上記 2 方式を含めることが合意された．

2.11 認証付き暗号化(19772)

19772 では対称暗号と MAC の組合せによる認証付き暗号アルゴリズムの国際規格を扱う．小部はない．ウィーン会議で規格のタイトルがデータカプセル化機構(Data Encapsulation Mechanisms)から認証付き暗号化(Authenticated Encryption)に変更されている．マドリッド会議前の時点では，OCB1.0，OCB2.0，AES Key Wrap，CCM，EAX，Encrypt-then-MAC の 6 つのメカニズムが掲載されていた．

マドリッド会議では，カナダ，英国，韓国から，OCB1.0 は OCB2.0 と比較して利点がないため削除すべきだという提案があり，討議の結果 OCB1.0 は規格から削除することが決定した．また，英国から AES Key Wrap メカニズムは使用するブロック暗号を AES に限っていないので名称を変更すべきという提案があり，討議の結果，単に Key Wrap メカニズムとすることになった．

現在のCD文書にはまだ ASN.1 記述や例の記載が欠けており 2ndCD となることで合意した．

---

[3] ストリーム暗号に関しては，欧州の暗号技術評価プロジェクト ECRYPT の一環のプロジェクトとして eStream を運営中で，方式の公募と選考を行っている．現在，一次審査を通った 35 方式について解析中で，2007 年春に最終報告が発行される予定である．

2.12 バイオメトリクス関連

JTC1/SC27 は，バイオメトリクス(生体認証)に関する標準化の中で，バイオメトリクス装置そのものやバイオメトリクス照合プロセス，およびバイオメトリクス応用システムのセキュリティ面での標準化を担当している．

JTC1/SC27 では Ad Hoc Group on Biometrics を設置，バイオメトリクス関係の標準化を進めている他の委員会(例えば JTC1/SC37 や JTC1/SC17 や ISO/TC68 や ITU-T/SG17)と情報交換や技術的な調整をしつつ，担当分野の標準化を進めている．

2.12.1 バイオメトリックテンプレート保護 (24745)

バイオメトリクス照合で参照データとして使用されるテンプレートの保護に関する標準化である．

昨年 4 月のウィーン会合で韓国より寄書が提出され，韓国の Park 氏を編集者として具体的活動が始まった．韓国は，バイオメトリクス技術に基づくテンプレート保護方式の標準化を提案してきたが，独米および日本は，未成熟で実用性も実証されていない技術に基づくテンプレート保護技術の標準化は時期尚早，暗号・認証技術に基づくテンプレート保護の標準化を急ぐべきであると主張してきた．

今回のマドリッド会合では，Park 氏が編集者を降りることになり，山田氏が臨時の編集者を務めた．会議の結論は，独米および日本の主張を反映したものとなった．

今後，新たな編集者を募集し，今回の会合の結論を踏まえた標準化が進められる見込みである．

2.12.2 バイオメトリクスのための認証コンテキスト (24761)

バイオメトリクスのための認証コンテキストを構成するテンプレート，デバイスの安全性・機能・性能の妥当性検証や実行結果の妥当性検証に関わる情報項目とその安全な通知に関する標準化の提案である．

今回のマドリッド会合では，2ndWD へ寄せられたカナダ，英国，および SC37 からのコメントを審議．その結果，SC37，TC68/SC2 との調整事項は残るものの，文書の主要な部分は既に記載され，かつコメントも無く，CD 投票に進むことが承認された．

2.12.3 バイオメトリック技術を用いるディジタル署名生成(検討期間)

バイオメトリクスによる本人確認の情報を用いて署名鍵を生成する技術に関する標準化の提案である．

WG2 の検討テーマであった「バイオメトリックデータの認証」への，韓国からの提案で検討が始まった．が，前述のバイオメリックテンプレート保護と同様の技術に基づく提案であり，独米および日本は，未成熟で実用性も実証されていない技術に基づく標準化は時期尚早と主張してきた．

前回のクアラルンプール会合にて，欠席した提案者から提案を取り下げたい由の連絡を受けた．そこで，ラポータ，寄書を再度募集したが応募が無く，今回のマドリッド会合で本提案の検討期間を終了させることが合意された．

2.12.4 バイオメトリクスのセキュリティ評価(19792)

バイオメトリクスのアルゴリズム，認証装置，アプリケーションのセキュリティ評価に関する WG3 傘下の標準化であるが，WG2 にあるバイオメトリクス関連の標準化と関係が深いため，報告する．

本規格はバイオメトリクスに特有の脅威にフォーカスし，セキュリティ評価の最上位の要件策定を目指している．本規格は WG3 にて進められており，Nils Tekampe(独),Eric Saliba(仏)，三村氏が共同編集者として参画している．

昨年 11 月のクアラルンプール会合では，活動の実態に合わせたタイトルの"Security Evaluation of Biometrics"への変更，スコープに従来の Verification(認証)に加え Identification(識別)も含めることが議決され，CD 投票へ進むことが承認された．

マドリッド会合では，大幅な改訂を必要とするコメントは無かったが，本標準化での懸案の事項であった BEM (Biometric Evaluation Methodology)の取り扱いが決定せず，2nd CD に留まることになった．

なお，BEM に関する標準化の検討期間を設定することとなった．

2.13 ロードマップ

WG2 の現状と将来について記述した WG2 内の文書である．この 5 年以内の検討項目として，

(1) ディジタル署名規格の再編成

(2) 楕円曲線暗号規格の新パート追加

(3) 暗号メカニズムの強度に関する技術レポート

(4) マルチパーティー計算

などが挙げられている．

また，さらに 5 年先の将来の検討項目として，

(5) 量子暗号

(6) サイドチャネル攻撃への対策

が挙げられている．

WG2 ロードマップのラポータに，櫻井氏(九大)が指名された．

2.14 Identity management/Privacy

Identity Managementの分野では，人や動物やデバイスなどのエンティティを特定する情報やその特定プロセスの安全な管理に関する標準化を目指している．昨年4月のウィーン会合にてA Framework for Identity ManagementがNWI投票にかけることが承認され，投票の結果，プロジェクト (24760)が発足した．マドリッド会合では 2nd 暫定文書の審議が行われ，1st WDに進むことが決まった．

Privacy の分野では，情報システムや通信システムによって操作されるプライバシー情報の管理や保護に関する標準化を目指している．昨年 4 月のウィーン会合にて SC27 とし

ての検討期間設置が承認され，検討が始まった．クアラルンプール会合での審議の結果，プライバシーに関するアドホック検討グループの設置が検討期間の活動の一環として承認された．今回のマドリッド会合での審議の結果，A privacy reference architecture と A privacy Framework の二つのテーマを NWI 投票へかけることが承認された．

3. 新規格

3.1. 新規楕円曲線暗号の標準化

楕円曲線暗号は，近年，双線型写像を利用した新たな技術が数多く提案されており，現状の 15946 では全ての技術を網羅できないのが現状である．このため，楕円曲線暗号の新たな国際規格の必要性が UK からクアラルンプール会議で要求された．前会議では具体的な標準化項目を結論付けることはできなかったが，その必要性については大筋で各国とも合意していた．本会議で必要な技術の明確化，具体的な国際規格の区分けを検討した．

現状の 15946 は4パートからなるが，15946-2， 15946-3，15946-4 はそれぞれ，署名及び鍵共有の改訂版に伴い，14888-3， 11770-3， 9796-3 に吸収される．一方，15946-1 は 14888-3， 11770-3， 9796-3 で必要となる全ての楕円曲線の技術を提供するように改訂中である．このような背景の下，15946 の下に，楕円曲線生成，双線型写像アルゴリズムの 2 規格の追加が UK より提案された．しかし，双線型写像に関しては規格の内容が未成熟なこともあり，次回の南アフリカで再度審議することになり，楕円曲線生成の規格(15946-5)のみ行うことが決まった．また楕円曲線生成の規格に関しては，楕円曲線関連の標準化をすでにこれまで 2 件行っている宮地氏(JAIST)が UK， US などの支持もあり，編集者として申請中である．

4. WG 再編について

4.1 WG 再編会議

参加者は，Walter Fumy 委員長(Siemens AG)，Marijke De Soete 副委員長(Philips Applied Technologies)，Edward J. Humphreys WG1 コンビーナ (XISEC Consultants Ltd.)，苗村憲司 WG2 コンビーナ (情報セキュリティ大学院大学)，Mats Ohlin WG3 コンビーナ (FMV)，及び各国代表者である．

WG 再編の投票結果は賛成多数で新 WG4 と新 WG5 の設置をおこない，SC27 は WG1から WG5 の5つの作業グループで構成されることになる．それぞれの新組織のスコープは以下のようになる．

WG1 の組織名は Information Security Management Systems で，旧 WG1 の 情報セキュリティマネジメント ISMS 27000 シリーズを引継ぐ．

WG2 の組織名は Cryptography and Security Mechanisms で，スコープは旧 WG2 と全く同じである．また，旧 WG2 の 24761 バイオメトリクスのための認証コンテキストと 24745 バイオメトリックテンプレート保護のみが WG5 に移管される．

WG3 の組織名は Security Evaluation and Assessment であり，現在の WG3 のプロジェクトを引き継ぐ．なお，バイオメトリクス関連である WG3 の 19792 バイオメトリクスのセキュリティ評価も WG3 残った．

WG4 の組織名は Security Controls and Services で，旧 WG1 の 27000 シリーズを除く全てのプロジェクト，すなわち，侵入検知，マネッジドセキュリティサービス，ビジネス継続プラン(BCP)/災害復旧サービス(DRS) などが移管される．つまり，ネットワークセキュリティサービス関連を担当する．なお，WG2 の 18014 タイムスタンプは WG4 へ移管する予定であったが，ドイツのコメントに基づいて WG2 に残すことになった．

WG5 の組織名は Identity Management and Privacy Technologies で，バイオメトリクス技術，プライバシー，ID 管理を取り扱う．バイオメトリクス関係のプロジェクトである旧 WG2 の 24761 と 24745 及び新たに需要が見込まれる ID マネジメントやプライバシーといった技術の標準化を取り扱う WG となる．

4.2 新 WG4 と新 WG5 のコンビーナの指名選挙

WG4 は無投票でシンガポールの Meng Chow Kang 氏(シンガポール Microsoft 社)に決まった．しかし，WG5 は，ドイツの Kai Rannenberg 氏(フランクフルト・ゲーテ大学)が立候補していたが，当日になって(WG5 の設置に反対していた)米国の Dick Brackney 氏(NCSC)も立候補し，決選投票になった．各国代表による無記名投票で開票も非公開としたが，結果的に両者の得票差が少ないので，決定は次回の WG 会議行うことになった(両者の得票が接近していたかは，非公開なので不明)．次の WG 会合まで WG5 の臨時のコンビーナをドイツと米国以外から SC27 のセクレタリが暫定的に選ぶことになった．

参考文献

[1]宮地 充子，近澤 武，竜田 敏男，大塚 玲，安田 幹(解説)「情報セキュリティの標準化動向について ー ISO/IEC JTC1/SC27/WG2 2005 年 4 月ウィーン会議報告ー」，電子情報通信学会，信学技報 ISEC 2005-30(2005)，155-164.

謝辞

日本の情報セキュリティ技術の国際標準化活動にあたり，苗村 WG2 コンビーナ，宝木 SC27 国内委員会委員長には，常日頃よりご指導頂いている．また，本報告書を作成するに当たり，櫻井 WG2 国内委員会主査，中尾 WG1 国内委員会主査，三村 SC27/WG3 オブザーバ，WG2 国内委員会各委員によりご助言を頂いた．社団法人情報処理学会・情報規格調査会の加藤氏，成田氏には，国際・国内標準化活動において常日頃よりサポートして頂いている．ここに感謝の意を表したい．

表1 SC27/WG2 マドリッド会議結果一覧 (2006-05-08/12) ※SC27 Plenary (2006-05-16/17)の結果を反映

規格番号	規格名 会議前ステータス	日本の投票/コメント/寄書	会議後ステータス	備考
7064	検査文字システム (Check character systems)			
	定期見直し	継続使用を提案	継続使用	ISO/IEC 7064:2003-02-01 (2nd edition) を継続使用.
9796	メッセージ復元型ディジタル署名 (Digital signature schemes giving message recovery)			
9796-2	第2部: 因数分解に基づく機構 (Part 2: Integer factorization based mechanisms)			
	追補 1st WD	コメントなし	PDAM	ISO/IEC 9796-2:2002-10-01 (2nd edition) を点検し, OIDとASN.1を追加する追補を作成中.
9796-3	第3部: 離散対数に基づく機構 (Part 3: Discrete logarithm based mechanisms)			
	FDIS 用テキスト作成	-	FDIS 投票	ISO/IEC 9796-3:2000-04-15 (1st edition) を改訂中. 宮地 充子 氏が編集者.
9797	メッセージ認証符号 (Message authentication codes)			
9797-1	第1部: ブロック暗号を用いる機構- (Part 1: Mechanisms using a block cipher)			
	1st CD	テキスト未着	1st CD 投票	ISO/IEC 9797-1:1999-12-15 (1st edition) を改訂中. OMACと CMACを追加することを決定.
9797-2	第2部: 専用ハッシュ関数を用いる機構 (Part 2: Mechanisms using a dedicated hash-function)			
	1st WD	テキスト未着	1st WD	ISO/IEC 9797-2:2002-06-01 (1st edition) を改訂中. Bart Preneel 氏は長いハッシュ値の関数の導入には否定的.
9797-3	第3部: 万能ハッシュ関数を用いる機構 (Part 3: Mechanisms using a universal hash-function)			
	1st WD	テキスト未着	1st WD	第2部を分割し, AESなどをハッシュ関数とする新提案.
9798	エンティティ認証 (Entity authentication)			
9798-1	第1部: 総論 (Part 1: General)			
	-	-	-	ISO/IEC 9798-1:1997-08-01 (2nd edition) を使用中.
9798-2	第2部: 対称暗号アルゴリズムを用いる機構(Part 2: Mechanisms using symmetric encipherment algorithms)			
	編集者募集	-	追補の 1st WD	ISO/IEC 9798-2:1999-07-15 (2nd edition) の追補を作成する. Hans von Sommerfeld 氏が編集者に就任.
	編集者募集	-	改訂版の 1st WD	ISO/IEC 9798-2:1999-07-15 (2nd edition) を全面改訂. 竜田 敏男 氏の編集者の承認を申請中.
9798-3	第3部: ディジタル署名技術を用いる機構 (Part 3: Mechanisms using digital signature techniques)			
	-	-	-	ISO/IEC 9798-3:1998-10-15 (2nd edition) を使用中.
9798-4	第4部: 暗号検査関数を用いる機構 (Part 4: Mechanisms using cryptographic check function)			
	定期見直し	コメントなし	継続使用	ISO/IEC 9798-4:1999-12-15 (2nd edition) を継続使用.
9798-5	第5部: ゼロ知識技術を用いる機構 (Part 5: Mechanisms using zero knowledge techniques)			
	-	-	-	ISO/IEC 9798-5:2004-12-01 (2nd edition) を使用中.
9798-6	第6部: 手動データ移動を用いる機構 (Part 6: Mechanisms using manual data transfer)			
	IS 出版	-	-	ISO/IEC 9798-6:2005-08-01 (1st edition) を使用中.
9979	暗号アルゴリズムの登録手続 (Procedures for registration of cryptographic algorithms)			
	廃止	-	-	ISO/IEC 9979:1999-04-01 (2nd edition) を廃止.
10116	nビットブロック暗号の利用モード (Modes of operation for an n-bit block cipher algorithm)			
	IS 出版	-	-	ISO/IEC 10116:2006-02-01 (3rd edition) を使用中.
10118	ハッシュ関数(Hash-functions)			
10118-1	第1部: 総論 (Part 1: General)			
	定期見直し	コメントなし	継続使用	ISO/IEC 10118-1:2000-06-15 (2nd edition) を継続使用.
10118-2	第2部: nビットブロック暗号を用いるハッシュ関数 (Part 2: Hash-functions using n-bit block cipher algorithm)			
	定期見直し	コメントなし	訂正を発行	ISO/IEC 10118-2:2000-12-15 (2nd edition) の訂正(COR1)の作成. 編集者は Debby Walner 氏が就任.
	定期見直し	コメントなし	全面改訂 編集者募集	ISO/IEC 10118-2:2000-12-15 (2nd edition) の改訂版を作成する.
10118-3	第3部: 専用ハッシュ関数 (Part 3: Dedicated Hash-functions)			
	追補発行	-	-	ISO/IEC 10118-3:2004-03-01 (3rd edition) の追補 Amendment 1: 2006-02-15 を発行した. "SHA-1"に関する SC27 の意見表明の改訂版を出す.
10118-4	第4部: 剰余演算を用いるハッシュ関数 (Part 4: Hash-functions using modular arithmetic)			

	編集者募集	応募せず 寄書なし	改訂中止 継続使用	編集者募集に応募者なし. ISO/IEC 10118-4:1998-12-15 (1st edition) の改訂を中止.
11770	かぎ管理 (Key management)			
11770-1	第 1 部: 枠組み (Part 1: Framework)			
	-	-	-	ISO/IEC 11770-1:1996-12-15 (1st edition) を使用中.
11770-2	第 2 部: 対称暗号技術を用いるかぎ確立機構 (Part 2: Mechanisms using symmetric techniques)			
	訂正文発行	-	-	ISO/IEC 11770-2:1996-04-15 (1st edition) の 訂正文書 Technical Corrigendum 1: 2005-07-15 を発行した.
	改訂開始	寄書なし	1st WD	ISO/IEC 11770-2:1996-04-15 (1st edition) の全面改訂を開始. 編集者に Chris Mitchell 氏が就任.
11770-3	第 3 部: 非対称暗号技術を用いるかぎ確立機構 (Part 3: Mechanisms using asymmetric techniques)			
	1st WD	コメントあり	1st CD	ISO/IEC 11770-3:1999-11-01 (1st edition) の改訂作業を開始. 改訂版には bilinear pairing を組み込む. 編集者は Chris Mitchell 氏が就任.
11770-4	第 4 部: 弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
	IS 発行-	-	-	ISO/IEC 11770-4:2006-05-01 (1st edition) を発行.
13888	否認防止 (Non-repudiation)			
13888-1	第 1 部: 総論 (Part 1: General)			
				ISO/IEC 13888-1:2004-06-01 (2nd edition) を使用中.
13888-2	第 2 部: 対称暗号技術を用いる機構 (Part 2: Mechanisms using symmetric techniques)			
	定期見直し	コメントなし	寄書募集 編集者募集	ISO/IEC 13888-2:1998-04-01 (1st edition) の改訂作業を開始.
13888-3	第 3 部: 非対称暗号技術を用いる機構 (Part 3: Mechanisms using asymmetric techniques)			
	定期見直し	コメントなし	寄書募集 編集者募集	ISO/IEC 13888-3:1997-12-01 (1st edition) の改訂作業を開始. 渡辺 創 氏の編集者の承認を申請中.
14888	添付型ディジタル署名 (Digital signatures with appendix)			
14888-1	第 1 部: 総論 (Part 1: General)			
	FCD 投票中	コメントなし 賛成	FCD 投票中	ISO/IEC 14888-1:1999-12-15 (corrected) を改訂中. 大塚 玲 氏が編集者.
14888-2	第 2 部: 因数分解に基づく機構 (Part 2: Integer factorization based mechanisms)			
	1st FCD	コメントあり 賛成	2nd FCD	ISO/IEC 14888-2:1999-12-15 (1st edition) を改訂中.
14888-3	第 3 部: 離散対数に基づく機構 (Part 3: Discrete logarithm based mechanisms)			
	FDIS 投票中	-	FDIS 投票中	ISO/IEC 14888-3:2001-09-15 (corrected) を改訂中.
15946	楕円曲線に基づく暗号技術 (Cryptographic techniques based on elliptic curves)			
15946-1	第 1 部: 総論 (Part 1: General)			
	1st CD	コメントなし 賛成	2nd CD	ISO/IEC 15946-1:2002-12-01 (1st edition) を改訂中. 宮地 充子 氏が編集者.
15946-2	第 2 部: ディジタル署名 (Part 2: Digital signatures)			
	-	-	-	ISO/IEC 15946-2:2002-12-01 (1st edition) を使用中.
15946-3	第 3 部: かぎ確立 (Part 3: Key establishment)			
	-	-	-	ISO/IEC 15946-3:2002-12-01 (1st edition) を使用中
15946-4	第 4 部: メッセージ復元型ディジタル署名 (Part 4: Digital signatures giving message recovery)			
	-	-	-	ISO/IEC 15946-4:2004-10-01 (1st edition) を使用中.
15946-5	第 5 部: 楕円曲線生成 (Part 5: Elliptic curve generation)			
	寄書募集	-	-	宮地 充子 氏の編集者の承認を申請中.
18014	タイム スタンプ サービス (Time stamping services)			
18014-1	第 1 部: 枠組み (Part 1: Framework)			
	1st CD 投票中	コメントなし 賛成	2nd CD	ISO/IEC 18014-1:2002-10-01 (1st edition) を改訂中. 空本 忠昭 氏が編集者.
18014-2	第 2 部: 独立トークンを生成する機構 (Part 2: Mechanisms producing independent tokens)			
	2nd WD	コメントあり	3rd WD	ISO/IEC 18014-2:2002-12-15 (1st Edition) を改訂中. スペインの J. Mañas 氏が編集者.
18014-3	第 3 部: リンク付きトークンを生成する機構 (Part 3: Mechanisms producing linked tokens)			
	-	-	-	ISO/IEC 18014-3:2004-02-15 (1st edition) を使用中.
18031	乱数生成 (Random bit generation)			
	IS 出版	-	-	SO/IEC 18031:2005-11-15 (1st edition) を使用中.

18032	素数生成 (Prime number generation)			
	-	-	-	ISO/IEC 18032:2005-01-15 (1st edition) を使用中.
18033	暗号アルゴリズム (Encryption algorithms)			
18033-1	第 1 部: 総論 (Part 1: General)			
	-	-	-	ISO/I EC 18033-1:2005-02-01 (1st edition) を使用中.
18033-2	第 2 部: 非対称暗号 (Part 2: Asymmetric ciphers)			
	IS 出版	-	-	ISO/I EC 18033-2:2006-05-01 (1st edition) を発行.
18033-3	第 3 部: ブロック暗号 (Part 3: Block ciphers)			
	IS 出版	-	-	ISO/I EC 18033-3:2005-07-01 (1st edition) を使用中.
	DCOR1	コメントなし 賛成	出版待ち	ISO/I EC 18033-3:2005-07-01 (1st edition) の追補を作成中.
18033-4	第 4 部: ストリーム暗号 (Part 4: Stream ciphers)			
	IS 出版	-	-	ISO/IEC 18033-4:2005-07-15 (1st edition) を使用中.
	追加の暗号 募集	追加暗号なし コメントあり	1st WD of Amendment 1	追加すべき暗号があれば追補を作成する. 編集者は Erik Zenner.
19772	データ カプセル化機構 (Data encapsulation mechanisms) → 認証付き暗号化 (Authenticated encryption)			
	1st CD	コメントあり 反対	2nd CD	初版作成中. タイトルを変更.
24745	バイオメトリックテンプレート 保護 (Biometric Template Protection)			
	2nd WD	コメントあり 寄書あり	3rd WD	韓国の Park 氏が編集者を辞任. 編集者募集と寄書募集.
24761	バイオメトリクスのための認証コンテキスト (Authentication Context for Biometrics)			
	2nd WD	コメントなし	1st CD	才所 敏明 氏が編集者.
Study Period	検討期間(Study Period): Digital signature generation using biometric technology			
	寄書募集 編集者募集	寄書なし 応募せず	中止	韓国の提案者が編集者を辞任したので寄付書と編集者を募集. どちらも応募が無かったので検討を中止.
Study Period	検討期間(Study Period): 低電力暗号 (Low Power Encryption)			
	-	-	-	JTC1 からの検討依頼
WG2 検討期間	WG2 ロードマップ (WG2 Road Map)			
	-	-	-	SC27/WG2 の委員長により適時に改訂される. 櫻井 幸一 氏をラポータに指名.