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

2007－ＣＳＥＣ－38 (24)
2007／7／19

情報セキュリティの標準化動向について
－ISO/IEC JTC1/SC27/WG2 2007年5月ロシア会議報告－

宮地 充子[I] 近澤 武[II] 竜田 敏男[III] 渡辺 創[IV] 大熊 建司[V]

[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]独立行政法人産業技術総合研究所 〒101-0021 東京都千代田区外神田 1-18-13-1102
[V]株式会社東芝／情報処理推進機構 〒212-8582 神奈川県川崎市幸区小向東芝町 1

E-mail: [I]miyaji@jaist.ac.jp [II]Chikazawa.Takeshi@bk.MitsubishiElectric.co.jp
[III]tatsuta@iisec.ac.jp [IV]h-watanabe@aist.go.jp [V]kenji.ohkuma@toshiba.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[1]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月に行われたロシア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，ロシア会議

On the Standardization of Information Security
－Report on the Russia Meeting in May, 2007－

Atsuko MIYAJI[I] Takeshi CHIKAZAWA[II] Toshio TATSUTA[III]
Hajime WATANABE[IV] Kenji OHKUMA[V]

[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, Yokohama, Kanagawa, 211-0835 Japan
[IV]AIST 1-18-13-1102 Sotokanda, Chiyoda, Tokyo, 101-0021 Japan
[V]Toshiba Corporation/IPA 1 Komukai Toshiba-cho, Saiwai-ku, Kawasaki, Kanagawa, 212-8582 Japan

E-mail: [I]miyaji@jaist.ac.jp [II]Chikazawa.Takeshi@bk.MitsubishiElectric.co.jp
[III]tatsuta@iisec.ac.jp [IV]h-watanabe@aist.go.jp [V]kenji.ohkuma@toshiba.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 Russia in May, 2007.

Keyword ISO, IEC, Information Security, Russia 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，本会議よりWG1，WG3，WG4，WG5の合計5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 ISMS 27000 などがその代表例である．

[1] 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．

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．19792 バイオメトリクスのセキュリティ評価も WG3 の担当となる．WG4 は侵入検知，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) などの国際規格の策定を担当する．WG5 はバイオメトリクス技術，プライバシー，ID 管理の国際規格の策定を担当する．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も WG5 の担当になる．

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からWG5の5つの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．2006 年は 5 月にマドリッド会議，11 月に南アフリカ会議を行った．本報告書は，昨年のマドリッド会議の報告[2]に続き，2007 年 5 月に行われたロシア会議の速報と現在 WG2 で策定中の国際規格について解説する．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 4 日(金)～8 日(火)
場所:モスクワ(ロシア)
WG2 の参加国(人数):ロシア(3)，オーストリア(1)，中国(2)，デンマーク(1)，独(2)，日本(9)，韓(2)，南アフリカ(1)，英(2)，米(1)
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(IPA，WG 国際幹事)，大熊(IPA)，櫻井(九州大)，市川(アマノ)，竜田(IISEC)，渡辺 (産総研)，田中，清本(KDDI)，宮崎(日立)，宮地 (JAIST)

なお，WG1～5 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た．

本会議でも前回報告のマドリッド会議に引き続き，日本人の参加人数が目立つが，マドリッド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素案に関する会議報告を記述する．

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となる．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．9796-2 は 2002 年に継続使用が認められ，9796-3 は 2003 年より改訂が進められた．

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 に楕円曲線暗号のメッセージ復元型署名の規格 IS15946-4 を包含する目的で 2003 年より改訂が始まった．ECNR (フィンランド)，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が務め，2006 年に IS として発行された．

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)

編集者の Bart Preneel 氏と共同編集者の Chris Mitchell 氏がともに欠席したため，1st CD に対する投票結果やコメントについての議論が行えなかった．会議では，両編集者に対して次回会議までに 2nd CD 投票が行えるように，2nd CD 文書の早急な作成を要請することが合意された．

2.2.2 第 2 部 専用ハッシュ関数を用いる機構 (9797-2)

編集者の Bart Preneel 氏が欠席しており，またロシア会議までに提出が期待されていた WD テキストが会議までに提出されなかった．会議では，編集者の Bart Preneel 氏と共同編集者の Liqun Chen 氏に対して，次回会議で CD へ進められるように，早急な WD 文書の作成と各国からのコメント収集を要請することが合意された．

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)

編集者の Bart Preneel 氏が欠席したが，共同編集者の Erik Zenner 氏が WD の準備稿として提出したテキストに対する各国から寄せられたコメントについて，同氏を中心に会議を行った．提出テキストが正式なものではなく準備稿で

あったため，議論自体は非公式なものとなった．次回会議でCDへ進められるように，編集者に対して早急なWDテキストの作成と各国からのコメント収集を要請することが合意された．

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た．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．また，旧規格にはASN.1によるOID規定がないという問題があったので，(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．2006年5月のマドリッド会合でHans von Sommerfeld氏を追補の編集者に，竜田氏を改訂作業の編集者に指名した．今回のロシア会合では，追補の1st WDと，改訂の2nd WDが審議された．その結果，追補についてはASN.1の記述についてコメントが無かったので完成したものとみなし，改訂作業に移管することになった．改訂作業はコメントに対する対処案を審議した結果，1st CDに進むことが決まった．

2.3.2 第5部 ゼロ知識技術を用いる機構

9798-5は本会議が見直しの時期に相当し，フランスのみが改定を提案した．改定理由は，近年どの暗号プロトコルも楕円曲線暗号が利用されるにも関わらず，現規格では楕円曲線暗号がサポートされていない．フランスの改定の理由はその点を改善し，楕円曲線暗号を利用できるように拡張するというものである．各国から反対意見はなく，改定を行うことが決定した．

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．ロシア会議では，改訂作業に入る予定の第2部と，今回定期見直しである第3部について審議が行なわれた．

2.4.1. 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，4つの方式が掲載されている．定期見直しの時期であり，前々回南アフリカ会議後，コメント及び編集者の募集が行なわれていた．

ロシア会議では唯一日本から出されていた新規方式の追加提案について審議した．新規方式は廣瀬准教授(福井大)が設計・評価したもので，内部変数のサイズがブロック幅の2倍の2nビットであり，安全性に関する証明がついている．既に規格に含まれている4つの方式で性能・安全性のバランスが最も良いHash-function 2と比較したとき，性能ではやや劣るものの，より安全であり，日本として追加が妥当であると主張した．この提案に対し，新規方式は2006年のFSE 2006で始めて発表されたものであり，まだ未成熟だとする意見や，NISTによるハッシュ関数の公募に提案してはどうかという意見が出された．また，この方式は既に前々回の南アフリカ会議でフランスが追加を提案していた2方式の1つであることが明らかになった．審議の結果，今回は参加国が少ないので日本及びフランス提案の議論は行わず，コメント募集を行い，その結果を受けて改訂作業を進めることが決まった．

また，編集者募集に対し，日本から編集者に吉田委員，共同編集者に近澤幹事(国際幹事兼任)を推薦し，合意された．

2.4.2. 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つのアルゴリズムを掲載して2004年に改訂され，その後，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2006年に発行されている．

ロシア会議では，定期見直しの準備段階として募集されていたコメント結果について審議を行った．コメントは5カ国から提出され，いずれもSHA-1の安全性低下に注目するものだった．米国，スウェーデン，ルクセンブルクが改訂を主張し，日本と英国はSHA-1が広く使用されているので一旦継続使用(confirmation)とし，SHA-1の削除は必要に応じて実施すべしとの意見だった．議論の結果，臨時rapporteurを務めた英国のLiqun Chen氏の主張が通り，SHA-1削除の改訂は時期尚早なので当規格は継続使用とし，SHA-1の安全性の欠陥が深刻になった時点で迅速に対応することが承認された．

また，今回は欠席だったが，米国のDebby Wallner氏より提出されていたSHA-1に対するrapporteur reportの改訂について審議した．改訂の内容は，NISTが予定している次世代ハッシュ関数の公募プロジェクト(AHS)の情報を追加することであり，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．

2.5 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. 編集者の Chris Mitchell 氏が欠席であったが, 事前に各国コメントに対する修正案を用意し, 臨時編集者が議事を進行した. 日本は唯一反対票を投じていたが, ほぼ日本のコメントが受け入れられたため, 賛成にまわった. 他国からのコメントも処理し, FCD に進むことになった.

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. 日本と米国は反対投票を行ったが, 日本および米国のコメントはすべて受け入れられたため, それぞれ賛成にまわった. 他国のコメントも処理したが, 編集者の Savard 氏が欠席したこともあり, 本会合の結論を反映させた修正ドラフトを作成し, 再度 FCD 投票を行うことになった.

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.

第 2 部と第 3 部は現在改訂作業中であり, 第 1 部について, 今回定期見直し時期にきたため, 改訂作業に入るかどうかの議論が行われた.

2.6.1. 第 1 部 総論 (IS 13888-1)

今回定期見直し時期に来たため, ロシア会議までに各国からの見直しに対しての意見が集められていた. その結果, 米国とルクセンブルクから改訂案が提出された. 議論の結果, 現在改訂中の第 2 部との不整合が存在するので, 改訂を開始することが合意された.

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

第 2 部は前回の南アフリカ会議で定期的な見直し時期に来たため, 改訂についての議論が行われ, 改訂を行うことが決定された. 今回ロシア会議では, それまでに編集者から提出されていた 1st WD ドキュメントと, それに対する各国からのコメントについて議論が行われた. その結果, 修正すべき点が多いこともあり, 2nd WD ドキュメントを作成することが合意された.

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

前回の南アフリカの会議後に提出された 1st CD ドキュメントに対し, CD 投票が行われた. 投票の結果, フランスのみが反対投票を投じていたが, ロシア会議には誰も出席しなかったため, 今回はフランスからのコメントを含む, 各国からのコメントに対する対応についての議論が行われた. 次回までに 2nd CD ドキュメントを提出し, それに対する CD 投票を再度行うことが合意された.

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 (総論)の規格 (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, 大塚氏が編集者を担当している. 前回の南アフリカ会議で FDIS に進むことが決定しており, 現在, 編集者からの FDIS ドラフトの提出を待っている状態である.

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. Louis Guillou 氏が編集者を務める. 前回の南アフリカ会議で FDIS に進むことが決定し, FDIS ドラフトが ISO 中央事務局[2]より回覧されるのを待っている状態である.

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 Joong Lee 氏が編集者を務める. 2006 年に IS として発行された.

[2] ISO 中央事務局の ITTF(Information Technology Task Force)が行う.

本会議において，ロシアより Elliptic curve Russian Digital Signature Algorithm の追加の提案が行われた．ロシアの方式は，いわゆる ECDSA 署名の変形であり，すでにロシア国内で標準方式として利用されている．今後，ロシアよりすでに規格化されている既存方式との違いなどを記載した Amendment(追補)を作成することになった．

[*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．本会議では，IS14888-3，IS9796-3の発行に伴い，2，4部の廃止の手続きを承認した．3部に関しては継続使用である．本会議では，改訂中の第1部及び新規格である第5部に関する報告を行う．

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，2005 年 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，韓国，ドイツ，ポーランド，日本などからコメント寄与があった．FCD 投票の結果，反対票がなく，本会議において FDIS 投票に進むことが決定した．

2.8.2. 第 5 部 楕円曲線生成 (15946-5)

15946-5 は楕円曲線に基づく暗号技術の実現に必要になる楕円曲線のパラメータの生成手法の規格で，2006 年 11 月の南アフリカ会議から審議が始まった．楕円曲線に基づく暗号技術には大きく分けて 2 つ存在する．1 つは 1986 年に Koblitz と Miller により提案された楕円曲線上の離散対数問題に基づく暗号方式であり，もう一つは 2001 年に Boneh と Franklin により提案された楕円曲線上の双線型写像を利用する暗号方式である．本規格では，両方の楕円曲線暗号に利用される楕円曲線に対する生成法を与える．付録として，楕円曲線の例も記載されている．

本規格には，UK，韓国，ドイツ，オランダなどからコメント寄与があった．大きな問題はなく，本会議において 1st CD 投票に進むことが決定した．

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，及び本会議で見直しを行った第 3 部の報告を行う．

2.9.1 第 1 部 枠組み (18014-1)

18014-1 はタイムスタンプサービスの実現に必要になる枠組みに関する規格で，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，タイムスタンプサービスの ASN.1 module も記載されている．

本規格には，US，フランスからコメント寄与があった．FCD 投票の結果，US のみが反対票であった．しかし，US の反対票は，記号の統一性の問題だけであり，本会議中に解決策を見出し，FDIS 投票に進むことが決定した．

2.9.2 第 2 部 独立トークンを生成する機構 (18014-2)

18014-2 は編集者が欠席したため，実質的な議論がされなかった．このため，2nd CD テキストを作成して再審議することが決定した．

2.9.3 第 3 部リンク付きトークンを生成する機構 (18014-3)

18014-3 は本会議が見直しの時期に相当し，US のみが改定を提案した．リンクトークン方式のタイムスタンプでは，予め定義した期間単位で各トークンのハッシュ値をツリー状にハッシュ生成しその最上位のハッシュ値(スーパーハッシュ値と呼ばれる)を公開しての信頼性の拠り所にするが，現規格ではタイムスタンプサービスの通信プロトコル上でのスーパーハッシュ値の取り扱いが定められてない．US の提案はその点の改善し，スーパーハッシュ値に関する情報(ロケーションなど)を含んだタイムスタンプトークンを利用することできるように拡張するというものである．各国から反対意見はなく，改定を行うことが決定した．

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．第 2 部(非対称暗号)は 2006 年 5 月に出版されている．

2.10.1 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，SEED の図が正しくなかったため，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．

一方，前回，TC68/SC2 から，規格の脚注にある，2-key

Triple DES の安全性への NIST 方針に関する記述「2009 年までしか NIST は保証しない」を見直すことが要求され，検討の結果，見直しの必要はないと回答した．これに対し，今回，再度の要請があったので，本会合で検討した結果，何らかの見直しをする方向で議論が進み，NIST について触れた箇所を削除することを支持する発言が欧州を中心に複数あったので，問題の記述を削除するための訂正文書を作成することになった．なお，削除される記述を含め，暗号アルゴリズムと鍵長に関する文書を Standing Document としてまとめることとなった．

2.10.2 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 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．なお，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ている．編集者は Erik Zenner 氏．フランスよりストリーム暗号 DECIM v2，韓国よりストリーム暗号 TSC-4 が提案されており，現在のドラフト文書では，この 3 つのアルゴリズムが掲載されている．本会合では，日本の KDDI より KCipher-2 が新たに提案され，eStream のフェーズ 2 の結果も出たことから，作業の進め方も含めて議論となった．結局，KCipher-2 を含めた 4 つのアルゴリズムについて各国にコメントを求めることとし，文書の更新は行わないことになった(WD のまま)．

2.11 認証付き暗号化(19772)

19772 は対称暗号技術を用いて秘匿と認証を一体で行う認証付き暗号アルゴリズムの国際規格である．小部はない．2005 年春の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．ロシア会議前の時点では，OCB 2.0， Key Wrap， CCM， EAX， Encrypt-then-MAC の 5 つのメカニズムが掲載されていた．

ロシア会議では，米国から，新規のメカニズム the Galois Counter Mode (GCM) 追加の提案があった．GCM はカウンタモード(CTR)の並列性とガロア体上の積算の高速性を活かした認証子の生成方式であり，通常の連鎖モードより高いスループットが期待できる．IEEE や NIST の規格にも取り入れられており，関連特許がないことも利点である．審議の結果，GCM を追加することで合意された．

現在 2nd CD であるが，新規メカニズムの追加という大きな変更があったので，FCD には進まず，3rd CD に留まることになった．

3. 国際規格検討期間中の項目

3.1 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．ラポータは櫻井氏(九大)．前々回以降，ロードマップ文書は更新されていない．更新前の内容は以下の通り．

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．

なお，次回会合までにロードマップ文書の更新が予定されており，超楕円曲線暗号や著作権の鍵管理などの項目が標準化項目候補として追加される予定である．

3.2 低電力暗号

低電力暗号は Low Power Encryption の訳である．SC27 の上部組織 JTC1 より低電力暗号の検討指示があり，06 年ウィーン会議より国際規格検討期間が始まった．ラポータは櫻井氏(九大)．前回会合で日本より提出した低電力暗号に関する概略的な寄書をベースに，具体的な暗号アルゴリズムの紹介を含む，ラポータ文書が作成され，本会合で議論を行った．

この文書は新規の暗号アルゴリズムしか取り上げていないが，既存の暗号アルゴリズムにも低電力用の特徴があるものもあるのでは，という意見も出されたため，各国にこの点について寄書を求めることとなった．

3.3 暗号プロトコルの安全性証明

暗号プロトコルの安全性証明は Formal proof and verification of the security of cryptographic mechanisms の訳である．以前より WG3 では，暗号技術，暗号プロトコルの形式的な安全性証明技術の規格化に関して，その可能性が検討されていた．規格化においては，暗号技術の安全性に関する技術的な検討が必要なこともあり，WG3より WG2 に対して，国際規格化への検討が依頼されていた．ロシア会議では，前回南アフリカ会議で募集され，それまでに提出された規格化に向けた意見を述べた寄書について審議が行われた．提出された寄書は，日本からのもの(セキュリティプロトコルの評価基準に関する提案)のみであった．

議論では，まず宮崎氏(日立)から提案内容が説明され，それに対して各国からさまざまな意見が出された．

- 具体的な評価メカニズムの規格化は WG2 の対象であるが，「評価基準」となると WG3 の対象ではないか(UK，デンマーク，南アフリカなど)？
- プロトコル評価は，ある一つまたは複数の，万能なメカニズムで評価できる状況にない．将来的にもそれは難しいと思われる．しかし一定の判断基準は必要かつ有用だと考える．専門知識が欠かせないので，WG2 での

議論が必須である.

- 内容自体は WG2 にとって有用である. Technical Report や, WG2 の内部文書として活用できるだろう (UK).

結論として, WG3 で同内容と議論の結果を報告して, 対応を WG3 と相談することになった.

WG3 で宮崎氏が同様の内容を発表し議論した結果, WG3 から NWI(新作業項目)として提案(暗号プロトコルの検証:Verification of Cryptographic Protocols)することになった. 宮崎氏が当面の編集者に指名された. 今後は WG3 において, NWI とするかどうか投票が行われ, 認められれば WD ドキュメントの作成へと進むことになる.

WG2 では規格化に向けた議論は今回で終了となるが, 引き続き同技術の規格化に WG3 に協力していくこととなった

3.4 署名付き暗号

署名付き暗号は Signcryption の訳である. ロシア会議までにコメントが求められ, UK からのみコメントが寄せられた. 本会議では同コメントが紹介され, それをもとに活発に議論が行われた.

この技術は暗号化と署名を効率よく行うものであり, やっていることは IS 19772 (authenticated encryption) と関連がある. 現状 IS 19772 は対称鍵暗号をベースとした技術のみが規格化されているが, これはその非対称鍵暗号をベースとした技術としても位置づけることが可能である. したがって IS 19772 を再構成し, その新たな1部として規格化する可能性もあり得る. といった意見が出された.

議論の結果, 署名付き暗号技術の規格化作業を開始することが決まった. しかしながら, 同技術をどのような位置づけとして規格化するのか, また具体的な候補技術としてどのようなものが存在するのか, まだ未確定部分や情報が少ない部分が残っているため, それらを含めたコメント募集を行うことになった.

3.5 ディジタル署名の規格の統合

SC27 には 9796 と 14888 の 2 種類のディジタル署名の規格がある. 9796 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メッセージ復元型署名の規格であり, 14888 は署名の中にメッセージは含まれず, 署名にメッセージそのものを添付させる添付型署名の規格である. 因数分解に基づく署名方式では, 両者の区分けが曖昧なため, ディジタル署名を一つの国際規格として改定しようというフランスの Louis Guillou 氏の提案であり, 彼がラポータを務める. しかし, 本会議ではラポータが欠席し, UK から統合に関する反対のコメントが報告されただけである.

4. 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 を設置し, 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, JTC1/SC17, ISO/TC68, ITU-T/SG17 など)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きた. その後, Ad Hoc Group は Advisory Group と改称されたが, ISO の各国際規格と関連する他標準化組織との関係が確立し, 今回のロシア会議で Advisory Group は役目を終え, 廃止された.

なお, SC27/WG5 の設立に伴い, 本標準化は SC27/WG2 より SC27/WG5 へ移管された.

4.1 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(マスターデータ)の保護に関する標準化である.

2005 年 4 月のウィーン会合で韓国から寄書が提出され, 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た. その結果, 2006 年 5 月のマドリッド会合で Park 氏が編集者を降り, 編集者を再募集して暗号技術を基に標準化作業を進めることになった. 2006 年 11 月のヨハネスブルグ会議で韓国の Myung Geun Chun 氏と Pil Joong Lee 氏が編集者に指名された. しかし, 今回のロシア会議には両編集者は参加せず, バイオ技術に基づくものでなければ編集者を降りたいという書簡を送ってきた. その取扱いを SC27 で協議した結果, 本来の依頼人である SC37 の委員長と SC27 の委員長とで協議することになった.

4.2 バイオメトリクスのための認証コンテキスト (24761)

バイオメトリクスによる認証プロセスで使用されるテンプレート, デバイス, 判定プログラムなどの安全性・機能・性能及び認証結果の妥当性検証に関わる情報項目とその通知方法に関する標準化の提案である.

2006 年 5 月のマドリッド会合では, 2nd WD 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. その後, SC37 や TC68/SC2 の他に, SC17(ID カード)や ITU-T とも調整作業を進めいている. 投票結果は賛成多数であったが, IC カード実装に関する情報を追加するために, 今回のロシア会議では 3rdCD に留まることを決定した.

4.3 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 にあったバイオメトリクス関連の標準化(現在は新設の WG5 に移管)と関係が深かったため，継続して報告する．

この標準案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．この標準化作業は WG3 において進められており，Nils Tekampe(独)，三村氏が共同編集者として参画している．

2006 年 5 月の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．その後，BEM に関する標準化を支持する意見が得られず，BEM 部分は廃案となった．今回のロシア会合では，BEM を除く本体部分の標準案に対する重大なコメントもなく，Final CD へ進むことになった．

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 －ISO/IEC JTC1/SC27/WG2 2005 年 4 月ウィーン会議報告－」，電子情報通信学会，信学技報 ISEC 2005-30(2005)，155-164．

[2] 宮地充子，近澤武，竜田敏男，大塚玲，安田幹，森健吾，才所敏明(解説)「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」，電子情報通信学会，信学技報 ISEC 2006-40-71(2006)，43-52

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，山田 WG5 国内委員，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，木村氏には，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 ロシア会議結果一覧 (2007-05-04/10) ※SC27 Plenary (2007-05-12)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 コメント審議	会議後ステータス	備考
7064	検査文字システム (Check character systems)			
	-	-	-	ISO/IEC 7064:2003-02-15 (1st edition) を使用中.
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 FPDAM	賛成	FDAM	ISO/IEC 9796-2:2002-10-01 (2nd edition) の 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)			
	IS 出版	-	-	ISO/IEC 9796-3:2006-09-15 (2nd edition) を使用中.
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	コメント付反対	2nd CD 投票	ISO/IEC 9797-1:1999-12-15 (1st edition) を改訂中. 編集者は Bart Preneel 氏，共同編集者は Chris Mitchell 氏 OMAC1 と CMAC が記載されている.
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. 編集者は Bart Preneel 氏，共同編集者は Liqun Chen 氏
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	AES などを利用してハッシュ関数を構成する新提案. 編集者は Bart Preneel 氏，共同編集者は Erik Zenner 氏
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)			

	追補の 1st WD	-	改版に統合	ISO/IEC 9798-2:1999-07-15 (2nd edition) の OID と ASN.1 を 追加する追補を作成中.
	2nd WD	-	追補を含めて 1st CD	ISO/IEC 9798-2:1999-07-15 (2nd edition) を全面改訂. 竜田 敏男 氏が編集者.
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)			
	-	-	-	ISO/IEC 9798-4:1999-12-15 (2nd edition) を使用中.
9798-5	第 5 部: ゼロ知識技術を用いる機構 (Part 5: Mechanisms using zero knowledge techniques)			
	定期見直し	コメントなし	全面改訂 編集者募集	ISO/IEC 9798-5:2004-12-01 (2nd edition) の改訂版を作成する.
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.
	訂正文 1st DCOR1	条件付反対	2nd DCOR1	ISO/IEC 10116:2006-02-01 (3rd edition) の訂正文書 Technical Corrigendum 1 を作成中.
10118	ハッシュ関数(Hash-functions)			
10118-1	第 1 部: 総論 (Part 1: General)			
	-	-	-	ISO/IEC 10118-1:2000-06-15 (2nd edition) を使用中.
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)			
	訂正文書 発行	-	-	ISO/IEC 10118-2:2000-12-15 (2nd edition), COR1:2006-10-01 及び COR2:2007-02-15 を使用中.
	寄書募集 編集者募集	寄書提出 編集者応募	1st WD	ISO/IEC 10118-2:2000-12-15 (2nd edition) の改訂版を作成中. 編集者は吉田氏, 共同編集者は近澤氏
10118-3	第 3 部: 専用ハッシュ関数 (Part 3: Dedicated Hash-functions)			
	定期見直し	継続使用 コメントあり	-	ISO/IEC 10118-3:2004-03-01 (3rd edition) 及び Amendment 1: 2006-02-15 を使用中. "SHA-1"に関する SC27 の意見表明の改訂版を発行.
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)			
	-	-	-	ISO/IEC 10118-4:1998-12-15 (1st edition) を使用中.
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)			
	1st CD	反対	Final CD	ISO/IEC 11770-2:1996-04-15 (1st edition) を改訂中. 編集者は Chris Mitchell 氏.
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)			
	Final CD	反対	2nd FCD	ISO/IEC 11770-3:1999-11-01 (1st edition) を改訂中. 編集者は Stephen Savard 氏
11770-4	第 4 部: 弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
	-	-	-	ISO/IEC 11770-4:2006-05-01 (1st edition) を使用中.
13888	否認防止(Non-repudiation)			
13888-1	第 1 部: 総論 (Part 1: General)			
	定期見直し	Approved	1st WD	ISO/IEC 13888-1:2004-06-01 (2nd edition) の改定作業を開始. Nataša Živić 氏の編集者の承認を申請中.
13888-2	第 2 部: 対称暗号技術を用いる機構(Part 2: Mechanisms using symmetric techniques)			
	1st WD	コメントあり	2nd WD	ISO/IEC 13888-2:1998-04-01 (1st edition) を改訂中. Nataša Živić 氏が編集者.
13888-3	第 3 部: 非対称暗号技術を用いる機構 (Part 3: Mechanisms using asymmetric techniques)			
	1st CD	コメント付賛成	2nd CD 投稿	ISO/IEC 13888-3:1997-12-01 (1st edition) を改訂中. 渡辺 創 氏が編集者.
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)			
	FDIS	テキスト未着	FDIS	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)			
	FDIS	テキスト未着	FDIS	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)			
	IS 発行	-	-	ISO/IEC 14888-3:2006-11-15 (2nd edition) を使用中.
	DCOR1	賛成	出版待ち	ISO/IEC 14888-3:2006-11-15 (2nd edition)の訂正文作成中.
	ロシア提案の追補を作成	-	追補の 1st WD	ISO/IEC 14888-3:2006-11-15 (2nd edition)の追補を作成開始.
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)			
	Final CD	コメント付賛成	FDIS	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) の廃止手続き承認.
15946-3	第3部: かぎ確立 (Part 3: Key establishment)			
	-	-	-	ISO/IEC 15946-3:2002-12-01 (1st edition) を 11770-3 改訂まで使用.
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) の廃止手続き承認.
15946-5	第5部: 楕円曲線生成 (Part 5: Elliptic curve generation)			
	2nd WD	---	1st CD	初版作成中. 宮地 充子 氏が編集者.
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)			
	Final CD	賛成	FDIS	ISO/IEC 18014-1:2002-10-01 (1st edition) を改訂中. 市川 桂介 氏と 宮地 充子 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)			
	1st CD	条件付反対	2nd CD	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)			
	定期見直し	継続使用	1st WD	ISO/IEC 18014-3:2004-02-15 (1st edition) の改定作業を開始.
18031	乱数生成 (Random bit generation)			
	-	-	-	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)			
	-	-	-	ISO/I EC 18033-2:2006-05-01 (1st edition) を使用中.
18033-3	第3部: ブロック暗号 (Part 3: Block ciphers)			
	COR1 出版	-	-	ISO/I EC 18033-3:2005-07-01 (1st edition) 及び COR1:2006-08-15 を使用中.
	DCOR2	賛成	出版待ち	ISO/I EC 18033-3:2005-07-01 (1st edition) の訂正文 COR2 を作成中.
	TC68 より訂正要求あり	-	DCOR3	ISO/I EC 18033-3:2005-07-01 (1st edition) の訂正文 COR3 の作成作業を開始.
18033-4	第4部: ストリーム暗号 (Part 4: Stream ciphers)			
	-	-	-	ISO/IEC 18033-4:2005-07-15 (1st edition) を使用中.
	2nd WD of Amendment 1	コメント提出	コメント募集	追加提案の暗号候補にコメント募集. 編集者は Erik Zenner.
19772	認証付き暗号化 (Authenticated encryption)			
	2nd CD	条件付反対	3rd CD	初版作成中.
24745	バイオメトリックテンプレート 保護 (Biometric Template Protection) → WG5 へ移管			
	3rd WD	テキスト未着	3rd WD	編集者の Chun 氏と Lee 氏から要請. SC27 と SC37 の委員長が協議.
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) → WG5 へ移管			
	2nd CD	条件付反対	3rd CD	初版作成中. 才所 敏明氏 → 山田 朝彦氏に編集者が交代.
WG2 検	WG2 検討期間(Study Period): WG2 ロードマップ (WG2 Road Map)			

討期間	前々回より更新なし	テキスト未着	更新予定	SC27/WG2 の会合ごとに改訂される. 櫻井 幸一 氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period): 低電力暗号 (Low Power Encryption)			
	ラポータ文書作成	なし	寄書募集	櫻井 幸一 氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period):著名付き暗号(Signcryption)			
	寄書募集	寄書なし	コメント募集	Liqun Chen 氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period): ディジタル署名の規格統合(Merge of 9796 and 14888)			
	寄書募集	テキスト未着	更新予定	Luis Guillou 氏がラポータ. 検討期間延長.
WG2 検討期間	WG2 検討期間(Study Period): 暗号プロトコルの安全性証明(Formal proof and verification of the security of cryptographic mechanisms)			
	寄書募集	寄書あり	検討期間終了	櫻井 幸一 氏がラポータ.
WG2 検討期間	WG2 検討期間(Study Period): 3 エンティティ認証(Three-party entity authentication)			
	中国からの新規提案	-	WG2 検討期間を開始	Liqun Chen 氏がラポータ.