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

2005－ＣＳＥＣ－30 (22)
2005／7／21

情報セキュリティの標準化動向について
－ISO/IEC JTC1/SC27/WG2 2005年4月ウィーン会議報告－

宮地 充子[†] 近澤 武[‡] 竜田 敏男[Ⅲ] 大塚 玲[Ⅳ] 安田 幹[Ⅴ]

[†]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
[‡]三菱電機株式会社 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1
[Ⅲ]日本アイ・ビー・エム株式会社 アジア・パシフィック標準 〒242-8502 神奈川県大和市下鶴間 1623-14
[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

E-mail: [†]miyaji@jaist.ac.jp [‡]chika@iss.isl.melco.co.jp [Ⅲ]tatsuta@jp.ibm.com
[Ⅳ]a-otsuka@aist.go.jp [Ⅴ]yasuda.kan@lab.ntt.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4月に行われたウィーン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, ウィーン会議

On the Standardization of Information Security
－Report on the Vienna Meeting in April, 2005－

Atsuko MIYAJI[†] Takeshi CHIKAZAWA[‡] Toshio TATSUTA[Ⅲ]
Akira OTSUKA[Ⅳ] Kan YASUDA[Ⅴ]

[†]JAIST 1-1 Asahidai, Nomi, Ishikawa, 923-1292 Japan
[‡]Mitsubishi Electric Corp. 5-1-1 Ohuna,Kamakura, Kanagawa, 247-8501 Japan
[Ⅲ]IBM Japan, Ltd. 1623-14 Shimotsuruma, Yamato, Kanagawa 242-8502 Japan
[Ⅳ]IPA/AIST 2-28-8 Honkomagome, Bunkyou, Tokyo 113-6591 Japan
[Ⅴ]NTT 1-1 Hikarinooka, Yokosuka, Kanagawa 239-0847 Japan

E-mail: [†]miyaji@jaist.ac.jp [‡]chika@iss.isl.melco.co.jp [Ⅲ]tatsuta@jp.ibm.com
[Ⅳ]a-otsuka@aist.go.jp [Ⅴ]yasuda.kan@lab.ntt.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 Vienna in April, 2005.

Keyword ISO, IEC, Information Security Security Vienna

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 は本報告書で取り扱うWG2の他，WG1，WG3の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.

SC27は毎年4月と10月に国際標準化会議を行う. 2004年は4月にシンガポール会議, 10月にブラジル会議が行われた. 本報告書は, 2005年4月に行われたウィーン会議の速報と現在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:2005年4月11日(月)～15日(金)
場所:Austrian Standards Institute – ON
WG2の参加国(人数):オーストラリア(2), ベルギー(2), カナダ(2), フランス(2), ドイツ(4), 日本(16), 韓国(6), ポーランド(1), ロシア(1), シンガポール(1), 英国(2), 米国(3), 中国(2), 南アフリカ(1), オーストリア(1)
WG2の日本からの参加者(順不同,敬称略):苗村(IISEC, WG2議長), 大塚(IPA), 竜田(IBM), 宮地(JAIST), 藤岡, 安田(NTT), 田中(KDDI), 大熊(IPA), 松尾(NTTデータ), 古屋(日立), 空本, 市川(アマノ), 才所, 山田(東芝ソリューション), 上繁(ISIT), 近澤(三菱)

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WG4も開催される.

本会議の最も大きな特徴は中国からの参加人数の増加である. 前回の会議はブラジルであったため, 中国からの参加者は少なかったが, 今回は前々回のシンガポール会議と同じ顔ぶれも多く, 今後精力的に参加してくると予想される. 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, 新しい標準化提案の3項目に関して行われる.

以降, 2章では国際標準化会議で用いられる用語について説明するとともに, WG2で取り扱われている標準化項目についてまとめる. 3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. 4章では新しい標準化提案に関する会議報告を記述する.

2. 標準化項目と用語の説明

WG2で取り扱われている標準化項目については表1(SC27/WG2ウィーン会議結果一覧)を参照されたい. なお, 国際標準化で利用される用語の説明を以下に示す. 日本語訳に関しては日本規格協会発行の「ISO/IEC Directives(第3版, 第4版)」に基づく.

- **WG**(Working Group, 作業グループ):SC傘下の実際に標準化の原案作成と審議を行うグループ.
- **SC**(Sub-Committee, 分科委員会):SC27はJTC1の下の27番目の委員会で, IT Securityを担当する. SCはWGの親委員会にあたる.
- **JTC1**(Joint Technical Committee 1):JTC1はISOとIECが標準化のために設置した合同技術委員会の1番目. JTC1は情報技術分野を担当する. JTC1はSCの親委員会にあたる. 現在はJTCは1番しかない.
- **Study Period**(検討期間):Study Periodとは標準化を行うかどうかを検討する期間を指す. Study Periodには期限や投票はなく, 標準化を行うかどうかの結論が出るまで続けられる. Study Period で標準化を行う結論が出た場合は, JTC1にNP投票を要請する.
- **NP/NWIP**(新業務項目提案): New Work Item Proposalの略. SCやWGでの新規標準化項目の提案のこと. 新規標準化項目の提案がされると, JTC1に対してNP文書を提出し, 各国に投票を依頼する. 賛成多数ならNPは承認されて正式に標準化作業を開始する.
- **WD**(Working Draft, 作業原案):規格文書の素案. 内容が審議中の段階であり, 公式な原案と認められない. WD 文書には投票は無くコメント募集だけを実施する. ある程度のレベルに達したとSCが判断したらCDに進む.
- **CD**(Committee Draft, 委員会原案):WDの次のレベルの原案. CD 文書は3ヶ月の投票にかけられる. 賛成多数なら次のFCDに進む. 賛成票が少数なら原案を修正して再度 CD 投票にかけられる. 2度目のCD投票を実施する文書を2nd CDと記述する.
- **FCD**(Final Committee Draft, 最終委員会原案):CDの次のレベルの原案. FCD は技術的にコメントできる最後のレベルなので, 4ヶ月の投票期間になっている. 賛成票が多数ならばFDISに進む.
- **FDIS**(Final Draft International Standard, 最終国際規格案):標準として発行される寸前の原案. FDIS は2ヶ月の投票にかけられる. 賛成多数ならばIS(International Standard)として発行される. IS 発行までの過程を次に示す. WD -> CD (3M LB) -> FCD (4M LB) -> FDIS (2M LB) -> IS 発行.
- **IS** (International Standard, 国際規格): FDISが投票で承認されると, ISとなって発行される. ISの表紙は, INTERNATIONAL STANDARD と規格番号(例えば, ISO/IEC 12345-6), 規格のタイトル, 発行年月日, 第何版が記載される.
- **Periodical Review** (定期見直し):ISやTRは原則として5年ごとに改訂しなければならない. そのためには改訂の作業期間を考慮して, 発行または前回の点検から3年程度を経過した時点で, 改訂(revision)するか, 継続使用を確認(confirmation)するか, 廃止(withdrawal)するか, をSCが判断してJTC1に通知し, 改訂を要する場合は作業を開始する. この点検作業を定期見直しという.
- **AMD**(Amendment, 追補):発行されているISの内容を変更したり補足する文書と方法. IS を改訂するので

は時間がかかるので，変更部分のみを発行する．AMD 発行までの過程を次に示す．WD→Proposed Draft Amendment (PDAM: 3M LB)→Final Proposed Draft Amendment(FPDAM: 4M LB) →Final Draft Amendment (FDAM: 2M LB) →Amendment (AMD) 発行．

- **COR**(Corrigendum, 訂正文書)：発行されているISに誤記がある場合に訂正する文書と制度．COR 発行までの過程を次に示す．Defect Report (欠陥報告)→Draft Corrigendum(DCOR: 3M LB) →Corrigendum (COR)発行．
- **TR**(Technical Report, 技術報告書)：一般的にISに比べて規定部分が少ないガイドラインや解説書などがTR に該当する．TR 発行までの過程を次に示す．WD →Proposed Draft Technical Report(PDTR: 3M LB) → Draft Technical Report (DTR: 3M LB) → Technical Report(TR)発行．
- **NB** (National Body, 参加国): ISO や IEC の活動に投票権を有して参加する国の呼び方．参加国が TC や SC の活動に参加する場合は，P-member (Participate member，活動参加国) または O-member (Observer member, 傍聴参加国) のいずれかの参加形態を選択できる．SC の P-member は，寄書の提出，SC 会議への参加，文書の閲覧，SC が扱う投票案件の投票，SC 傘下の WG への専門家の派遣などができる．SC の O-member は，SC が扱う投票案件の投票ができない点を除き，P-member とほぼ同等の活動ができる．
- **LB**(Letter Ballot, 郵便投票)：投票には郵便，e-メール，事務局が開設する Web 投票画面などの手段で行う投票と，会議の席上で行う投票の2種類があり，慣例で前者を郵便投票と称している．投票結果の判定は，どのレベルの投票かで異なる．SC 事務局が扱う投票(NP 投票，CD 投票，FCD 投票，PDAM 投票，FPDAM 投票，PDTR 投票，DCOR 投票)は，SC の P-member だけが投票できる．投票結果は，大多数の賛成が得られたかで判断される．これに対して，ISO 中央事務局が扱う投票(FDIS 投票，FDAM 投票，DTR 投票，DIS 投票)は，(1) JTC1 の P-member の投票総数の内の賛成票が 2/3 を超える，(2) ISO と IEC の参加国の投票総数の内の反対票が 1/4 を超えない，の両方を満足していると賛成多数と判定される．
- **Contribution**(寄書)： NB(参加国)，expert(専門家)及びリエゾン(提携先の組織)から提出される文書で，新規提案，修正提案，情報提供，コメントなどが該当する．

3. 標準化段階及び現国際規格の見直しの報告

3.1. 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 つから構成される．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．

3.1.1 第 2 部 因数分解に基づく機構 (IS 9796-2)

IS 9796-2 は 1997 年に国際規格の第一版が発行され，その改訂版が 2002 年に発行された．記述されているメカニズムは 3 方式である．どのメカニズムも RSA 署名により署名を生成するが，署名に入力するメッセージのフォーマット生成の違いにより 3 方式が規格化されている．なお，フォーマット生成の違いにより，2 方式は，確定的署名方式(同じ平文に対する署名が同じ)，1方式が確率的署名方式(同じ平文に対する署名が同じとは限らない)となる．なお，確率的署名方式は PSS-R とほぼ同じである．

今回の定期見直しの会議においては，目立った問題もなく継続使用をすることが決定した．

3.1.2 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 年より改定が始まった．本規格の編集者は宮地 充子氏が務める．

本会議は，FCD 投票の結果(19 賛成票，1反対票(UK))を踏まえての対応だった．UK からの主な反対理由は，1．各メカニズムの実装に必要な楕円曲線や有限体の記述の追加，2．各メカニズムを楕円曲線と有限体の両方で記述の2点だった．会議の結果，1 に関しては全て ANNEX に記述し，2に関しては現規格(IS9796-3, IS15946-4)に従うことになった．この結果，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)の各方式が規格化されることになる．

本会議で，本規格は FDIS に進むことになったが，FDIS 投票は 10 月会議以降になると考えられる．

3.2. メッセージ認証符号 (9797)

9797 はメッセージ認証符号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，本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.

3.2.1. 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, 現在の国際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ているアルゴリズム5と6の2つを削除することで改訂が進められている. 本会議では直前にNIST SP800-38B:2005 "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication" (2005/3/9)が発行されたため, これを規格文書に反映するために改訂が間に合わなかった. 現在審議中の改訂版では, 前述の通りMACアルゴリズム5と6の2つを削除して, 新たにOMACとCMACが追加になっている. 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. Bart Preneel 氏が編集者を務めている. 1st CD投票に進む.

3.2.2 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. 現在の国際規格には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. 本会議では定期見直しが行われ, SHA-1攻撃論文は本規格に影響ないことや, 長い出力値を持つハッシュ関数を盛り込むことへの疑問(速度が遅い)のコメントもあったが, 改訂することで合意された. Bart Preneel 氏が編集者を務める. 現在, 寄書を募集している.

3.2.3 第3部 万能ハッシュ関数を用いる機構(9797-3)

ベルギーより, universal hash functionを用いたMACの標準化提案があり, 9797にパートを追加して規格化することが合意された. 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 氏が編集者を務める. 現在, 寄書を募集している.

3.3. 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.

3.3.1 第1部 総論 (IS 9798-1)

第1部(総論)は定期見直しの時期を迎えており, 前回のブラジル会議で改訂することが決定していた.

しかしウィーン会議にて, 改訂を提唱していた唯一の国である米国のNBコメント(参考文献等の更新に関するもの)を見直した結果, 改訂に値するほどのものではないという結論に至った. さらに, もし改訂することになった場合, 編集者への立候補がないことも判明した. これらの結果を受けて, 結局は改訂を取りやめ現規格(1997年版)を継続使用するということで合意した.

3.3.2 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)は定期見直しの時期を迎えており, ウィーン会議では改訂を行うべきか否かの検討がされた. 日本を含む5カ国から改訂の意見が提出されており, ウィーン会議での議論の結果, 改訂を行うことが決定された. 今後は寄書と編集者の応募が行われる運びとなっている.

3.3.3 第3部 ディジタル署名技術を用いる機構 (IS 9798-3)

第3部(ディジタル署名技術を用いる機構)は定期見直しの時期を迎えているが, 特に改訂すべきとの強い意見は出されなかったため, ウィーン会議では1998年版を継続使用することが決定された.

3.3.4 第5部 ゼロ知識技術を用いる機構(IS 9798-5)

第5部(ゼロ知識技術を用いる機構)はつい最近(2004年)FDIS投票が終了し, IS出版になったばかりの規格である.

ところが, FDIS投票時に提出されていたイギリスのNBコメントがISに反映されなかった(ITTF編集者が拒絶)ため, 英国より欠陥報告が提出された.

多くのNBは特に意見がなかったため, 苗村コンビーナの調整の結果, 英国が欠陥報告を取り下げることで決着した.

3.3.5 第6部 手動データ移動を用いる機構 (9798-6)

第6部(手動データ移動を用いる機構)は他の部とやや趣を異にする部で, 予めの鍵共有を前提としない場合の相互エンティティ認証を扱う. 現在, 4つのメカニズムが採録されている.

ウィーン会議の時点で既にFDIS投票の結果が出ていたので, ウィーン会議では本規格がIS出版に進むことが承認された.

3.4. ハッシュ関数 (10118)

ハッシュ関数の国際規格を定める10118は, General(ハッシュ関数全般)の規格(10118-1), n-bitブロック暗号アルゴリズムを利用したハッシュ関数(10118-2), 専用ハッシュ関数(10118-3), モジュラー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. 本会議では10118-3に対する修正案と10118-4の2つが審議されたので, その報告を行う.

3.4.1. 第3部 専用ハッシュ関数 (10118-3AMD1)

IS10118-3:2004 は,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. これに対し, 米連邦標準 FIPS 180-2 に採用されている SHA-224 と動作確認用のテストベクタを追加する追補の発行が合意されており, 本会議ではこの追補について審議し, FDAM 投票(FDIS 投票に相当)に進むことが承認された.

この規格審議とは別に, 最近の SHA-1 の安全性低下を示す研究結果に対する SC27 としての対応策を協議し, SHA-1 の安全性に関する情報の募集と SHA-1 に関する SC27 からのステートメントを HP に掲載することで合意した.

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

10118-4:1998 はモジュラー演算を用いるハッシュ関数に関する規格である. 10118-4:1998 には 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. 本会議では 10118-4:1998 の定期見直しが行われた. 日本と英国が利用されていないこと, 計算効率が悪いことなどを理由に廃止を提案した. しかし, 本会議では SHA-1 の問題もあるので残しておき 5 年後に見直してその時点でも使用実績がなければ廃止すれば良いとのコメントが出され, さらにカナダからも具体的に修正すべき箇所が示されていたことから, 最終的には改訂することで合意した.

3.5 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 と 11770-2 は 1996 年, 11770-3 は 1999 年にそれぞれ国際規格となっている. 11770-4 は 2002 年から審議が開始されており, 現在審議中である.

3.5.1 第 1 部 枠組み (IS 11770-1)

11770-1 は鍵管理の枠組みの規格で, 鍵のライフサイクル, 鍵の用途別種類の定義, 鍵配送のモデルについて記述されている.

日本は文献をアップデートする必要があるとして改訂とコメントしていたが, 今回の定期見直しの会議において, 技術的内容の修正ではないので, 結局継続使用となった.

3.5.2 第 2 部 対称暗号技術を用いる鍵確立機構 (IS 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.

昨年, 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を指摘する論文[*]が出されたため至急対応が必要となった. この方式 12 を削除する訂正文書に対する投票が行われた結果, 反対無しで承認され, 訂正文書発行と決定した.

また, 同時に行われた定期見直しにおいても, 各国から方式 12 を削除すべきとのコメントが出て, 改訂することになった.

[*] Z. Cheng and R. Comley, Attacks on an ISO/IEC 11770-2 key establishment protocol, Cryptology ePrint Archive, Report 2004/249 (http://www.iacr.org)

3.5.3 第 3 部 非対称暗号技術を用いるかぎ確立機構 (IS 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.

今回の定期見直しの会議において, 改訂することが合意された.

3.5.4 第 4 部 弱い秘密に基づく機構 (11770-4)

11770-4 は弱い秘密(パスワードのような人間が覚える秘密情報:選択する範囲が狭い)に基づく鍵管理の規格で, パスワード認証鍵共有機構, および鍵回復機構をそれぞれ幾つか規定している.

本会議で, 本規格は FDIS に進むことになったが, 投票用のドラフト回覧前にエキスパートに修正ドラフトを確認してもらうことになっている.

3.6 添付型ディジタル署名 (14888)

14888 は付録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.

3.6.1 第 1 部 総論 (14888-1)

14888-1 は付録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 玲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, 14888-1 は 1stCD に進むことで合意した.

3.6.2 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), RSA (RSA-PSS), GQ1, GQ2, GPS1, GPS2, ESIGN の7つのアルゴリズムが掲載されている. 本会議では FCD に進むことに

反対するNBが多かったため，2nd CDとなることで合意した．Louis Guillou 氏が編集者を務める．

3.6.3 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 FCD 投票へ進むことが合意された．

[*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.

3.7 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，第4部を除いた全ての規格が定期見直しとなったのでその報告を行う．

3.7.1. 第1部 総論 (IS 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ある．付録として，楕円曲線の各種加算公式も記載されている．

今回の定期見直しの会議において，IS 15946-1 は，現在策定中である 9796-3, 14888-3, 11770-3 等で必須となる技術が含まれていないため，改定の提案が日本とUKからあった．定期見直し会議の結果，規格の改定が決定し，宮地充子氏の編集者の申請中である．

3.7.2. 第2部 ディジタル署名 (IS 15946-2)

15946-2 は楕円曲線を用いたディジタル署名の規格である．具体的な方式として，EC-GDSA (ドイツ)，EC-DSA (米国)，EC-KCDSA(韓国)の各方式が規格化されている．

IS 15946-2 は，現在改定中である添付型ディジタル署名の国際規格 14888-3 に統合される予定である．このため，現策定中の国際規格の出版まで継続使用を行い，新規格発行後，廃止されることが確認された．

3.7.3. 第3部 かぎ確立 (IS 15946-3)

15946-3 は楕円曲線に基づく鍵確立の規格である．鍵確立の技術は Key agreement(鍵共有)と Key transport(鍵輸送)からなる．鍵共有では，鍵共有を行うエンティティはそれぞれ対等であり，どのエンティティも共有鍵の値を予め決定できない．鍵輸送では，一方が共有する鍵を決定し他方に輸送することで鍵確立を行う．15946-3 では，これら 2 種類の鍵確立として，全 10 方式が規格化されている．

IS 15946-3 は，現在改定中である鍵確立の国際規格 14888-3 に統合される予定である．このため，現策定中の国際規格の出版まで継続使用を行い，新規格発行後，廃止されることが確認された．

3.7.4. 第 4 部 メッセージ復元型ディジタル署名 (IS 15946-4)

15946-4 は楕円曲線に基づくメッセージ復元型署名の規格である．15946-2 ではメッセージの全てが署名検証の入力に必要な署名方式を取り扱うのに対し，15946-4 ではメッセージの一部が署名検証の入力に必要になる，あるいはメッセージの入力を必要としない署名方式を取り扱う．本規格においては ECNR (フィンランド)，ECMR (日本，松下電器)，ECAO(日本，NTT)，ECPV(米国)，ECKNR(韓国)の各方式が規格化されている．

3.8 タイムスタンプサービス (18014)

IS 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．最近，日本にもタイムスタンプを生成して時刻証明書を発行するサービスを実施している企業があり，そのプロトコルやパラメータに問題意識が生まれている．

3.8.1 第1部 枠組み (IS 18014-1)

第 1 部はちょうど定期見直しの時期になっているので，本会議に向けて各国の意見が募集された．日本とスペインが改訂と回答して，他の国々は特に意見も無く継続使用とした．日本の改訂理由は，(1) seraialNumber というパラメータが規定されているが使用されていないのでオプションにすべき，(2) accuracy というパラメータがあるが常時誤差を測定するのは困難なので一定の保証値で示すべき，(3) 申請者はレシートを受け取るとなっているがレシートの中身が定義されていない，というもの．スペインの改定理由は普及を進めるために，(1) ASN.1 の他に XML フォーマットの採用，(2) 署名サービスに時刻も入れた同一のサービス化，(3) タイムスタンプサービスの品質評価基準の検討，(4) 利用者によるタイムスタンプの評価の実現，などというもの．結果的に具体的な提案をした日本とスペインの意見が通って改訂することになった．改訂作業の編集者には空本忠昭氏が就任した．

3.8.2 第 2 部 独立トークンを生成する機構 (IS 18014-2)

こちらも同時に定期見直しの時期になっているので，本会議に向けて各国の意見が募集された．日本とスペインが改

訂と回答して，他の国々は特に意見も無く継続使用とした．日本の改訂理由は，(1) 公開鍵暗号を使用しているPKIタイムスタンプシステムにリンク情報を拡張フィールドに移すオプションの追加，(2) 上記説明の追加，でした．スペインの意見は18014-1と共通でした．結果的に具体的な提案をした日本とスペインの意見が通って改訂することになった．改訂作業の編集者は，スペインのJ. Mañas 氏が就任した．

3.9. 乱数生成 (18031)

乱数生成の国際規格を定める18031は，乱数生成のモデルや乱数生成器の要求条件を規定し，Deterministic な乱数生成アルゴリズム (以下 DRBG)の例として，SHA-256を用いた乱数生成，AES を用いた乱数生成，Micali-Schnorr 法(以下 MS 法)など，Non- deterministic な乱数生成アルゴリズムとして仮想 noisy diode を用いた例など，を掲載している．2000 年より審議が開始されている(2001 年にタイトルを Random number generation から Random bit generation に変更)．

FCD 文書に対して唯一反対票を投じていた日本は，MS 法よりも，以前掲載されていた Blum-Blum- Shub DRBG(以下 BBS)や Blum-Micali DRBG の方が有名だとして，「これらを復活させるべき」との主張であるが，編集者側は，非技術的な理由(早期規格化および体裁を合わせる手間)により，この日本の主張に否定的であった．会議上，「もしBBS等を追加したいのなら，規格成立後に日本から追補を出す」可能性があることが確認され，結局日本は賛成にまわった．また，本文に記述されている要求条件に合うDRBG であれば，掲載の DRBG 以外にも使用できる旨の記述追加が決定されたこともあり，最終的にFDIS へ進むことが合意された．

3.10 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．

3.10.1 第2部 非対称暗号(18033-2)

第 2 部(非対称暗号)には，ECIES-KEM(米国)・PSEC-KEM(日本)・ACE-KEM(スイス)・RSAES・RSA-KEM(米国)・HIME(R)(日本)の6つのアルゴリズムが採録されている．

本規格はブラジル会議の時点で既に FCD 投票結果が出ていたが，本規格の編集者がブラジル会議を欠席したためブラジル会議では特に議論がされず，ウィーン会議まで持ち越しとなっていた．ウィーン会議では特に大きな問題はなく，FDIS 投票へ進むことで各国が合意した．

3.10.2 第3部 ブロック暗号 (18033-3)

第3部(ブロック暗号)には，64ビット暗号ではTDEA(米国)・MISTY1(日本)・CAST-128(カナダ)の3つのアルゴリズムが，そして128ビット暗号ではAES(米国)・Camellia(日本)・SEED(韓国)の3つのアルゴリズムが採録されている．

ウィーン会議ではFDIS 投票の最中であり，特に大きな問題も無かったので，本規格のセッションは設けられなかった．

なお，FDIS 投票の結果はウィーン会議後の5月23日付で告示され，賛成多数により本規格のIS 出版が確実となった．

3.10.3 第4部 ストリーム暗号 (18033-4)

ウィーン会議の時点で，第 4 部(ストリーム暗号)にはMUGI(日本)とSNOW 2.0(スウェーデン)の2つのアルゴリズムが採録されており，FDIS の投票中であった．

そこにデンマークからの寄書として，新たなストリーム暗号アルゴリズム Rabbit を追加する旨の追補を作成すべきとの提案があった．これを受けて，各国に追加のストリーム暗号アルゴリズムを募集し，その結果を見て追補を作成するか否かを検討することになった．

なお，FDIS 投票の結果はウィーン会議後の5月23日付で告示され，賛成多数により本規格のIS 出版が確実となった．

3.11 データカプセル化機構 (19772)

19772 ではデータカプセル化機構 (DEM，対称暗号と MAC の組合せ方)の国際規格を扱う．小部はない．ウィーン会議前の時点では，OCB・AES Key Wrap・CCMの3つのメカニズムが記載されていた．

ウィーン会議では，主にイギリスからの寄書により，記載されるメカニズムが3つから7つに増えることになった．この大幅な変更を受けて，WDから1st CDに進めるべきかどうかの議論がなされた．その結果，FCD に進める前に(CD の段階で)各メカニズムを精査し最終的に採録すべきメカニズムを吟味するという前提条件の下に，今回は1st CD へ進めることで各国が合意した．

なお，ウィーン会議では本規格のタイトルを “Data encapsulation mechanisms” から “Authenticated encryption” に変更することも決定している．

4.新規格

4.1 バイオメトリクス関連

最近銀行の ATM に静脈などの生体認証装置が付いてきたが，このような生体認証(バイオメトリクス)装置などの標準を作成するのは，JTC1/SC37 の担当である．しかし，生体認証装置のセキュリティや，生体認証装置とサーバとの間のプロトコルのセキュリティ面での標準化をJTC1/SC27が担当する．そこでJTC1/SC27は，バイオメトリクス関係の標準化で他の委員会(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するために Ad Hoc Group on Biometrics という臨時委員会を設置した．この委員会はウイーン会議で Advisory Group on Biometrics と改称され，常設の委員会になった．以下の説明はこの Advisory Group のウイーン会議での報告書を元にしている．

4.1.1 バイオメトリック技術のセキュリティ評価及び試験の枠組み(NP 19792)

NP19792 はSC27/WG3で実施されている. 開始してから1年以上が経過するが, 具体的な標準原案がなく, 本会議では3rd WDが審議された. 日本の寄書は, バイオメトリクス特有の脆弱性があるので, 一般的な手法で脆弱性を点検するのでなく, アルゴリズムレベル, インプリメンテーションレベル, システム環境とアプリケーションレベルに分けて脅威と対策を検討すべきというものである. 具体的な標準原案の提出は初めてで, 本寄書の採用が決まった. また寄書提出者である三村昌弘氏は共同編集者に就任した.

4.1.2 バイオメトリックテンプレート保護 (NP 24745)

NP24745 はJTC1/SC37から依頼されたもので, 生体認証装置で読み取った生体情報をマスターデータとしてサーバに蓄積してデータベースを構築する際の, マスターデータのセキュリティ強化を目的とした標準化である. 各国に提案を呼びかけていたが, ようやく韓国から寄書が提出されたので, これをベースに具体的な原案作成作業を開始することになった. 編集者は寄書を提出した韓国の Park 氏が就任した.

4.1.3 バイオメトリックデータの認証 (WG2 検討期間)

これは各国に提案を呼びかけていたが, ようやく韓国と日本から寄書が提出された. 韓国の寄書(バイオデータを基にして暗号や署名の鍵を生成する)は, 各国から実現性について疑問が呈されたため, 韓国に9月頃を目処に寄書を修正して再提出を要請し, 修正版を各国がレビューすることになった. 一方, 日本の寄書は生体認証装置で本人確認をした結果をサーバに送る際に, セキュリティの証明書などを添付してサーバが認証結果を信用出来るようにする提案. ISO/TC68(金融サービス業務の標準化を担当)の委員から, ISO/CD 19092 に応用できるので TC68/SC2 と連携したいとコメントがあり, 日本寄書を添付したリエゾン文書を SC37 と TC68/SC2 と ITU-T/SG17 に送ることになった. また, この日本寄書の"Biometric Authentication Context"という名称をNWIP のプロジェクト名として JTC1 に提出することになった. 編集者は寄書を提出した才所敏明氏が就任した. この決定によって検討期間は終了した.

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 議長, 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. ここに感謝の意を表したい. 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, 平野 WG1 委員, WG2 国内委員会各委員, 情報処理学会の三田氏によりご助言を頂いた. ここに感謝の意を表したい.

表1 SC27/WG2 ウィーン会議結果一覧 (2005-04-11/19) ※SC27 Plenary (2005/4/18-19)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)			
				ISO/IEC 7064:2003-02-01 (2nd 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 msg recovery)			
9796-2	第2部: 因数分解に基づく機構 (Part 2: Integer factorization based mechanisms)			
	定期見直し	改訂	継続使用	ISO/IEC 9796-2:2002-10-01 (2nd edition) を点検. OIDとASN.1を追加する追補を作成する. 編集者募集.
9796-3	第3部: 離散対数に基づく機構 (Part 3: Discrete logarithm based mechanisms)			
	FCD	賛成	FDIS	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	改訂テキスト未着で未投票	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)			
	定期見直し	改訂	改訂	ISO/IEC 9797-2:2002-06-01 (1st edition) の見直し. Bart Preneel 氏は長いの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)			
	-	-	第2部分割	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)			
	改訂	-	改訂中止	編集者応募者が無いため, 改訂を中止して継続使用に. ISO/IEC 9798-1:1997-08-01 (2nd edition) を再見直し.
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)			
	定期見直し	改訂	改訂	ISO/IEC 9798-2:1999-07-15 (2nd edition) を見直し.
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)			
	定期見直し		継続使用	ISO/IEC 9798-3:1998-10-15 (2nd edition) を見直し.
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)			
	IS 出版済み	-	-	英国の欠陥報告は取り下げられた. 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			
	FDIS	賛成	IS 出版予定	初版作成中.
9979	暗号アルゴリズムの登録手続 (Procedures for registration of cryptographic algorithms)			
	アンケート	廃止	廃止	ISO/IEC 9979:1999-04-01 (2nd edition) を点検. JTC1 での廃止投票に移行する.
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)			
	Revised FCD	-	FDIS	ISO/IEC 10116:1997-04-15 (2nd edition) を改訂中
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)			
				ISO/IEC 10118-2:2000-12-15 (2nd edition) を使用中.
10118-3	第 3 部: 専用ハッシュ関数 (Part 3: Dedicated Hash-functions)			
	FPDAM	コメント付賛成	FDAM	ISO/IEC 10118-3:2004-03-01 (3rd edition) の追補を作成中. "SHA-1"に関する SC27 の意見表明を出す.
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			
	定期見直し	廃止	改訂	ISO/IEC 10118-4:1998-12-15 (1st edition) を見直し. 日本と英国の廃止提案に各国が追随し, 廃止で一旦合意したが, 後日 Bart Preneel 氏の反対で, 改訂することに.
11770	かぎ管理 (Key managemen)			
11770-1	第 1 部: 枠組み (Part 1: Framework)			
	定期見直し	改訂	継続使用	ISO/IEC 11770-1:1996-12-15 (1st edition) を見直し. 参考文献のみの改訂要求であれば継続使用となった.
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)			
	DCOR	賛成	Corrigendum 発行	ISO/IEC 11770-2:1996-04-15 (1st edition) の訂正文書を作成中.
	定期見直し	改訂	改訂	ISO/IEC 11770-2:1996-04-15 (1st edition) を見直し. 寄書を募集する. Mitchell 氏が編集者に就任.
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)			
	定期見直し	改訂	改訂	ISO/IEC 11770-3:1999-11-01 (1st edition) を見直し. 寄書と編集者を募集.
11770-4	第 4 部: 弱い秘密に基づく機構 (Part 4: Mechanisms based on weak secrets)			
	FCD	賛成	FDIS	初版作成中.
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)			
				ISO/IEC 13888-2:1998-04-01 (1st edition) を使用中.
13888-3	第 3 部: 非対称暗号技術を用いる機構 (Part 3: Mechanisms using asymmetric techniques)			
				ISO/IEC 13888-3:1997-12-01 (1st edition) を使用中.

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)			
	1st WD	コメントなし	1st CD	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 CD	コメント付賛成	2nd CD	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)			
	1st CD	コメント付賛成	FCD	ISO/IEC 14888-3:2001-09-15 (corrected) を改訂中. 日本のコメントは一部が不採用.
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)			
	定期見直し	改訂	改訂	ISO/IEC 15946-1:2002-12-01 (1st edition) を見直し. 宮地充子氏が編集者就任の要請.
15946-2	第 2 部: ディジタル署名 (Part 2: Digital signatures)			
	定期見直し	継続使用	継続使用	ISO/IEC 15946-2:2002-12-01 (1st edition) を見直し.
15946-3	第 3 部: かぎ確立 (Part 3: Key establishment)			
	定期見直し	継続使用	継続使用	ISO/IEC 15946-3:2002-12-01 (1st edition) を見直し.
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.
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)			
	定期見直し	改訂	改訂	ISO/IEC 18014-1:2002-10-01 (1st edition) を見直し. 空本 忠昭 氏が編集者に就任.
18014-2	第 2 部: 独立トークンを生成する機構 (Part 2: Mechanisms producing independent tokens)			
	定期見直し	改訂	改訂	ISO/IEC 18014-2:2002-12-15 (1st Edition) を見直し. スペインの Mañas 氏が編集者に就任.
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)			
	FCD	反対	FDIS	初版を作成中. BBS 等を追加するのであれば amendment を提案.
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/IEC 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)			
	2nd FCD	賛成	FDIS	初版作成中.
18033-3	第 3 部: ブロック暗号 (Part 3: Block ciphers)			
	FDIS	コメント付賛成	IS 出版予定	初版作成中.
18033-4	第 4 部: ストリーム暗号 (Part 4: Stream ciphers)			
	FDIS	コメント付賛成	IS 出版予定	初版作成中. 追加のストリーム暗号を募集. 募集結果によって追補を作成するかどうかを検討.
19772	データ カプセル化 機構 (Data encapsulation mechanisms)			
	2nd WD	コメントあり	1st CD	初版作成中. タイトルを"Authenticated encryption"に変更.
19792	バイオメトリック技術のセキュリティ評価及び試験の枠組み A framework for security evaluation and testing of biometric technology			
	3rd WD	寄書提出	4th WD	初版作成中. 日本からの寄書を採用. 三村昌弘氏が共同編集者に就任.
24745	バイオメトリック テンプレート 保護 (Biometric Template Protection)			
	韓国から寄書	コメントなし	1st WD	初版作成中. 韓国の Park 氏が編集者に就任.
WG2 検討期間	バイオメトリック データの認証 (Authentication of biometrics data)			
	寄書募集	寄書提出	検討期間終了	日本寄書はリエゾン文書として SC37, TC68, ITU-T へ送付. タイトルが"Biometric authentication context − BAC"となり NWIP 投票に進む. 才所 敏明 氏が編集者に就任.
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.