☞TOPICS

情報技術の国際標準化と日本の対応

－ 2003 年度の ISO/IEC JTC 1 および情報規格調査会の活動 －

情報規格調査会

1. ISO/IEC JTC 1 の活動

1.1 概要

2003 年度の ISO/IEC JTC 1（以降 JTC 1 と略す）の活動を報告する．

まず，JTC 1 の運営活動については，JTC 1 のビジネスプラン等の今後への動き，JTC 1 の将来の活動テーマを検討している SWG（Special Working Group）for Technology Watch などの JTC 1 総会での活動について報告する．また，日本が幹事国の JTC 1/SC 23 が JTC 1/SC 11 を統合したことおよび Directives 第 5 版の発行などついても報告する（1.5 章参照）．

2003 年度に経済産業省から受託した事業“メタモデル相互運用枠組み”の活動についても報告する（1.4.5 章参照）．

また，2003 年度も情報技術に関する有益な標準化が多く進められたが，本報告では特に最近の市場でのニーズに応える 5 項目に絞って報告する（1.4 章参照）．

1.2 最新の組織

最新の組織構成を図 -1 に示す．2003 年度は，SWG for Technology Watch の活動から Web Services SG および Privacy Technology SG が新設され，JTC 1/SC 23 が JTC 1/SC 11 を統合した．

1.3 国際規格の実績（2003 年 1 ～ 12 月）

2003 年の国際規格の出版数は，IS 112 件，ISP 11 件，TR 10 件で合計 133 件（2002 年：IS 139 件，ISP 0 件，TR 10 件で合計 149 件）で，昨年に比べ 16 件（11%）減少した．また，2003 年に国際規格案となったものが FDIS/DIS 83 件，DISP 0 件，DTR 13 件で合計 96 件あり（2002 年：FDIS/DIS 95 件，DISP 0 件，DTR 12 件で合計 107 件），昨年とほぼ同じ水準を維持した（表 -1，表 -2 参照）．

1.4 技術的トピックス

最近の市場のニーズに応える標準化活動のトピックスとして，JTC 1/SC 7 の活動，ICAO（国際民間航空機関）と JTC 1/SC 17/WG 3 が協力して策定している E- パスポートの標準化状況，Linux の国際標準化，情報技術標準 NEWSLETTER 61 号より転載した楕円曲線暗号の原理と国際規格化およびメタモデル相互運用枠組みについての 5 項目を報告する．

1.4.1 JTC 1/SC 7 の活動

SC 7 専門委員会 委員長　山本喜一

JTC 1/SC 7 は，ソフトウェア開発に関連したソフトウェアおよびシステム技術の標準化に取り組んでおり，現在は 11 の WG で多数のプロジェクトが進行している．2003 年度は，5 月にカナダのモントリオールで第 16 回総会と各 WG 会議が開催され，さらに WG ごとに 1，2 回の国際会議が開催され，きわめて活発に活動を行っている．総会には 17 カ国から 109 名を超す代表が参加し，日本からは 11 名が参加した．活動の成果としては，FDIS 6 件，FCD 2 件，CD 13 件，DTR 2 件，NP 17 件，FPDAM 1 件，DCOR 1 件，CDR 他 2 件の審議，投票を行い，7 件の管理的な事項についての意見提出，投票も行っている．さらに，WG 6 のコンビーナ，セクレタリおよび総合プロジェクトエディタ 1 名のほか，多くの WG にプロジェクトエディタ合計 12 名を提供している．

それぞれの WG が活発に活動を行っており詳細を述べることはできないが，今年度発行された IS，承認された NP，FDIS および DTR 投票を終了した案件を中心に述べる．

（1）ソフトウェアのドキュメンテーション（WG 2）

応用ソフトウェアのユーザ文書の設計と準備（IS 18019 Guidelines for the design and preparation of user documentation for application software）が出版され，ソフトウェア文書の管理要領（DTR 9294 Guidelines for the management of software documentation）が承認された．

（2）ツールと CASE 環境（WG 4）

要求技術ツールの要件（Requirement Engineering Tool Requirements），およびケースツールの採用ガイド（TR 14471 Guidelines for the adoption of CASE tools）とケース

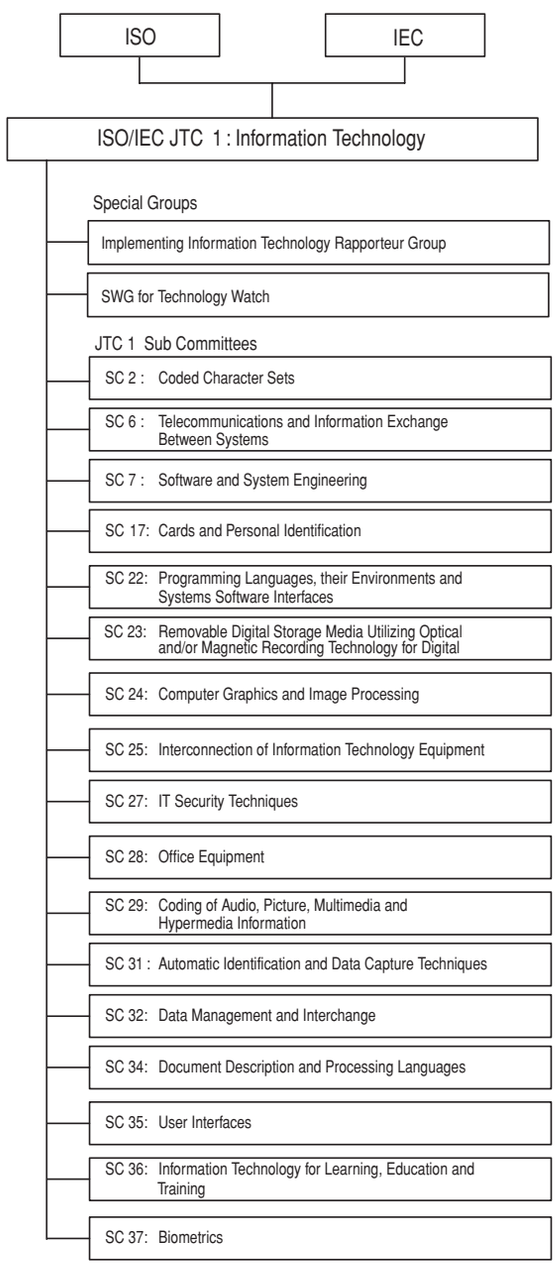

図 -1　ISO/IEC JTC 1 の構成

区　分		件 数	総ページ	平均ページ
IS	IS（初版）	22（ 54）	1,750（ 5,032）	79（ 93）
	IS（改訂版）	54（ 19）	10,337（ 4,224）	191（222）
	Amendment	14（ 9）	353（ 415）	25（ 46）
	Corrigendum	22（ 57）	554（ 252）	25（ 4）
	小 計	112（139）	12,944（ 9,923）	116（ 71）
ISP	ISP	11（ 0）	505（ 0）	46（ 0）
	Amendment	0（ 0）	0（ 0）	0（ 0）
	小 計	11（ 0）	505（ 0）	46（ 0）
TR		10（ 10）	593（ 593）	53（ 59）
合　計		133（149）	14,038（10,516）	105（ 71）

() 内は 2002 年の数字

（注記） IS：国際規格
ISP：国際標準プロファイル
TR：技術報告書

表 -1　2003 年に出版された国際規格，他の集計

区　分		件 数	総ページ	平均ページ
DIS	FDIS・DIS	60（ 84）	10,783（ 10,873）	179（129）
	FDAM・DAM	23（ 11）	1,473（ 556）	64（ 50）
	小 計	83（ 95）	12,256（ 11,429）	147（120）
DISP	FDISP・DISP	0（ 0）	0（ 0）	0（ 0）
	FDAM・DAM	0（ 0）	0（ 0）	0（ 0）
	小 計	0（ 0）	0（ 0）	0（ 0）
DTR		13（ 12）	833（ 1,488）	67（124）
合　計		96（107）	13,139（12,917）	136（120）

( ) 内は 2002 年の数字

（注記） DIS：国際規格案
DISP：国際標準プロファイル案
DTR：技術報告書

表 -2　2003 年に投票に付された国際規格案，他の集計

ツールの評価と選択のガイド（TR 14102 Guidelines for the evaluation and selection of CASE tools）の改訂が NP として承認された．

（3）ソフトウェア製品の品質評価と測定（WG 6）

9126 シリーズのパート 2：外部測定法（External metrics），パート 3：内部測定法（Internal metrics）およびパート 4：利用時の品質測定法（Quality in use metrics）が TR として発行され，国際規格制定作業を完了した．また，全体が 14 冊で構成される IS 25000 SQuaRE（Software quality requirements and evaluation）シリーズは，25000：SQuaRE の利用ガイド（Guide to SQuaRE），25020：測定の参照モデルおよびガイド（Measurement reference model and guide），25030：品質要求事項およびガイド（Quality requirements and guide），25021：測定基本要素（Measurement Primitives）について作業を進めた．

（4）ライフサイクル管理（WG 7）

ソフトウェアライフサイクルプロセス－保守（IS 14764 Software lifecycle process Maintenance）の改訂が NP として認められた．

（5）システムの完全性（WG 9）

コンピュータソフトウェアへの ISO 9001：2000 適用ガイド（IS 90003 Guidelines for the application of ISO 9001:2000 to computer software）が出版され，ソフトウェアライフサイクルプロセス－リスク管理（IS 16085 Software lifecycle process Risk management）が NP として認められた．

（6）プロセスの評価（WG 10）

日本からの提案により 5 部構成とすることになった国際規格案は，TR 発行後の試行の結果を踏まえて 2003 年に 2 部が審議を終了している．パート 2：アセスメントの実施（IS 15504-2 Process assessment Part 2: Performing an assessment），パート 3：アセスメントの実施のガイド（IS 15504-3 Process assessment Part 3: Guidance on performing an assessment）を発行し，パート 4：プロセス改善と能力決定への利用ガイド（FDIS 15504-4 Process assessment Part 4: Guidance on use for process improvement and process capability determination）が FDIS 投票を通過している．

（7）機能的規模測定法（WG 12）

パート 5 は 2003 年度に TR として出版された．他に，機能規模測定の具体的な手法である COSMIC-FFP も IS 19761 として出版された．また，機能規模測定法－パート 6：ISO/IEC 14143 および関連国際規格の利用ガイド（Functional size measurement Part 6: Guide for use of ISO/IEC 14143 series and related international standards）が NP として承認された．

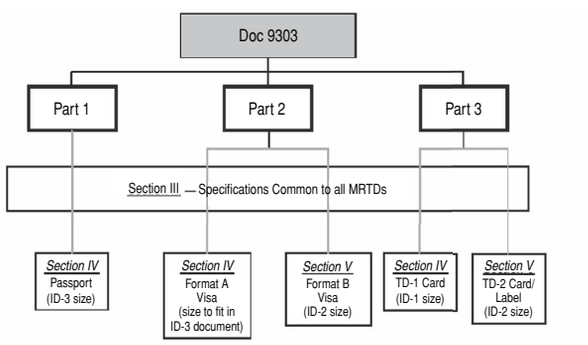

図 -2　Doc 9303 の構成

（8）モデリング言語，メタデータ，ODP フレームワークおよび部品（WG 19）

CDIF セマンティックメタモデル－パート 3：データ定義（CDIF Semantic meta model Part 3: Data definition）およびパート 5：データフローモデル（Part 5: Data flow models）が NP として承認された．

（9）ソフトウェア技術知識体系（WG 20）

ソフト工学の基礎知識（DTR 19759 Guide to the software engineering body of knowledge SWEBOK）が DTR として承認された．

1.4.2　E- パスポートの標準化状況

SC 17/WG 3 国内主査　榊　純一

（1）標準化範囲

JTC 1/SC 17/WG 3（以下 WG 3 とする）は Machine Readable Travel Documents（機械可読旅行文書，以下 MRTD とする）の標準化を担当する作業部会であり，国際コンビーナは Joel Shaw 氏（加），セクレタリは Jacques Perron 氏（加）である．作業範囲には Passport（旅券），Visa（査証）および旅行記録などが含まれる．規格作成は International Civil Aviation Organization：（以下 ICAO とする）が主導的に行っており，WG 3 は ICAO の下部組織である ICAO-TAG-MRTD（Technical Advisory Group-Machine Readable Travel Documents）とリエゾン関係にある．ICAO における MRTD の規格（Doc 9303）は，ISO での Fast-track 投票を経て ISO/IEC 7501 となる（図 -2 参照）．

（2）ICAO と WG 3 の関係

WG 3 は Fast-track 投票においてコメントを提出することができるが，より積極的なかかわりを持つために WG 3 側メンバが ICAO の会議に加わるなどの方法により貢献を行っている．

（3）電子化の取組み

ICAO では 1990 年代の半ばより生体認証データを記録することが可能な方式による電子化を検討してきた．この標

準化原案は2003年6月に下記4つのICAO Technical Report（TR）としてWeb上で一般公開されている（http://www.icao.int/mrtd/Home/Index.cfm）.

- Biometrics deployment of MRTD：バイオメトリクスのMRTDへの応用に関する技術報告
- Use of Contactless Integrated Circuits：コンタクトレスICに関する技術報告
- Logical Data Structure（LDS）：カード内の論理データ構造に関する技術報告
- PKI Digital Signatures Tech Report：公開鍵基盤と電子署名に関する技術報告

これらTRは最終的にはDoc 9303に反映される予定だが，2004年中はTRの改定にとどまる予定である.

（4）TR開発状況

1）搭載する第一のバイオメトリクスとして顔画像，任意で指紋および虹彩を追加使用できる．バイオメトリクスデータはすべて任意であるが，米国は査証免除国に対してバイオメトリクスデータの記録を義務づけているため，日本を含めた査証免除国にとっては実質上顔データの記録が必須である.

2）記録方式はISO/IEC 14443（A型またはB型）が選択された.

3）顔データに関しては読み出し制限は基本的に設定されない見通し.

4）盗聴対策としてOCRデータを元に暗号通信する方式が任意で搭載可能.

5）改ざん防止対策としてすべての記録データに対して電子署名が採用されている.

6）電子署名や失効リストの配布方法などが今後の課題.

1.4.3 Linuxの国際規格化の検討

SC 22専門委員会 幹事　後藤志津雄

2002年11月のJTC 1総会で，Linux Study Group（LSG）を設置することが決まり，Linux関連技術の国際規格化の方針について検討することになった．日本のSC 22専門委員会は，親委員会の情報規格調査会技術委員会や経済産業省と連携してこれに対応してきた．2003年5月の英国LSG会議，9月のJTC1/SC 22総会などの会議のたびに寄書を出したほか，2004年2月には，日本でLinux Rapporteur Group会議を開催するなど，積極的にこれに関与した．その結果として，日本が希望した方向で，次の方針が決まった.

1）The Free Standards Group（FSG）が開発したLinux Standards Base（LSB）標準をFSGがPAS提案者となり国際規格として提案する.

2）日本がLinux関連の国際規格の候補として挙げた技術が中長期的課題として認知され，それらの技術の標準をオープンソースコミュニティが開発したものをPASなどで国際規格化する.

FSGは，JTC 1にPAS提案者の申請を行い，2003年11月に承認された．FSGから，2004年度早々にLSB標準のPAS提案が行われる予定である.

LSB標準以外の国際規格化候補については，その時期や方法が明確になっていない．2004年9月のSC 22総会などを通してこれから議論がされていく.

1.4.4 楕円曲線暗号の原理と国際規格について

SC 27/WG 2小委員会 委員　宮地充子

（1）はじめに

JTC 1/SC 27/WG 2では，情報セキュリティのアルゴリズムおよびプロトコルに関する国際規格の策定を進めている．その中の1つのプロジェクトである15946はcryptographic techniques based on elliptic curves（楕円曲線に基づく暗号手法）に関する国際規格を定める．15946は4つの技術から構成される．このたび，著者がプロジェクトエディタを務める15946-4の国際規格が完成し，15946の全4技術の国際規格が発行されることになった．本稿においては，楕円曲線暗号の原理について解説するとともに，国際規格となった15946-4を含む15946に関して解説する．楕円曲線暗号および暗号全般に関して，詳しく知りたい読者は文献1）を，また楕円曲線について興味を持たれた読者は，文献2）を読まれることをお薦めする.

（2）楕円曲線暗号

楕円曲線暗号とは，1985年に発表された楕円曲線上の離散対数問題（ECDLP）の難しさを安全性の根拠にする暗号である．一般に楕円曲線暗号とは，ECDLPに基づく公開鍵暗号の総称であり，メッセージの秘匿を実現する暗号，完全性を実現するディジタル署名，鍵共有法等の機能が実現できる．エルガマル暗号やDSA署名などの既存の有限体上の離散対数問題（DLP）を用いる暗号系は，すべて楕円曲線暗号に変換できる．ECDLPはDLPに対する強力な解法である指数計算法が直接適用できないことから，同じ安全性を高速かつコンパクトに実現できるとして，有望な公開鍵暗号系として盛んに研究されるようになった.

（a）楕円曲線暗号と有限体上の暗号の違い

楕円曲線暗号と有限体上の暗号にはプロトコル自体の大きな違いはない．基本的に有限体の元を楕円曲線の元に，有限体の乗法を楕円曲線の加法に対応させて，双方のプロトコルが実現できる．両者の大きな違いは，その安全性であるECDLPとDLP上の既存攻撃にある．DLPに対する攻撃である指数計算法やその改良は，すべてのDLPに準指数時間の攻撃を与える．このため，10^{12}MIPS年の安全性を確保するには1,024ビットほどの大きさの有限体が必要になる．一方ECDLPには，任意の楕円曲線に対して適用可能な準指数時間攻撃は提案されていない．この結果，指数時間攻撃しか存在しない楕円曲線が構成でき，現時点では160ビットほどの大きさで同じ安全性が実現できる.

（b）楕円曲線

暗号で利用する楕円曲線について簡単に述べる．楕円曲線とは，有限体F_p（$p \geqq 5$の素数）の元a，bに対して，

$$E: y^2 = x^3 + ax + b \quad (D = 4a^3 + 27b^2 \neq 0) \qquad (1)$$

で定まる曲線である．ここで$D = 4a^3 + 27b^2$は判別式と呼ばれる．楕円曲線は（1）を満たす点の集合であるが，$x \to \infty$のとき$y \to \infty$と考えて，無限遠点$o = (\infty, \infty)$もEの点になる．特に，楕円曲線のF_p-有理点の集合を，

$$E(F_p) = \{(x, y) \in F_p^2 \mid y^2 = x^3 + ax + b\} \cup \{o\}$$

で定める．楕円曲線のパラメータa，bを含む体F_pを楕円曲線Eの定義体と呼ぶ．楕円曲線にはoが零元になるような加法が定義でき，たかだか数回の定義体上の演算で実現できる．この加法により$E(F_p)$は有限可換群になり，暗号系が構成できることになる.

（c）楕円曲線暗号の例

具体的な楕円曲線暗号として楕円ディッフィ・ヘルマン鍵共有法について紹介する．楕円曲線暗号の安全性は，有限体F_p上の楕円曲線E/F_p上の離散対数問題（ECDLP）に基づく．ここで，ECDLPについて定義する.

定義 [ECDLP]

有限体F_p上の楕円曲線E/F_p, $E(F_p) \ni G, Y$に対して，

$$Y = xG = G + \cdots + G \quad (G \text{ の } x \text{ 回の和})$$

となるxが存在するなら，そのxを求めよ．　❖

ECDLPにおいて楕円曲線とその加法の代わりに有限体と

その乗法を用いる問題，すなわち $y=g^x$（mod p）より x を求める問題が DLP である．

以下 E/F_p を楕円曲線とし，$G \in E(F_p)$ を位数（$lG = O$ となる最小の正整数 l）が大きな素数 l の元とする．$E(F_p)$ および G はシステム内で共通に利用されるデータで，システムパラメータと呼ばれる．

ユーザ A の鍵生成

1. 乱数 $x_A \in \{1, \cdots, l-1\}$ を選ぶ．
2. $P_A = x_A G$ を計算する．
3. x_A を秘密鍵，P_A を公開鍵として出力する．

ユーザ B も同様に鍵（x_B, P_B）を生成する．

鍵共有

A と B が通信なしに，それぞれの公開鍵 P_A，P_B を利用して，鍵を共有する場合を考える．

1. A は公開ファイルから B の公開鍵 P_B を入手し，
   $K_{A,B} = x_A P_B = x_A x_B G$
   を計算する．
2. B は公開ファイルから A の公開鍵 P_A を入手し，
   $K_{B,A} = x_B P_A = x_B x_A G$
   を計算する．
3. A と B は E（K）の元 $K_{A,B} = K_{B,A}$ を鍵として共有する．

（3）国際規格 ISO/IEC 15946（楕円曲線に基づく暗号手法）について

楕円曲線に基づく暗号手法の国際規格を定める ISO/IEC 15946 は，General（楕円曲線全般）の規格（15946-1），Digital signatures（添付型署名）の規格（15946-2），Key establishment（鍵確立）の規格（15946-3），Digital signatures giving message recovery（メッセージ回復型署名）の規格（15946-4）の 4 つから構成される．15946-1，2，3 の各パートは 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，2004 年に国際規格となった，

15946-1 は楕円曲線暗号を実現する際に必要になる要素，楕円曲線のパラメータの生成方法やその検証方法，楕円曲線の元を整数に変換する方法等の規格である．付属書として，楕円曲線の各種加算公式も記載されている．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．15946-3 は楕円曲線を用いた鍵共有法の規格である．Key establishment の技術は Key agreement（鍵共有）と Key transport（鍵輸送）からなる．Key agreement においては，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あらかじめ決定できない．Key transport においては，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 Key establishment として，全 10 方式が規格化されている．15946-4 は楕円曲線を用いたメッセージ回復型署名の規格である．15946-2 ではメッセージのすべ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．本規格においてはメッセージ回復型署名具体的な方式として，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．

（4）おわりに

楕円曲線暗号は必要な安全性を小さな鍵サイズで実現できるため，有限体上の暗号より高速かつコンパクトに実現できる．今後，携帯電話などの携帯端末の高機能化に伴い，暗号機能の装備は必須となるだろう．このとき楕円曲線暗号のはたすべき役割は非常に大きい．また楕円曲線暗号の研究開発分野における日本の技術水準は非常に高い．本国際規格が楕円曲線暗号の普及への布石となり，高セキュリティ機能を掲載した端末が普及することを願う．

参考文献
1）宮地充子，菊池浩明 共編：情報セキュリティ，オーム社（2003）．
2）山本芳彦：現代数学への入門－数論入門 2 －，岩波書店（1996）．

1.4.5 メタモデル相互運用枠組み

SC 32/WG 2 小委員会 主査　堀内　一

（1）規格の背景

JTC 1/SC 32（データ交換と管理）の WG 2（メタデータ・レジストリ）は，データ要素の管理属性や命名規則，さらに登録法などに関する ISO/IEC 11179 規格の開発と維持を担当している．11179 規格は，すでに，8 年近く改定を繰り返して現在に至っている規格群である．一方，2002 年 5 月，新たなプロジェクト「メタモデル相互運用枠組み（Framework for Metamodel Interoperability：ISO/IEC 19763）」を，日本，中国，韓国，英国，およびカナダによる 5 カ国共同プロジェクトとして発足させた．ようやく，2003 年 10 月の WG 2 メルボルン会議で，規格の一部が CD 登録投票に入った段階である．なお，国内では，2003 年度より経済産業省の「国際規格共同開発事業」の 1 つとして推進中である．

（2）規格案の目的と構成

メタモデル相互運用枠組み規格（ISO/IEC 19763）案は 4 部構成の規格群である．各部とも，原則として 2 カ国の共同編集体制をとり，国際共同作業による規格成立を目指している．本規格案は，e ビジネスにおける企業間連携で求められるメタデータや業務モデルの共有に関するものである．各産業分野で，業界ごと企業ごとに構築される登録簿の，それぞれが具備するメタモデル（モデルを記述するモデル）の枠組みと記述方法，さらに登録方法の標準化を通じて，たとえば，ebXML，UBL，あるいは UDDI などの仕様に従って開発されるレジストリ（そのメタモデル）群の相互運用を期すものである．

本規格案の構成は次のようなものである．

第 1 部：参照モデル（日，英）
メタモデル枠組みの概念およびアーキテクチャを規定する．以下の第 2 部から第 4 部の規格開発に適用される．

第 2 部：コアモデル（日，韓）
メタモデル枠組みの中核部分（コアモデル）について規定する．メタモデル枠組み規格の開発に使われるメタモデル記述の機構，および規範的な構成要素を提供する．

第 3 部：オントロジーのためのメタモデル枠組み（加，中）
各種オントロジー・スキーマを登録するためのメタモデル枠組みを規定する．

第 4 部：モデルマッピングのためのメタモデル枠組み（日）
モデル間のマッピングの種類と規則を記述するためのメタモデル枠組みを規定する．

1.5 Management に関するトピックス

JTC 1 の今後の戦略に関する検討状況，SC 11 の SC 23 への統合，Linux SG の活動および JTC 1 Directives の第 5 版の発行について報告する．

1.5.1 JTC 1 の今後

（1）JTC 1 ビジネスプラン

JTC 1 シンガポール総会（2003 年 11 月開催）で ICT（Information and Communications Technology）分野において引き続き効率的に標準を開発すること，新たな標準化への

取組みに力を入れること，パートナー組織および必要に応じて他の組織とも協力して，産業界，ユーザ，消費者のニーズを満足する標準を開発するという戦略に沿う今後1年間のビジネスプランを決定した．

(2) JTC 1 長期ビジネスプラン（LTBP，LTMP Imp）

2002 年 10 月の JTC 1 ソフィア・アンティポリス総会で承認した長期ビジネスプランとその実現プランは有効であることがシンガポール総会でも確認され，プランに沿って活動を続けることとなった．

(3) SWG for Technology Watch と新規 Study Group の設置

(a) SWG for Technology Watch

ソフィア・アンティポリス総会で設置された特別ワーキンググループ（JTC 1 SWG for Technology Watch）の継続とカナダの Coallier 氏の議長継続を確認した．

(b) Web Services SG の設置

Web Services の標準化に関する JTC 1 の貢献戦略を検討するための Study Group（SG）の設置（議長 D. Deutsch（米），セクレタリ F. Coallier（加））を決定した．

Web Services SG の第 1 回会議が 2004 年 2 月にパリで米，仏，加，日等 9 カ国と W3C，OASIS，WS-I 等 Web Services の標準にかかわる 6 つのコンソーシアムが参加して開催され，JTC 1 とコンソーシアム間の協力関係強化に向けて具体化することが提案された．その第 2 回会議を 6 月にモントリオールで開催し，次回 JTC 1 総会（2004 年 10 月）で活動結果が報告される．

(c) Privacy Technology SG の設置

Privacy Technology（プライバシポリシ，プロセス，システム）の標準化に関する JTC 1 の貢献戦略を検討するための SG の設置（議長 J. Hopkinson（加））を決定した．6 月にモントリオールで第 1 回の会議が開催され，次回 JTC 1 総会（2004 年 10 月）で活動結果が報告される．

1.5.2 JTC 1/SC 11 の JTC1/SC 23 への統合

2002 年末に JTC 1/SC 11（磁気記録関係を担当）の幹事国と議長を担当していた米国がそれらの担当を終了したいとの意向を表明したが，SC 11 の解散は日本の磁気テープ業界に対する影響が大きいことと，今後も磁気記録関係の規格が作成される可能性が残っているなどの理由で日本としては存続を希望した．しかしながら SC 11 単独で運営するほどの規格作業量も見込めないため，SC 11 と SC 23 を合併して新 SC 23 を作ることを 11 月の JTC 1 シンガポール総会に日本案として提案し，了承された．

1.5.3 JTC 1 Directives 第 5 版の発行

1998 年に第 4 版が発行されてから 5 年以上経過してやっと第 5 版（JTC 1N7364）が 2004 年 2 月初めに公開された．

第 4 版に対して，修正・追加された主な項目は以下の通りである．

- PAS 手続きの追加（14 章および Annex M）．
- Stabilized Standard の追加（維持しておくことが必要で，5 年見直しは不要）．
- 開発設定期間を ISO と同じく 36 カ月とした（短期は 24 カ月，理由がある場合 48 カ月）．
- Workshop Mode of Operation の追加（Annex L）．
- 国際標準以外の仕様の Normative References 記載へのガイドラインの追加（Annex N）．

その他，日本提案の手続きを明確化した NP の修正も行われている．

2. 日本の対応

2.1 国際活動における日本の主な役割

日本が担当する役職数は，欧州諸国に比肩する規模を維持している．

(1) 議長，コンビーナ，ラポータ

SC 2，SC 23，SC 28，SC 29 の議長，SC 7/WG 6，SC 22/WG 16，SC 32/WG 4，SC 34/WG 2，SC 35/WG 2，SC 35/WG 4，SC 36/WG 2 のコンビーナ，SC 29/WG 1/JBIG，SC 31/WG 4/Application のラポータを担当した．

(2) プロジェクトエディタ

SC 6（6 名），SC 7（11 名），SC 11（9 名），SC 22（1 名），SC 23（9 名），SC 27（4 名），SC 29（34 名），SC 31（1 名），SC 32（5 名），SC 34（8 名），SC 35（3 名），SC 36（2 名）の計 93 名（プロジェクト数 166）であった．

(3) 幹事国

SC 2（当調査会），SC 7/WG 6（当調査会），SC 23（当調査会），SC 28（JBMIA），SC 29（当調査会），SC 36/WG 2（当調査会）の 6 つの国際事務局を担当した．

2.2 国内委員会の活動

2.2.1 委員会等の開催状況

事業執行に関しては，規格総会，規格役員会，運営委員会，広報委員会および表彰委員会を計 35 回開催した．技術活動のうち，JTC 1 全体に関する事項は，技術委員会，技術委員会／幹事会および DIS 等調整委員会で対応し，SC への対応は，専門委員会と関連する小委員会等が担当した．技術活動関係の委員会開催回数は，計 454 回であった．技術委員会以下の委員の総数は，重複を含めて 1,200 名，オブザーバは 194 名，メールメンバは 5 名であった（議長／委員長は**表 -3** 参照）．

2.2.2 各専門委員会の活動の概況

(1) 第 1 種専門委員会関係

JTC 1 の組織変更等に対応して，国内委員会の組織の変更を行った．

- SC 6 専門委員会：作業課題の変更に対応して無線 LAN SG を WG 1 小委員会に統合した．
- SC 34 専門委員会：国際 WG 3 の活動が活発になってきたのに対応して，国内に WG 3 小委員会を設立した．
- SC 37 専門委員会：作業項目の目処がついたのに伴い，SC 37 総会（2003 年 9 月）で，SG 1 から SG 6 を解散して WG 1 から WG 6 を設立したのに呼応して，国内も同様に組織変更を行った．

(2) 第 2 種専門委員会関係

- 学会試行標準専門委員会：新たに 4 件の NP が承認され，また，7 件の学会試行標準が完成し，当調査会のホームページで公開することが承認された．
- 文字情報データベース専門委員会（汎用電子情報交換環境整備プログラム）：文字情報収集システムについて法務省から提供された約 56,000 文字の整備体系化に対応できるような機能改善，文字情報公開システムについては試験公開の開始が大きな目標で，これらの両方が円滑に遂行するため今年度は 4 回開催した．
- メタモデル相互運用枠組み標準化専門委員会：経済産業省から受託した「メタモデル相互運用枠組み」に関する国際規格共同開発事業を円滑に遂行するため 2003 年 5 月に設立し，今年度は 10 回開催した．
- 光ディスク用語専門委員会：光ディスクに関する用語を整理し，その結果を学会試行標準の「情報技術用語データベース」に反映するため 2003 年 4 月に設立した．

(3) 第 3 種専門委員会関係

次の 2 つの委員会を設けて活動した．

- C# 言語仕様 JIS 原案作成委員会：ISO/IEC 23270 JIS 原案作成
- プログラム言語 COBOL JIS 改正原案作成委員会：JIS X 3002 の改正原案作成

委員会（タイトル）	議長／委員長
技術委員会関係	
技術委員会（情報技術）	石崎　俊
技術委員会／幹事会	石崎　俊
DIS 等調整委員会	村谷　公俊
第１種専門委員会関係	
SC 2　（符号化文字集合）	大蒔　和仁
SC 6　（通信とシステム間の情報交換）	今井　和雄
SC 7　（ソフトウェア技術）	山本　喜一
SC 11（フレキシブル磁気媒体）	荒木　学
SC 17（カードおよび個人識別）【ビジネス機械・情報システム産業協会担当】	大山　永昭
SC 22（プログラム言語，その環境およびシステムソフトウェアインタフェース）	筧　捷彦
SC 23（情報交換用光ディスクカートリッジ）	田中　邦麿
SC 24（コンピュータグラフィクスおよびイメージ処理）	藤村　是明
SC 25（情報機器間の相互接続）	山本　和幸
SC 27（セキュリティ技術）	宝木　和夫
SC 28（オフィス機器）【ビジネス機械・情報システム産業協会担当】	山田　尚勇
SC 29（音声，画像，マルチメディア，ハイパーメディア情報符号化）	小林　直樹
SC 31（自動識別およびデータ取得技術）	柴田　彰
SC 32（データ管理および交換）	芝野　耕司
SC 34（文書の記述と処理の言語）	小町　祐史
SC 35（ユーザインタフェース）	山本　喜一
SC 36（学習，教育，研修のための情報技術）	仲林　清
SC 37（バイオメトリクス）	瀬戸　洋一
第２種専門委員会	
学会試行標準	石崎　俊
光ディスク用語	金沢　安矩
メタモデル	堀内　一
文字情報データベース	石崎　俊
第３種専門委員会	
C# 言語仕様 JIS 原案作成	黒川　利明
プログラム言語 COBOL JIS 改正	今城　哲二
その他	
ISO 2375 登録	三上　喜貴

表 -3　技術活動関係委員会

2.2.3　国際会議への参加

2003 年度は 238 回の会議が開催されたが，うち 209 回の会議に日本から 853 名が参加した（うち外国開催 205 回，日本からの参加者 828 名）．なお，当調査会がホストとなり日本で開催したものは**表 -4** に示す 4 回であった．

2.3　情報技術標準化フォーラムの開催

規格賛助員を対象としての講演会を 2003 年度は，5 回開催した．その概要を以下に報告する．

2.3.1　バイオメトリクス技術の国際標準化に対する産業界の取組み

開催日：2003 年 7 月 19 日

講師：瀬戸洋一（日立）

参加人数：42 名

概要：2001 年 9 月 11 日に発生した米国同時多発テロを境に，ホームランドセキュリティの観点からバイオメトリック技術の見直しが起こり，出入国管理への導入が始まった．米国においては 2004 年の 1 月より顔，指紋の登録が入国の際，行われている．また，ユビキタスネットワーキングにおける端末の個人認証などの観点から自国の産業の指導権を握るため，技術の標準化を戦略的に行う動きがでてきた．たとえば，電子パスポートに代表されるように，その利用は 1 つの組織内ではなく，人の活動とともに世界中に広まっている．つまり相互接続性，精度評価などの共通認識が重要となっている．この意味で JTC 1/SC 37 の設置はタイムリであり，重要な意味を持つ．JTC 1/SC 37 は，正式には 2003 年 9 月のローマ総会で WG の設置が決まり本格的な活動を開始した．WG は，用語から社会倫理までを扱うため 6 つの組織で構成されている．日本国内も SC 37 専門委員会の発足に併せ，2003 年に産業コンソーシアムの設置，学会研究会の設置が相次いで行われ，新市場の創出，国際標準化対応の強化のための体制が整備された．

開催会議名	開催期間（開催地）	出席者（うち日本出席者）
SC 32（データ管理および交換）/WG 1（開放型 edi）	2003-06-23/27（小樽）	7（ 2）
SC 29（音声，画像，マルチメディア，ハイパーメディア情報符号化）/WG 1（静止画像符号化）/JBIG Ad hoc	2003-07-15/16（東京）	5（ 4）
SC 29（音声，画像，マルチメディア，ハイパーメディア情報符号化）/WG 1（静止画像符号化）/JBIG SG	2003-12-09/10（東京）	3（ 2）
SC 22（プログラム言語，その環境およびシステムソフトウェアインタフェース）/Linux RG	2003-02-03/05（東京）	35（17）
		50 名（25 名）

表 -4　日本で開催した国際会議（2003 年度）

2.3.2　UN/CEFACT の e ビジネス戦略説明・討論会

開催日：2003 年 9 月 11 日

講師：Ray Walker（UN/CEFACT 運営グループ議長），Klaus-Dieter Naujok（UN/CEFACT 技術と方法論グループ議長），伊東健二（UN/CEFACT 運営グループ副議長）

参加人数：35 名

概要：UN/CEFACT（国連・貿易簡易化と電子ビジネスセンタ）は，政府，商業，産業のための電子商取引に関する国際標準の開発を先導している機関である．米国の OASIS とともに ebXML（企業間商取引［BtoB］向けの XML 規格）仕様を策定したことでも有名である．UN/CEFACT では，BCF（Business Collaboration Framework）と呼ばれる新たなモデル化の枠組みを中心とした e ビジネス戦略の普及を目的として，UN/CEFACT の幹部が，香港，東京，ソウルと巡回説明会を展開している．電子商取引，あるいはビジネスプロセスモデリングに関心を持つ日本の情報技術標準化関係者や学術有識者にその戦略を説明し討議の機会を設けた．

2.3.3　MPEG 符号化コンテンツの保護・配信形式の国際標準化動向説明会

開催日：2003 年 9 月 19 日

講師：Leonardo Chiariglione（JTC 1/SC 29/WG 11 コンビーナ），金子　格（早大，SC 29/WG 11/MPEG 知財コンテンツ情報小委員会主査），Ji Ming（PSL 研究所，ISO/IEC 13818-1:2000/AMD2 MPEG-2/IPMP エディタ），Dr. Xin Wang（ContentGuard 社，ISO/IEC 21000-5 MPEG-21 Part 5 エディタ），Craig Shultz（ISO/IEC 14496-1:2001/AMD3

MPEG-4/IPMP エディタ）
参加人数：89 名
概要：JTC 1/SC 29 の WG 11 MPEG 作業グループ（MPEG 国際標準化を担当）では，2003 年に MPEG 符号化コンテンツの配信に関する国際標準を相次いで完成させた．MPEG-2/IPMP および MPEG-4/IPMPX は，MPEG-2，MPEG-4 コンテンツにさまざまなコンテンツ保護方式の付随データを付与する際の汎用的な方法を規定している．本標準を利用すると，MPEG 符号化データに MPEG 規格外の個別のコンテンツ保護形式を用いるのに比べ，MPEG-4 システムなどの多重化方式との整合性が高まり，端末および通信システム間の相互運用性が向上する．MPEG-21 ではコンテンツ保護や配信ビジネスに必要なさまざまな付随データ用のフレームワークを規定している．その主要部分は，コンテンツ利用システムの非常に抽象化，一般化された「モデル」と，その各インタフェースの XML スキーマ記述である．ネットワークベースのコンテンツ利用が主流となる時代に備え，これらの規格を利用するメリットと規格の概要を説明した．

2.3.4 標準化活動の新展望

開催日：2003 年 11 月 10 日
講師：John Hill（Sun Microsystems，JTC 1/SC 22 議長）
参加人数：28 名
概要：情報規格の標準化は，1 つの曲がり角に差しかかっている．昨年，米国では，情報技術産業諮問会（IT Industry Council），商務省（Department of Commerce）および MIT の呼びかけで，IT 産業の CEO，CIO を招いて，情報規格の標準化活動に関する問題点を探る会議が 2 日間にわたって開かれた．Sun Microsystems はこの会議を資金的に後援した．そこで取り上げられたのは，次の 5 つの点であった．（1）組織・構造，（2）政府の役割，（3）経済，（4）知的財産権，（5）教育．この 5 点にわたって，何が問題であり，どんな解決策が考えられるかをこの会議での結論を踏まえて紹介した．同時に，Sun Microsystem が複数の組織と共同して開始した，問題の抽出やデータの収集，そして改善に向けての諸活動も紹介した．

2.3.5 ソフトウェア工学国際標準化による競争力強化

開催日：2003 年 12 月 2 日
講師：Francois Coallier（Ecole de technologie superieure，JTC 1/SC 7 議長），勝亦眞人（経済産業省），東　基衛（早大，JTC 1/SC 7/WG 6 コンビーナ）
参加人数：80 名
概要：ソフトウェア工学の国際標準化は，プロダクト規格とともにプロセス規格へのシフトが強調されてきているが，この両者をバランスよく適用することが高い信頼性を持つソフトウェアの開発には不可欠である．また，近年の組込みソフトウェアの重要性の増大に伴い，ソフトウェア工学ばかりでなくシステム工学の視点を取り入れた，新たなソフトウェア工学への取組みも必要不可欠となってきている．JTC 1/SC 7 議長である Francois Coallier 教授が来日する機会を得て，国内のソフトウェアを開発している産業の関係者に SC 7 における国際標準化の動向を広報するとともに，国内企業がソフトウェア製品の生産性，品質および信頼性を向上するためには，これらの規格をどのように利用すればよいのかを知らしめることを狙いとしてこのフォーラムを開催した．現在，国内のソフトウェア関連産業界においては，残念ながらソフトウェアの品質向上への責任感，およびそれに関連した国際標準化活動への理解はきわめて低いといわざるを得ない．このため，あらゆる機会を捉えて広く呼びかける必要があると考え，今回の講演会もその一環と捉えて開催した．

2.4 学会の全国大会における標準化活動の紹介

学会の会員が標準化活動について理解を深め，また標準化活動への参加を促進する目的で，2001 年 3 月の全国大会から標準化セッションを開催しているが，2003 年度は 2004 年 3 月に慶應義塾大学湘南藤沢キャンパスで開催された全国大会で，SC 6 専門委員会と SC 28 国内委員会が具体的な標準化活動の紹介を行った．

3. その他

3.1 情報規格調査会の表彰

当調査会事業に関連して，顕著な功績あるいは貢献があった者を，2003 年 7 月 18 日に開催した規格総会で表彰した．氏名の後の括弧内は表彰時点の所属を表す．

1）標準化功績賞：2 名
近藤昭弘（日立），斎藤　輝（日本 IBM）
2）標準化貢献賞：12 名
青野雅樹（日本 IBM），小林龍生（ジャストシステム），櫻井幸一（九大），菅谷寿鴻（東芝），杉山秀紀（日本 IBM），助田裕史（日立），鈴木健司（東京国際大），谷津行穂（日本 IBM），中尾好秀（シャープ），西村和夫（駒澤大），宮地充子（北陸先端科学技術大学院大），室中健司（富士通）

3.2 NEWSLETTER 発行

「情報技術標準 NEWSLETTER」：季刊誌（年 4 回）および別冊（年 1 回）を発行した．

3.3 プレスリリース

- MPEG 符号化コンテンツの保護・配信形式の国際標準化動向説明会（2003 年 8 月 28 日）
- ISO/IEC JTC 1/SC 29 が第 1 回アイカー賞を受賞（2003 年 10 月 15 日）
- ソフトウェア工学国際標準による競争力強化－ ISO/IEC JTC 1/SC 7 の国際標準イニシアティブと標準化政策についての日本政府の対応（2003 年 11 月 6 日）

4. むすび

2003 年度の標準開発の活動状況についてその一端を報告した．特に，最近新聞でも話題となっているバイオメトリクスを導入した E- パスポートを外務省は 2005 年から導入を始めると発表している．また，暗号についても，2003 年 3 月に電子政府が推奨暗号リストを公表しており，IT 技術が応用面でも浸透が始まってきている．これらには日本の関係者が多く活躍しており，国際標準への貢献が著しい．

さらに，マネジメント面では，2001 年から JTC 1 の将来に関する議論から，これまでの事業および周辺技術について，Technology Watch というロードマップを作成し，取り組むべき新規技術分野について議論してきた成果が徐々に現れてきた状況である．Linux に関する標準化の取組み，Web サービス，プライバシー技術に関する調査がその成果である．今後もいくつかのテーマが取り上げられることになると思われる．

情報規格調査会は，上記のような活動に対し，国際・国内の両面で活動を支援・展開している．

また，新たに学会試行標準も 2 件が追加され，その一部が国際提案へとその活動が広がっている．

このような活動を学会会員の皆様に広く理解していただくために，春の情報処理学会全国大会・標準化セッションでの活動報告，プレスリリース発行などの広報活動に努力している．今後も，学会との密接な情報交換を行い，共存共栄をはかっていきたいので，学会会員の方々の一層のご支援ご協力をよろしくお願いいたします．