

金融情報技術の国際標準化について

2006 年 10 月

金 融 研 究 所

目 次

要 旨

1. はじめに
2. 国際標準化の枠組み
 - (1) 標準化の目的
 - (2) 標準・規格の分類
 - (3) 国際標準化のための組織
 - (4) 国際標準化の進め方
3. 金融情報技術に関する国際標準化活動
 - (1) I S O / T C 68 の概要
 - (2) I S O / T C 68 に対応する国内の取組み
4. 金融情報技術の国際標準化を巡る最近の話題
 - (1) 暗号アルゴリズムの 2010 年問題と金融業界への影響
 - (2) 金融機関の情報セキュリティ対策に関する国際標準化
 - (3) 金融業務における通信メッセージ等に関する国際標準化
5. おわりに

金融機関同士が円滑に金融取引を行うためには、取引に用いられる手順や様式が「標準化」されていることが重要である。金融のシステム化が進んだ現代においては、金融業務における標準化の対象は、従来の紙とペンを用いるものから、通信メッセージ・フォーマットやコード体系といった情報通信技術や、暗号技術、ＩＣカード、生体認証技術といった情報セキュリティ技術に移ってきている。こうした金融情報技術の標準化を推進していくことは、単に金融機関の情報システムが相互に接続可能となるだけでなく、金融取引における不要な多様性を排除し、金融機関の事務合理化や顧客の安全性、利便性の向上にも資するものである。

わが国の金融業界においては、従来は、国内・業界内のみを適用領域とする標準化が主流であったが、最近では、情報技術革新に伴う内外市場の統合化、金融の国際化の影響を受けて、金融情報技術に関する国際標準化への認識が高まりつつある。

金融情報技術の国際標準化は、国際標準化機構（ＩＳＯ）の専門委員会の１つである金融サービス専門委員会（ＴＣ６８）において行われている。日本銀行は、ＩＳＯ／ＴＣ６８の日本における事務局を務めており、国内の銀行、証券会社等が構成メンバーとなったＩＳＯ／ＴＣ６８国内委員会を定期的開催しているほか、関連する国際会議への出席や、国内意見の取り纏めを行っている。

現在、ＩＳＯ／ＴＣ６８では、様々な領域の金融情報技術についての国際標準化が進められているが、とりわけ注目されるのが、金融取引の安全性を確保する情報セキュリティ技術にかかる国際標準化である。金融機関の情報システムにおいては、取引情報の機密性と完全性を確保するために、様々な暗号技術が利用されているが、現在利用されている暗号アルゴリズムの多くは、近年の暗号解読技術やコンピュータ技術の急速な進歩を背景に、2010年頃にはその安全性が低下してしまうことが指摘されている（暗号アルゴリズムの2010年問題）。ＩＳＯ／ＴＣ６８では、日本からの提案を受けて新たなスタディ・グループを組成し、金融分野で利用される暗号の強度についての検討を進め、2010年問題に対する推奨対応策を取り纏めた。既に制定された規格やガイドラインに規定されている暗号アルゴリズムについても、今後、必要な見直しが行われ、より強度の高い暗号アルゴリズムが推奨されることとなっている。

このほか、金融分野で公開鍵基盤（ＰＫＩ）を利用する際に、金融機関が認証機関を運営する場合の注意事項や、金融機関が生体認証技術を利用する場合のシステム設計上の留意点等についても、ＩＳＯ／ＴＣ６８のもとで国際標準化が進められている。

また、銀行や証券会社が利用する通信メッセージ・フォーマットについても、従来の固定長のメッセージに代わって、拡張性に優れたXMLを利用する新たな国際標準の体系が整備されてきている。欧米では、この新しい国際標準を積極的に利用して、銀行取引や証券取引のイノベーションに取り組む動きがみられ始めている。

今後、わが国においても、情報通信ネットワークを利用した国際的な金融ビジネスを展開するうえでの国際競争力を高めていくために、金融情報技術に関する国際標準化動向への理解を深めておくことが、ますます重要となってくるものと考えられる。日本銀行としても、ISO/TC68の国内事務局を務める立場から、金融情報技術に関する国際標準化の動きを適切にフォローするとともに、関連情報を積極的に国内に還元していくことにより、そうした理解の深化に貢献していきたいと考えている。

1. はじめに

金融機関同士が相互に円滑に金融取引を行うためには、取引に用いられる手順や様式が「標準化」されていることが重要である。かつて、金融業務が主として紙とペンを用いて行われていた時代には、手形、小切手の様式や各種帳票類が標準化の対象となっていたが、その後、金融業務がコンピュータ・ネットワークを經由してシステムの処理されるようになると、通信メッセージ・フォーマット、コード体系等の情報通信技術が新たな標準化の対象に加わった。さらに、電子化された金融取引においては、その安全性を確保するために様々な情報セキュリティ技術を活用する必要があるが、暗号技術、ICカード、生体認証技術等、情報セキュリティを確保するための様々な情報技術も、金融機関における標準化の対象となった。これらの金融情報技術に関する標準化を推進することは、単に金融機関の情報システムが相互に接続可能となるだけではなく、金融機関の事務合理化や顧客の安全性、利便性向上にも資するものである。

わが国の金融業界においても、こうした標準化の取組みは進められてきたが、それは国内・業界内を念頭に置いた「国内標準化」が中心であった。わが国の金融機関では、国際的な金融取引を担当する一部の部署を除けば、もともと使用する言語の壁等もあって、海外の業務システムとの互換性や整合性といった観点はあまり重視されて来なかったからである。ところが、情報技術革新に伴う内外市場の統合化、金融の国際化の影響を受けて、近年、わが国の金融業界においても、金融情報技術に関する「国際標準化」に対する認識が高まってきている。例えば、ISO 27000に基づく、情報セキュリティマネジメントシステムに関するISO認証の取

得が進んでいるのは、その一例である。わが国の金融機関は、今後、海外の金融機関との調和や、業務の整合性を確保する観点から、金融情報技術の国際標準化を意識していくことが必要と考えられる。

日本銀行は、こうした金融情報技術の国際標準化を担当する国際標準化機構・金融サービス専門委員会（ISO/TC68）の日本における事務局を務めている。本稿では、日本銀行における国際標準化活動を通じて得られた情報を基に、ISO/TC68における金融情報技術の国際標準化活動の枠組みと、そこで制定された主な国際標準について、最近の関連するエピソードを交えつつ紹介する。

2. 国際標準化の枠組み

（1）標準化の目的

標準化とは、「規格の制定と認証を通じ、自由に放置すれば多様化、複雑化、無秩序化するものや事柄を、関係者のコンセンサスにより、少数化、単純化、秩序化を図る活動」と定義されている（JISC [1998]）。一般的には、「標準」あるいは「規格」と呼ばれる技術文書を策定し、それを普及させることにより、標準化が達成される。

こうした標準化の目的としては、以下のような点が挙げられる。

① 関係者の相互理解を深める

用語、単位、記号などの規格により、広く情報伝達の手段として相互理解を促進する。

② 互換性やインターフェースを確保する

製品・システムなどにおいて、相互に接続される箇所における関係を合理化する。近年

は、システムや情報処理などソフトウェア面で、インターフェースにおける両立性が重視されている。

③ 不必要な多様性の調整を通じて、生産効率の向上を図る

多様化したニーズを満たしつつ、製品、プロセス、サービスの形式やサイズなどの種類を最適に抑え、産業活動を合理化する。

④ 性能や品質の明示により消費者の利益を確保する

製品、プロセス、サービスの内容を明確に表示することにより、消費者が誤解なく適切なものを選定できるようにする。

標準化の対象としては、従来は「モノ（製品）」や「サービス」に関する各種規格の制定が中心に行われていたが、1990 年前後からは、ISO 9000（品質マネジメントシステム）やISO 14000（環境マネジメントシステム）、最近では、ISO 27000（情報セキュリティマネジメントシステム）等の「プロセス（方法）」に関する標準化が活発に進められている。

（2）標準・規格の分類

「標準」あるいは「規格」には様々な種類のものがあり、その影響範囲や策定手続きの違い等によって、一般に次のような分類がされている。

（強制力による分類）

遵守することが法規などにより強制されてい

るものは「強制規格」、遵守することが任意のものは「任意規格」と呼ばれる。「強制規格」の例としては、電気用品安全法、道路運送車両法、薬事法等の法令で定められている電気製品、自動車、薬品等の安全基準が挙げられる。ISO やJISなどで規定されている国際標準、国内標準は、一般にはそれ自体が遵守を強制されるものではないため、「任意規格」に分類される。

（標準化策定手続きによる分類）

「デジュール標準(de jure standard、公的な標準)」とは、ISO、JIS、JAS等、公的な標準化機関により、透明性の高いプロセスで、関係国/関係企業のコンセンサスに基づいて制定された標準をいう。これに対し、「デファクト標準(de facto standard、事実上の標準)」とは、標準を巡る競争が市場で行われ、その結果、標準が事実上決定されたものをいう。

（適用領域による分類）

デジュール標準は、標準を策定した標準化機関の性格によって、適用される地理的な領域が異なってくる。当該標準化機関が想定している適用領域が、世界全体か、特定の地域か、特定の国か等によって、それぞれ、「国際標準」、「地域標準」、「国内標準」等と呼称されることが多い。

（3）国際標準化のための組織

金融情報技術の国際標準化は、ISO^(注1)（国際標準化機構）の活動の一部として行われている。

ISOは、「物質及びサービスの国際交換を容易にし、知的、科学的、技術的及び経済的活

（注 1）ISO: ISOは「平等・等しい」を意味するギリシャ語 (isos) に由来する言葉である。国際標準化機構を加盟各国の言葉に翻訳して、その略語を利用した場合、例えば英語ではIOS (International Organization for Standardization)、フランス語ではOIN (Organisation Internationale de Normalisation) などと各国異なった略語表現が氾濫する恐れがある。このため、どの国においても同一表現となるように国際標準化機構の組織略称をISOとしている。

動分野における国際間の協力を助長するために世界的な標準化及びその関連活動の発展開発を図ること」を目的として、1947年に設立された。本部はスイスのジュネーブにあり、どの国にも属さない非政府組織である。ISOへの参加は、各国の最も代表的な標準化機関が、会員団体（member body）として、1機関だけ加入できることになっており、現時点で157カ国の代表機

関が加入している。わが国からは、日本工業標準調査会（JISC）が1952年に加入している（主要国のISO会員団体については、BOX1参照）。

なお、国際標準を制定する代表的な国際標準化機関としては、ISO以外に、電気・電子技術分野を担当するIEC^{（注2）}、および通信分野を担当するITU^{（注3）}がある。

[BOX1]

主要国のISO会員団体

| 名称（略称） | 概要 |
|---|---|
| 米国規格協会 (ANSI: American National Standards Institute) | 1918年に設立された米国の代表的な標準化機関。規格の作成自体は行わず、他の公認標準機関（ASO: Accredited Standards Organization）で作成された規格案を審議し、米国国家規格（ANSI規格）として制定している。現時点で、約11,000件のANSI規格が制定されている。 |
| 英国規格協会 (BSI: British Standards Institution) | 1901年に設立された英国の代表的な標準化機関。規格の開発・制定のほか、審査登録業務を行っている。同協会で制定された英国国家規格はBS規格と呼ばれている。現時点で、約20,000件のBS規格が制定されている。 |
| フランス規格協会 (AFNOR: Association Française de Normalisation) | 1926年に設立されたフランスの代表的な標準化機関。同協会で制定されたフランス国家規格はNF規格と呼ばれている。現時点で、約31,000件のNF規格が制定されている。 |
| ドイツ規格協会 (DIN: Deutsches Institut für Normung e. V.) | 1917年に設立されたドイツの代表的な標準化機関。同協会により制定・発行された規格はドイツ工業規格（DIN規格）と呼ばれている。2002年時点で、約27,000件のDIN規格が制定されている。 |
| 日本工業標準調査会 (JISC: Japan Industrial Standards Committee) | 工業標準化法に基づき設置された諮問機関であり、日本工業規格（JIS規格）の制定を行っている。その事務局業務は、経済産業省産業技術環境局基準認証ユニットが担当している。現時点で、約9,700件のJIS規格が制定されている。 |

（注2）IEC（International Electrotechnical Commission＜国際電気標準会議＞）：電気、電子、通信、原子力などの分野で各国の標準規格の調整を行う国際機関。1906年に設立され、電気・電子技術分野の国際標準化を担当している（本拠地：スイス・ジュネーブ）。

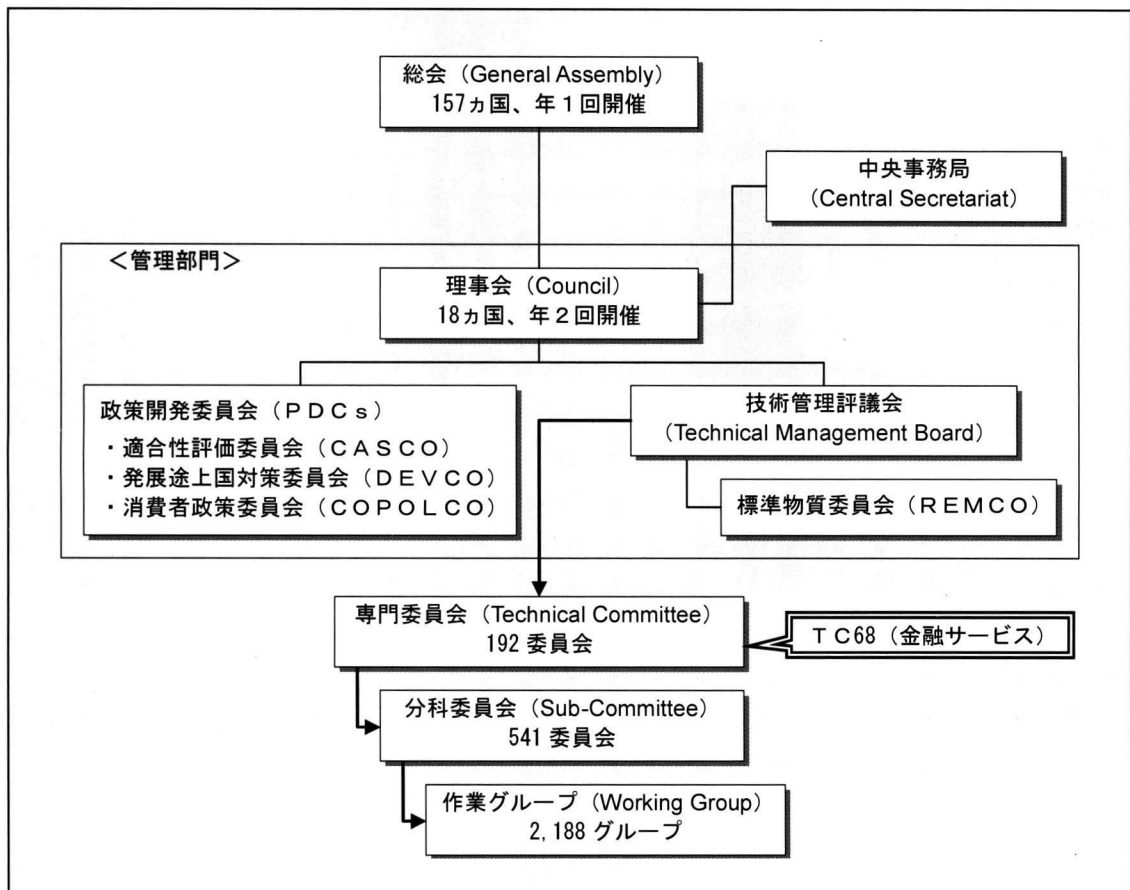
（注3）ITU（International Telecommunication Union＜国際電気通信連合＞）：1865年創設の万国電信連合と1906年創設の国際無線電信連合が1932年に合体した組織である。電気通信に関する制度の検討、電気通信技術の標準化、電気通信サービスの運用に必要な情報収集・周知、電気通信インフラの開発・推進等を目的として設立された国際連合（UN）の専門機関の1つ（本拠地：スイス・ジュネーブ）。

I S Oの標準化担当分野は、機械、化学、材料、建築等多岐にわたっており、分野ごとに専門委員会（T C : Technical Committee）が設置されている。T Cについては、設置順にT C 1（ねじ）からT C 229（ナノテクノロジー）まで 229の委員会が設置されているが、現時点で活動中のものは 192 の委員会である。金融情報技術の国際標準化は、T Cの1つであるT C 68 におい

て行われている。

T Cの配下には、実際の標準化作業を担当する分科委員会（S C : Sub-Committee）が、さらにS Cの配下には、国際規格の原案を検討する作業グループ（W G : Working Group）が設置され、各担当分野において審議が行われている。現在、S Cは 541 の委員会が、またW Gは 2, 188 のグループが活動している（図表 1 参照）。

（図表 1）I S Oの組織図



(4) 国際標準化の進め方

I S Oの国際規格は、通常、6段階の策定プロセスを経て作成される^(注4)。各標準化プロジェクトは委員会(T CまたはS C)において、下記の段階(ステージ)に従って標準化が進められ、最終的にI S(国際規格)として発行される(図表2参照)。

① 第1段階：提案段階(Proposal Stage)

新たな国際規格の制定を希望する「参加国」等は、「NP: New work item Proposal(新業務項目提案)」を提案することができる。NPは、電子メールによる投票、もしくはS C年次総会の決議により、Pメンバー^(注5)の参加国の過半数による同意が得られ、かつ最低5ヵ国以上が、当該規格策定プロジェクトの推進に積極的に参加する意向を表明した場合に承認される。NPによる新しいプロジェクトが承認されると、プロジェクト・リーダーが任命される。

② 第2段階：作成段階(Preparatory Stage)

通常、委員会によって、プロジェクト・リーダーが議長(コンビナー)を務める専門家の作業グループが設けられ、「WD: Working Draft(作業原案)」の作成が進められる。WDの作成作業が完了すると、委員会に回付され、「CD: Committee Draft(委員会原案)」としてI S O中央事務局に登録される。

③ 第3段階：委員会段階(Committee Stage)

CDは、賛否の意見を問うため、委員会のすべての参加国(PメンバーおよびOメンバー)に回付され、その結果について会議で審議を行い、また必要な場合には電子メールによる投票を行う。技術的内容について、コンセンサスに達するまで、繰り返しCDを検討し続ける。コンセンサスが得られた場合、またはPメンバーによる投票で2/3以上の賛成が得られた場合には、「DIS: Draft International Standard(照会原案)」としてI S O中央事務局に登録される。

④ 第4段階：照会段階(Enquiry Stage)

I S O中央事務局は、DISをすべての参加国(PメンバーおよびOメンバー)に電子的に回付して、5ヵ月以内に投票とコメントを求める。委員会の審議に参加する国の2/3以上が賛成して、かつ反対が投票総数の1/4以下であれば、「FDIS: Final Draft International Standard(最終国際規格案)」としてI S O中央事務局に登録される。承認基準に達しなかった場合は、さらに検討を加えるように原案を委員会に差し戻し、改訂された文書は再度DISとして投票とコメントを求めて、電子的に回付される。

⑤ 第5段階：承認段階(Approval Stage)

I S O中央事務局は、FDISをすべての参加国(PメンバーおよびOメンバー)に電子

(注4) 既に国内標準、業界標準として広く利用されている等、実績のある規格については、ファースト・トラック手順(迅速手順)を適用して、途中段階の審議・投票手続きを省略し、直接、照会原案(DIS)や最終国際規格案(FDIS)として提出することにより、短期間で国際標準化を行う場合もある。

(注5) Pメンバー(Participating member): 投票権を有する参加国のこと。I S Oの標準化作業に参加することができる。また、標準化作業におけるすべての審議案件、および国際規格の原案について、その国を代表して賛否を表明する義務がある。これに対して、投票権を持たない参加国をOメンバー(Observer member)と呼んでいる。

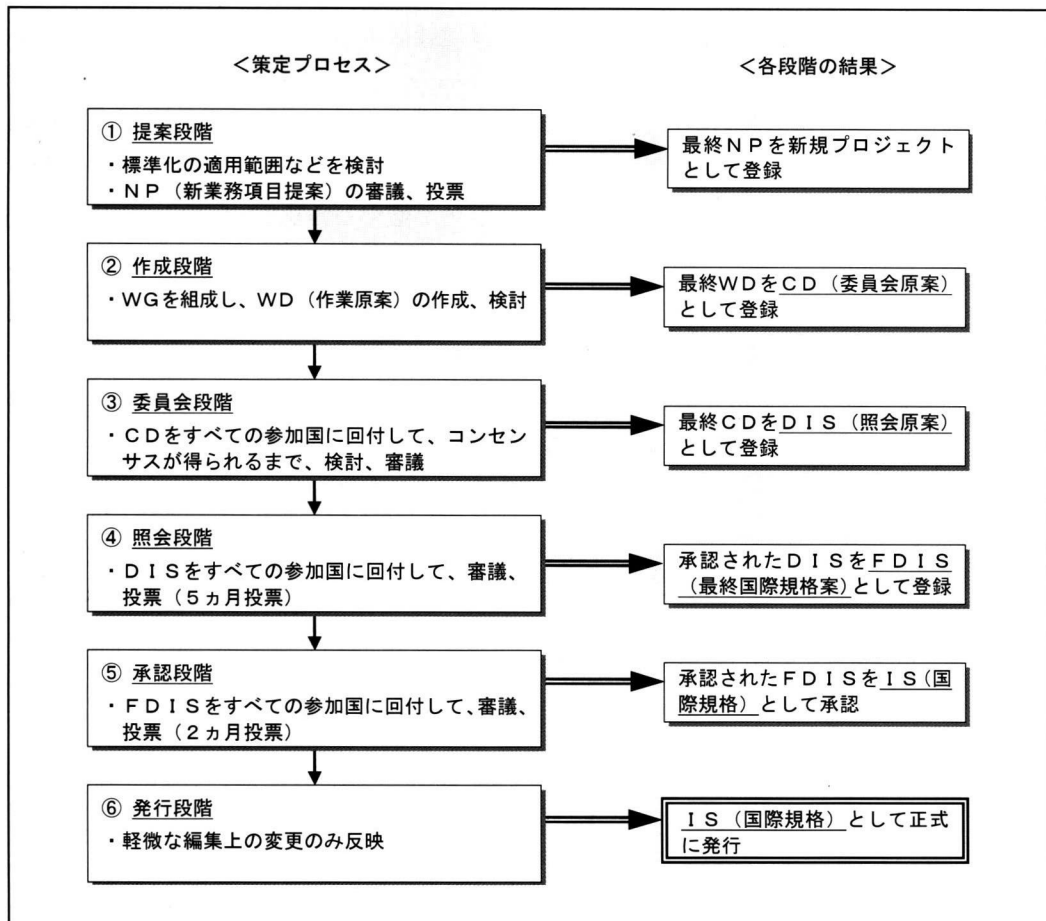
的に回付して、2ヵ月以内に最終的な賛否の投票を求める。この段階では、技術関係の修正は不可能であり、賛成か反対かのみを回答する。委員会の審議に参加する国の2/3以上が賛成して、かつ反対が投票総数の1/4以下であれば、FDISを「IS: International Standard (国際規格)」として発行することが承認されたことになる。承認基準に達しなかつ

た場合は、作成に当たった委員会に差し戻される。

⑥ 第6段階：発行段階 (Publication Stage)

ISとして発行することが承認されたFDISについては、必要な部分に限り、軽微な編集上の変更だけを反映したうえで、ISO中央事務局から、正式にISとして発行される。

(図表2) ISOの国際規格策定の流れ



以上のように、I S（国際規格）の策定プロセスにおいては、各段階において意見、賛否を求めた投票が繰り返し行われ、各国の意見を盛り込むための修正が加えられることにより、関係国間で合意が得られた I S が完成するという仕組みとなっている。

なお、すべての I S は、発行後の技術進歩や情勢変化に対応するため、当該 I S の維持管理を担当する委員会によって 5 年ごとに定期的な見直しが行われる。定期見直しの際の取扱いとしては、①特段の修正を加えることなく再承認する、②技術進歩を踏まえて改正する、③標準化の必要性がなくなり廃止する、のいずれかの選択肢があるが、その決定は当該委員会の P メンバーの参加国の過半数の意思に委ねられている。

3. 金融情報技術に関する国際標準化活動

(1) I S O / T C 68 の概要

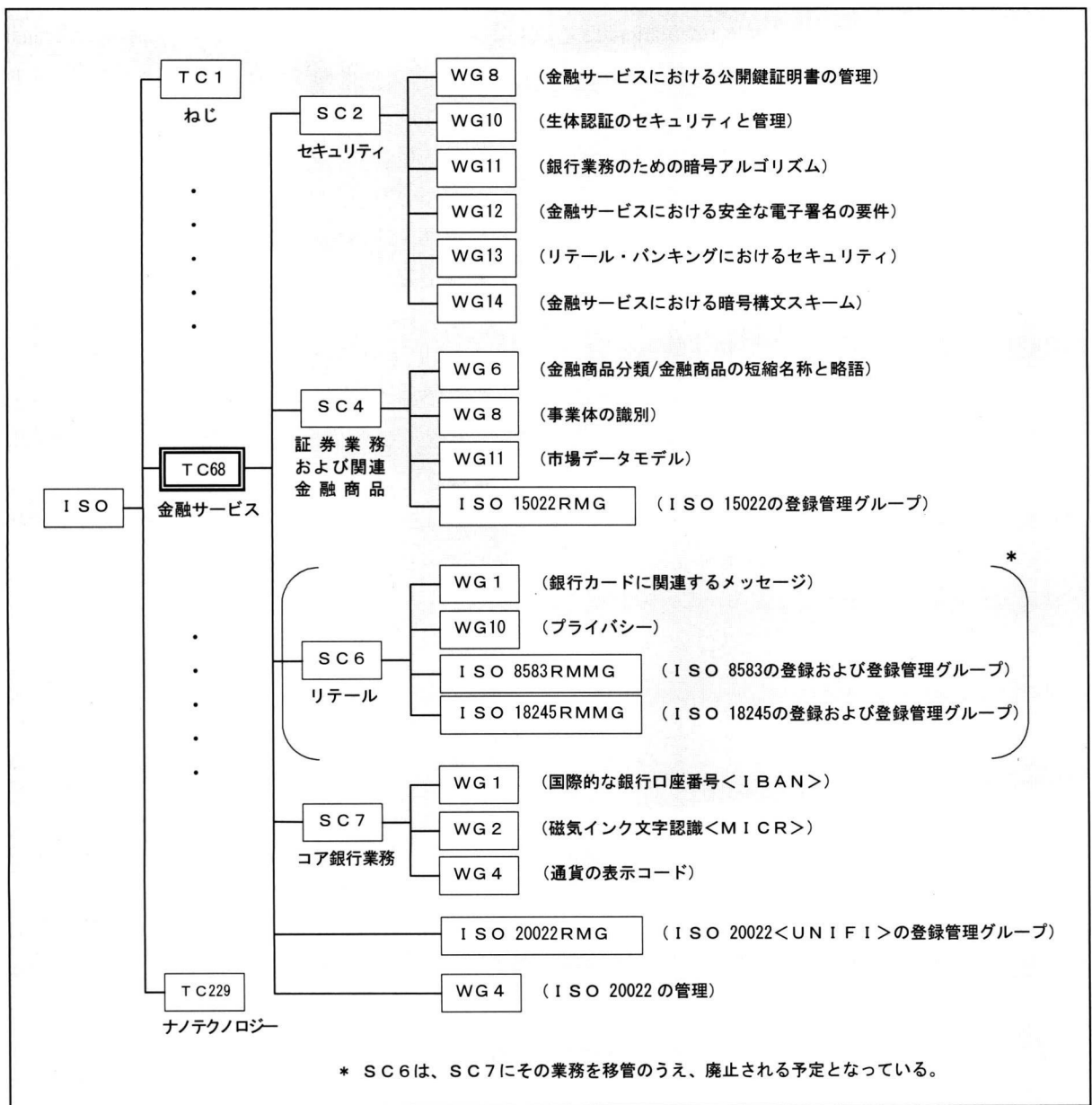
金融情報技術の国際標準化は、I S O の専門委員会の 1 つである T C 68 において行われてい

る。T C 68 は、「金融サービス（Financial Services）」を対象とする専門委員会であり、金融業務に利用される情報通信技術、情報セキュリティ技術等に関する国際標準化を担当している。

T C 68 の配下には、S C 2、S C 4、S C 6、および S C 7 の 4 つの分科委員会^(注 6)が設置され、さらに各 S C の配下には作業グループ (WG) が設置され、各担当分野において国際規格立案の審議が行われている。このほか、T C 68 の配下には、I S O 20022 (U N I F I <ユニファイ>: U N I v e r s a l F i n a n c i a l I n d u s t r y m e s s a g e s c h e m e) の登録管理グループ (R M G : R e g i s t r a t i o n M a n a g e m e n t G r o u p) 、および I S O 20022 の維持管理を担当する作業グループ (WG) も設置されている。また、コードやデータベースの登録および維持管理が必要な規格については、登録・維持管理グループ (R M M G : R e g i s t r a t i o n M a n a g e m e n t M a i n t e n a n c e G r o u p) が設置され、その対応に当たっている (図表 3 参照)。

(注 6) このうち S C 6 は、2006 年の T C 68 年次総会において、S C 7 にその業務を移管のうえ、廃止されることが決議されている。

(図表 3) ISO/TC68 の組織および標準化内容



TC68の委員長は、米国の Mark Zalewski 氏^(注7)が務め、事務局は、米国規格協会 (ANSI)

が務めている。TC68への参加状況を見ると、日本を含む23カ国がPメンバーとして、また、

(注7) Mark Zalewski氏は2006年一杯で退任し、2007年から Karla McKenna氏を新議長とすることが2006年のTC68年次総会において決議されている。

38 カ国がOメンバーとして参加している。このほか、TC68のリエゾン団体（連携関係にある団体）として、SWIFT^(注8)、VISA International、MasterCard Internationalなどの10機関が参加している。

以下、各SCについて、組織構成および制定された主な国際規格の概要について整理する。

イ. SC2（セキュリティ）

SC2は、金融サービスに関連するセキュリティについての国際標準化を担当する分科委員会である。主として、PIN（個人識別番号）管理とセキュリティ（ISO 9564）、金融業務における公開鍵基盤（PKI）^(注9)（ISO 15782、21188）、生体認証のセキュリティと管理（ISO 19092）、情報セキュリティ・ガイドライン（ISO/TR 13569）等の国際規

格を制定しており（主な国際規格の概要については、図表4参照）、下部組織として6つの作業グループを持つ。委員長は米国の Michael Versace 氏、事務局は米国規格協会（ANSI）が務めている（図表5参照）。

従来SC2は、SC6との間で、それぞれホールセール分野とリテール分野で管轄する国際標準化作業を住み分けていたが、両分野に必要とされる情報セキュリティ技術に類似性が高まったことから、2004年のTC68年次総会の決議により、SC6が管轄する国際規格のうち、セキュリティ関連の規格はすべてSC2に移管された。

SC2への参加状況をみると、日本を含む15カ国がPメンバーとなっているほか、SWIFT、VISA International、MasterCard Internationalなど9機関がリエゾン団体となっている。

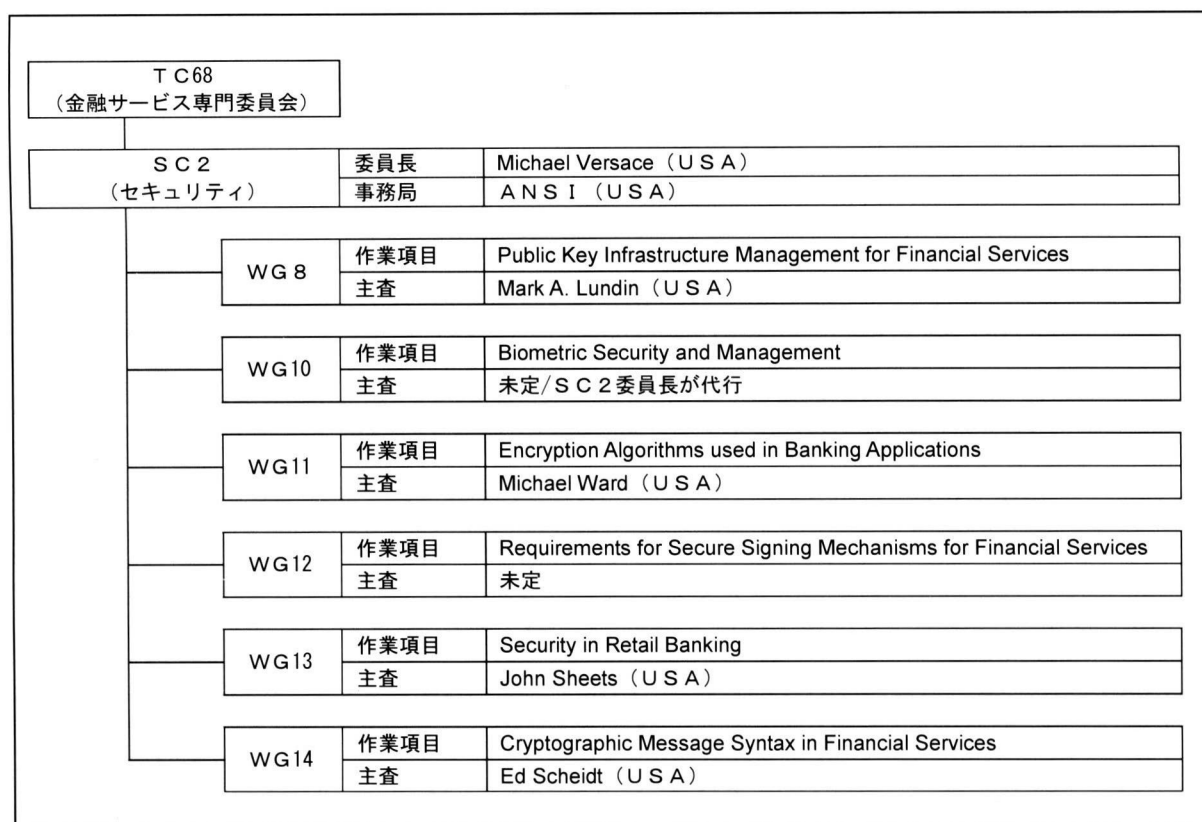
(注8) SWIFT (Society for Worldwide Interbank Financial Telecommunication) : 世界約200カ国、8,000を超える金融関連機関および中央銀行、決済機構等が、国際間の資金決済やトレーディング、証券業務などで利用している金融機関間の通信ネットワークを運営する非営利団体（本拠地：ベルギー・ブラッセルズ）。

(注9) 公開鍵基盤 (PKI : Public Key Infrastructure) : 認証機関 (CA) と呼ばれる機関を設置し、利用者の公開鍵の真正性を保証する「公開鍵証明書」(Certificate) を発行させることによって実現される。「公開鍵証明書」には公開鍵とその利用者を特定する情報が含まれており、CAが電子署名を付与することによって正当性を証明する仕組みである。

(図表 4) T C68/ S C 2 で制定された主な国際規格の概要

| 国際規格の名称 | 概要説明 |
|---|--|
| P I N (個人識別番号) 管理とセキュリティ (I S O 9564 シリーズ) | 銀行取引カード (キャッシュカード、クレジットカード、デビットカード) 等とともに利用される個人識別番号 (P I N : Personal Identification Number) について、その設定、保管、入力、送信等に関する一般的な規則について規定している。P I N の長さ、暗号化の際に利用するアルゴリズム、暗号化の際のパディング等について規定している。 |
| 安全な暗号装置 (I S O 13491 シリーズ) | リテール金融取引において利用される物理的かつ機能的に保護された暗号装置 (S C D : Secure Cryptographic Devices) に要求される機能について規定している。S C D の概念と必要条件、暗号プロセス評価用のチェック・リスト等について規定している。 |
| 金融取引における鍵管理 (I S O 11568 シリーズ) | リテール金融分野、特に C D / A T M で P I N を暗号化する際に、C D / A T M とセンターが暗号鍵を安全に共有するための鍵管理方式について規定している。 |
| 金融サービスにおける公開鍵証明書の管理 (I S O 15782 シリーズ) | 金融機関が金融業務に利用する目的で P K I を構築し、認証機関 (C A : Certification Authority) を運営する場合に C A として果たすべき役割や責任、公開鍵証明書の管理や拡張方法等について規定している。本規格に関連する最近の話題については、4 (2) を参照。 |
| 金融サービスのための公開鍵基盤 —— 運用と方針の枠組み (I S O 21188) | 金融業務で P K I を利用する際に必要となる認証ポリシー (C P : Certificate Policy)、および認証機関運用規程 (C P S : Certification Practice Statement) の作成方法について規定している。本規格は、I S O 15782 シリーズには詳しく触れられていない C P / C P S の枠組みを新たに規定し、これを補完する位置付けのものである。 |
| 生体認証のセキュリティと管理 (I S O 19092 シリーズ) | 金融業務において生体認証を利用する際のセキュリティ確保のための枠組みについて規定している。生体認証技術の概説、技術面の分析、生体認証システムの基本構造、運用・セキュリティ要件、セキュリティ分析、生体認証機器のセキュリティ要件等を網羅した、生体認証技術のセキュリティに関する詳細な技術規格である。本規格に関連する最近の話題については、4 (2) を参照。 |
| 情報セキュリティ・ガイドライン (I S O / T R 13569) | 金融機関が情報セキュリティ対策を実施する際の行動指針に関する技術報告書 (T R : Technical Report) である。まず、情報管理方針を明確に規定した情報セキュリティ・ポリシーを制定し、次に、それに基づき、情報セキュリティ管理部門の設置方針、役職員への情報セキュリティに関する研修プログラム、災害情報等の情報伝達・復旧プラン等に関する情報セキュリティ・プログラムを作成する必要があるとしている。 |
| 金融システムにおけるセキュリティの枠組み (I S O / T R 17944) | 金融業界が制定したセキュリティに関連する既存の各種規格 (I S O 以外の規格も含む) を担当分野別の一覧にして、必要に応じて適切な規格が選択できるように取り纏めたリスト集である。 |

(図表 5) T C 68/ S C 2 の組織図



ロ. S C 4 (証券業務および関連金融商品)

S C 4 は、証券業務に利用される情報技術に関する国際標準化を担当する分科委員会である。主として、国際的な証券識別コード (I S O 6166)、金融商品の分類コード (I S O 10962)、国際的な事業体識別コード (I S O 16372)、金融商品の短縮名称・略語 (I S O 18773、18774) など証券業務に関する国際規格を制定しており (主な国際規格の概要については、図表 6 参照)、下部組織として 3 つの作業グループを持つ。こ

のほか、証券取引用通信メッセージ・スキーム (I S O 15022) に基づく通信メッセージ標準について RMG を設置し、その維持・管理に当たっている。委員長はスイスの Nourrendine Yous 氏、事務局はスイス規格協会 (S N V) が務めている (図表 7 参照)。

S C 4 への参加状況をみると、日本を含む 20 カ国が P メンバーとなっているほか、S W I F T、ANNA^(注10)、Euroclear、Clearstream、E C B S^(注11) など 13 機関がリエゾン団体となっている。

(注 10) A N N A (Association of National Numbering Agencies) : C F I コードと I S I N コードの管理・登録を行う国際機関 (本拠地 : ベルギー・ブラッセルズ) で、各国の付番機関 (日本からは東京証券取引所) がメンバーとして加盟している。

(注 11) E C B S (European Committee for Banking Standards) : 1992 年に設立された E U 加盟国の金融機関のための技術標準化機関 (本拠地 : ベルギー・ブラッセルズ)。

(図表 6) T C 68/ S C 4 で制定された主な国際規格の概要

| 国際規格の名称 | 概要説明 |
|---|--|
| 証券取引用通信メッセージ・スキーム (I S O 15022 シリーズ) | 国際的な証券取引に用いられる通信メッセージ標準について規定している。各国事情に合わせた証券メッセージ・フォーマットを作成可能とするために、各国証券市場において参加者間の送受信が必要とされる情報（メッセージの内容、メッセージ・フォーマット等）の作成規則を規定している。以前利用されていた I S O 7775 の後継規格として、1999 年に制定された。本規格の改訂版（2nd edition）は、XML などの新しい要素技術を取り入れ、金融業務全般における幅広い利用を想定した通信メッセージ標準として位置付けられ、I S O 20022 として発行されている。I S O 20022 に関連する最近の話題については、4 (3) を参照。 |
| 国際的な証券識別コード (I S I N) (I S O 6166) | 国際的に証券を識別するコード (I S I N : International Securities Identification Number)、およびその管理手順について規定している。I S I N コードの付番権限は、各国当たり 1 機関に与えられており、わが国では東京証券取引所が付番機関に指定されている。 |
| 金融商品の分類コード (C F I) (I S O 10962) | 国際的な証券識別コード (I S I N) で定められた証券関連金融商品の属性を示すコード (C F I : Classification of Financial Instruments)、およびその管理手順について規定している。 |
| 国際的な事業体識別コード (I B E I) (I S O 16372 シリーズ) | 銀行識別コード (B I C) が割り当てられていない金融取引参加主体を識別するためのコード (I B E I : International Business Entities Identifier)、およびその管理手順について規定している。 |

(図表 7) T C 68/ S C 4 の組織図



ハ. SC6（リテール）

SC6は、リテール金融サービスに関する国際標準化を担当する分科委員会である。主として、金融取引カード用の通信メッセージ（ISO 8583-1）、ICカードと端末間の通信メッセージ（ISO 9992）などリテール金融サービスに関する国際規格を中心に制定してきており（主な国際規格の概要については、図表8参照）、下部組織として2つの作業グループを持つ。このほか、カード発行機関識別コード等（ISO 8583 シリーズ）、および加盟店業種別分類コード（ISO 18245）について、RMMG

を設置し、その維持・管理に当たっている。委員長はフランスの René Beltrando 氏、事務局はフランス規格協会（AFNOR）が務めている（図表9参照）。

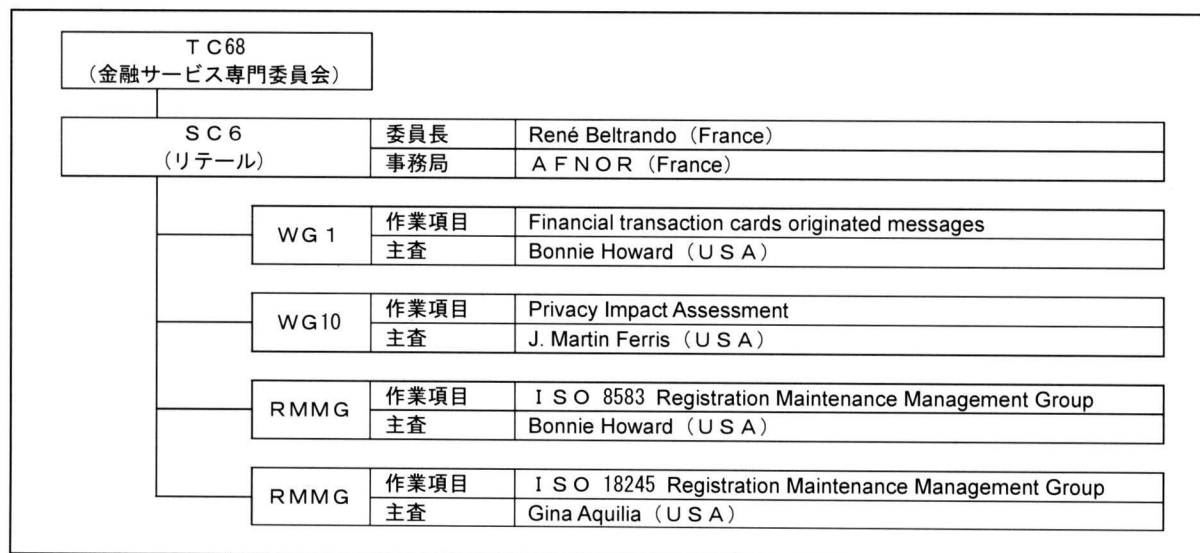
SC6への参加状況を見ると、日本を含む16カ国がPメンバーとなっているほか、ECBS、American Express、VISA International、MasterCard International など5機関がリエゾン団体となっている。

なお、本分科委員会は、取り扱う国際規格の数が少なくなったことから、SC7にその業務を移管のうえ、廃止されることが予定されている。

（図表8）TC68/SC6で制定された主な国際規格の概要

| 国際規格の名称 | 概要説明 |
|--------------------------------------|---|
| 金融取引カード用の通信メッセージ (ISO 8583 シリーズ) | 銀行カードによる取引において、加盟店、カード発行機関等の中で交換される通信メッセージの仕様（ビットマップ・フォーマットの定義）、維持管理方法、およびカード発行機関識別コードの申請・登録手続き等について規定している。 |
| ICカードと端末間の通信メッセージ (ISO 9992 シリーズ) | ICカードをリテール金融取引に用いるためのカードと端末間のデータの処理手順（読取り、書込み等の指示やそれに対応するレスポンス）と通信メッセージの構造等について規定している。 |

（図表9）TC68/SC6の組織図



二. SC7（コア銀行業務）

SC7は、コア銀行業務に関連する国際標準化を担当する分科委員会であり、2005年に新設された比較的新しい分科委員会である。主として、磁気インク文字認識（ISO 1004）、通貨の表示コード（ISO 4217）、銀行識別コード（ISO 9362）、国際的な銀行口座番号（ISO 13616）などのコア銀行業務分野の国際規格を制定している。最近では、最新の技術情報を踏まえての制定内容の見直し、規格制

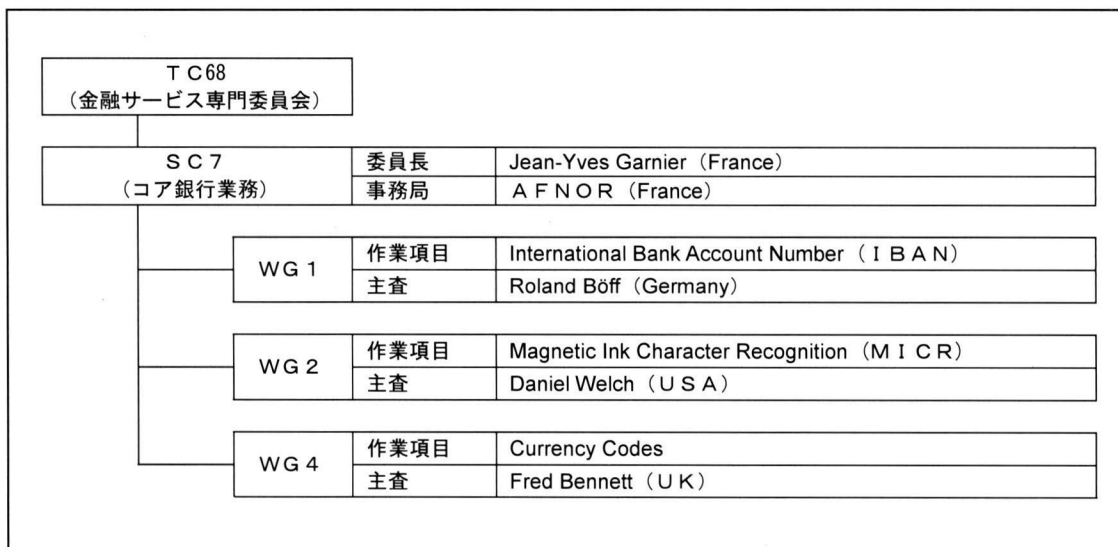
定後の適切な維持管理方法などについての検討が進められており（主な国際規格の概要については、図表10参照）、下部組織として、3つの作業グループを持つ。委員長はフランスのJean-Yves Garnier氏、事務局はフランス規格協会（AFNOR）が務めている（図表11参照）。

SC7への参加状況をみると、日本を含む17カ国がPメンバーとなっているほか、SWIFT、ECBSなど3機関がリエゾン団体となっている。

（図表10）TC68/SC7で制定された主な国際規格

| 国際規格の名称 | 概要説明 |
|--------------------------------------|--|
| 磁気インク文字認識（MICR） （ISO 1004） | 手形・小切手等で利用される磁気インク文字認識（MICR：Magnetic Ink Character Recognition）の各種仕様について規定している。わが国の手形・小切手では、本規格をJIS化した規格（JIS X9002）に基づくMICR印字がプリントされ、手形交換所における機械読取に利用されている。 |
| 通貨の表示コード （ISO 4217） | 貿易取引や銀行業務において使用される通貨の表示方法を統一する目的で作成された国際規格である。各国で発行されている通貨について、アルファベット3文字からなる略称（基本的には、最初の2文字はISO 3166で定義された国名コードであり、残りの1文字は通貨のイニシャル）と数字3桁からなるコードを定めている。例えば、わが国の通貨である円については、略称はJPY、コードは392となっている。 |
| 銀行識別コード（BIC） （ISO 9362） | SWIFTで利用される、国際的に銀行を唯一に識別するコード（BIC：Bank Identifier Code）について規定している。 |
| 国際的な銀行口座番号（IBAN） （ISO 13616 シリーズ） | 国際的な銀行口座番号（IBAN：International Bank Account Number）に関するフォーマット、登録機関の役割・責務等について規定している。欧州では、2004年7月以降、EU指令により、域内のクロスボーダー為替取引においては、顧客を特定するためにIBANを用いることが義務付けられている。本規格に関連する最近の話題については、4(3)を参照。 |

(図表 11) T C 68/ S C 7 の組織図



(2) I S O / T C 68 に対応する国内の取組み

イ. I S O / T C 68 国内委員会

わが国の I S O 会員団体である J I S C では、I S O の各専門委員会 (T C) ごとに業界団体等に国内意見の取り纏め等を行う国内審議団体を委嘱している。金融サービスに関する T C 68 については、日本銀行が国内審議団体の運営の委嘱 (事務局事務は日本銀行金融研究所情報技術研究センターが担当) を受けている (図表 12 参照)。

日本銀行は、国内の銀行、証券会社、業界団体、メーカー、通信事業者、学者、官公庁等をメンバーとする I S O / T C 68 国内委員会 (委員長: 横浜国立大学 松本勉教授) を定期的に開催しているほか、関連する国際会議への出席や、

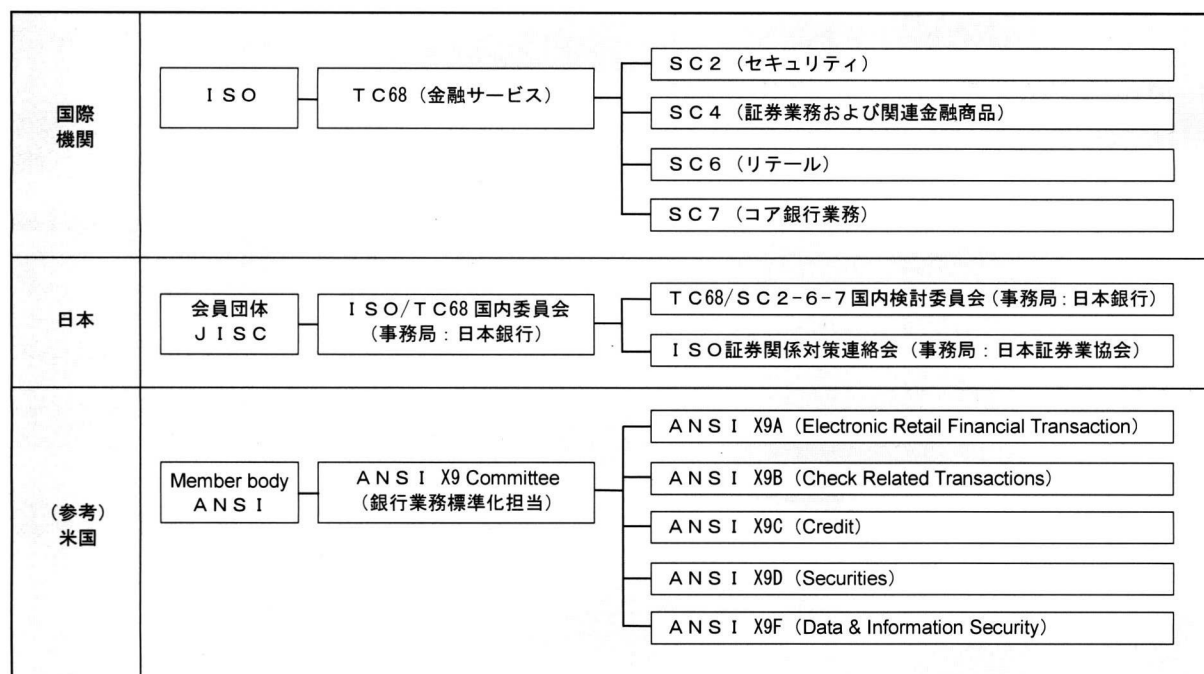
国内意見の取り纏め等を行っている^(注 12)。

I S O / T C 68 の下に設置された 4 つの分科委員会 (S C 2、S C 4、S C 6、および S C 7) についても、対応する国内組織が組成されている。4 つの分科委員会のうち、S C 2 (セキュリティ)、S C 6 (リテール)、および S C 7 (コア銀行業務) については、I S O / T C 68 / S C 2-6-7 国内検討委員会^(注 13) (事務局: 日本銀行) が、S C 4 (証券業務および関連金融商品) については、I S O 証券関係対策連絡会 (事務局: 日本証券業協会) が、各々の国内審議を担当している。これらの国内組織では、国内の金融機関、メーカー等の参加を得て、国際標準化に関する投票案件についての国内関係者の意見集約、国際会議の報告等を行っている。

(注 12) I S O / T C 68 国内委員会のホームページは、<http://www.imes.boj.or.jp/iso/> を参照。

(注 13) 現時点では、「S C 2-6-7 国内検討委員会」という名称であるが、T C 68 年次総会において S C 6 の廃止が決議されたため、今後、本委員会の名称は「S C 2-7 国内検討委員会」に変更される予定にある。

(図表 12) ISO/TC68 に対応する国内の国際標準化体制



ロ. 他の国内委員会とのリエゾン

ISO/TC68 の国際標準化領域は、他の標準化機関の領域とオーバーラップしている部分があるため、国際標準化を整合的に、かつ重複作業をせずに円滑に進めるには、他の標準化機関との連携が重要となる。ISOなどの国際標準化機関では、「リエゾン (Liaison、連携役)」と呼ばれる委員を相互の委員会に派遣し、連携を図ることが多い。このリエゾン関係は、国際レベルでも国内レベルでも実施されているが、現在、ISO/TC68 関連において国内でリエゾン関係を持っているのは、ISO/IEC JTC1^(注14) の分科委員会である SC17、SC27、および SC37

の3つである。

(イ) SC17

JTC1/SC17 は、カードおよび個人認証に関する国際標準化を担当している。SC17 にかかる国内審議は、SC17 専門委員会 (事務局：(社) ビジネス機械・情報システム産業協会) が担当しており、同委員会は、IDカードおよびその読取装置の国内主要メーカーとユーザーが委員となっている。

SC17 には、IDカードの物理的特性および試験方法等を担当する WG1、機械読取旅行文書を担当する WG3、外部端子付き ICカード

(注14) JTC1 (Joint Technical Committee 1 <合同専門委員会>)：情報技術革新の進展に伴い、コンピュータ技術やネットワーク技術の双方に跨る「情報技術分野」の標準化推進ニーズが増大したため、ISOとIECは1987年にJTC1を設立し、この分野の国際標準化を担当させている。

等を担当するWG 4、カード発行者番号システムを担当するWG 5、金融取引カードを担当するWG 7、無端子ICカード等を担当するWG 8、光メモリカード等を担当するWG 9、運転免許証および関連資料を担当するWG 10、生体認証関連を担当するWG 11 の計 8 つの作業グループがあり、SC 17 専門委員会は、各作業グループに対応する国内委員会を取り纏め、日本としての案件の審議を担当している。

(ロ) SC 27

JTC 1/SC 27 は、汎業界的なセキュリティ技術の国際標準化を担当している。SC 27 にか

かる国内審議は、SC 27 専門委員会（事務局：（社）情報処理学会）が担当しており、同委員会は、国内主要電機メーカーや通信事業者が委員となっている。

SC 27 には、情報セキュリティ関係の各種ガイドラインを担当するWG 1、暗号技術を担当するWG 2、セキュリティ評価基準を担当するWG 3 の計 3 つの作業グループがあり、SC 27 専門委員会は、各作業グループに対応する国内委員会を取り纏め、日本としての案件審議を担当している（情報セキュリティ対策に関する評価・認証を行う国際標準については、下掲BOX 2 参照）。

[BOX 2]

情報セキュリティ対策に関する評価・認証を行う国際標準について

TC 68 では、前述のとおり、SC 2 において金融サービスに関連するセキュリティについての各種規格・ガイドラインを制定しているが、セキュリティ対策に関する評価・認証のための枠組みについては策定していない。JTC 1/SC 27 では、各企業で実施済みの情報セキュリティ対策について、第三者機関が評価・認証を行う際に利用する国際標準を規定している。具体的には、情報システムのセキュリティ機能面について認証・評価を行うための規格である、ISO 15408（情報技術セキュリティの評価基準）、および情報システムのセキュリティ運用・管理面について認証・評価を行うための規格である、ISO 27000 シリーズ（情報セキュリティマネジメントシステム）等である。

情報システム全体としてのセキュリティ対策を適切に行うためには、これらの認証・評価のための規格を適宜選択して利用することにより、実施したセキュリティ対策について「お墨付き」を得ながら対応を進めることが効率的である。システム全体を意識しながらセキュリティ対策の検討を進めることによって、費用対効果の観点からセキュリティ機能面では対策がとれない部分に対しては、運用面で対応するなど、総合的にみて漏れのないセキュリティ対策が実現されることになる。

ただし、これらの規格は、汎業界向けに策定されたものであり、金融サービスに特化したものではないことに注意が必要である。金融機関が利用する際には、TC 68 で規定される各種のセキュリティ関連規格を併用しつつ対応することが必要となる。

(ハ) SC37

JTC1/SC37は、生体認証技術の国際標準化を担当している。SC37にかかる国内審議は、SC37専門委員会（事務局：（社）情報処理学会）が担当しており、同委員会は、バイオメトリクス関連機器の国内主要メーカーとユーザーが委員となっている。

SC37には、生体認証関係の専門用語を担当するWG1、テクニカル・インターフェースを担当するWG2、データ交換フォーマットを担当するWG3、アプリケーションの運用仕様を担当するWG4、生体認証技術の試験および報告を担当するWG5、社会的課題を担当するWG6の計6つの作業グループがあり、SC37専門委員会は、各作業グループに対応する国内委員会を取り纏め、日本としての案件審議を担当している。

4. 金融情報技術の国際標準化を巡る最近の話題

(1) 暗号アルゴリズムの2010年問題と金融業界への影響

イ. 暗号アルゴリズムの2010年問題とは

金融分野においては、金融取引に用いられる各種データの機密性や一貫性を確保する、あるいは取引相手を認証するための重要な要素技術として暗号アルゴリズムが活用されている。現在のところ、共通鍵暗号^(注15)としては2-keyトリプルDES、公開鍵暗号^(注16)およびデジタル署名^(注17)としては鍵長1024ビットのRSA、ハッシュ関数^(注18)としてはSHA-1が、デジタル、デファクト双方の国際標準の中に規定されており、世界各国の金融業界で広く利用されている。しかし、これらの暗号アルゴリズムは、近年の暗号解読技術やコンピュータ技術の急速な進歩を背景に、2010年頃にはその安全性が低下し、利用に適さなくなることが指摘されている。特に、米国の政府機関であるNIST^(注19)では、2010年末までに上記の暗号アルゴリズムについて、安全性に関する「お墨付き」を取り

(注15) 共通鍵暗号：暗号化と復号に同一の鍵を利用する暗号方式である。ネットワーク上でやり取りされるデータや外部記憶媒体に保管されるデータを秘匿するために用いられるほか、無権限者によるデータの改ざんを防止・検出するための技術としても利用されている。

(注16) 公開鍵暗号：暗号化用の鍵（公開鍵）と復号用の鍵（秘密鍵）が異なる暗号方式であり、ある特定のデータが得られない状況において暗号化用の鍵から復号用の鍵を算出することが計算量的に困難（理論的には可能であるが、膨大な時間と費用を要するため事実上不可能）であるため、暗号化用の鍵を公開することができるという特徴を持つ。PKIの基本となる技術である。

(注17) デジタル署名：電子文書の正当性を保証するために付けられる暗号化された署名情報。文書が正当な発信者から発信され、受信されるまでの間に途中で改ざん等が行われていないことを証明する。一般にデジタル署名では、公開鍵暗号方式を利用する。

(注18) ハッシュ関数：任意長の入力データを固定長の「ハッシュ値」に圧縮する関数のこと。ハッシュ値から原文を再現することが困難であるとともに、同じハッシュ値を持つ異なるデータを作成することは極めて困難であるような性格を持つものが利用される。

(注19) NIST (National Institute of Standards and Technology<米国立標準技術研究所>)：米国連邦政府の機関で、工業技術の標準化を支援している。1988年にNBS (National Bureau of Standards) が改組して誕生した。米国連邦政府機関の情報システムで利用する標準暗号を制定する機関でもある。

消すことを表明している。こうした状況下、これらの暗号技術を現在のままの形で、今後も長く利用し続けることには問題が多いと考えられる。今後、暗号アルゴリズムの移行をどのように進めるかが重要な問題となっており、こうした問題を総称して「暗号アルゴリズムの2010年問題」（以下、「2010年問題」と略す）と呼んでいる。

ロ. TC68における2010年問題への取組み

TC68では、2005年9月のTC68/SC2年次総会において、日本から2010年問題に関する研究論文（宇根・神田〔2006〕）の要旨を提出し、問題提起を行ったところ、SC2の配下に新たにスタディ・グループ（SG）を組成し、金融分野で利用される暗号の強度評価などの検討を進めることが合意された。その後、当該SGにおいて議論を重ねた結果、2010年問題に対するTC68としての推奨対応策の素案（ISO〔2006〕）が纏まった。また、本議論の結果に基づき、TC68で既に制定された規格やガイドラインにおいて規定されている推奨暗号アルゴリズムの見直しを行い、より強度の高いアルゴリズムが推奨されることとなっている。

2010年問題は、1990年代の共通鍵暗号DES（シングルDES）の強度低下に伴う論議と同様な展開を辿っている。1994～1995年当時、共通鍵暗号の事実上の国際標準であったDESについて、米国代表から強度低下に関する問題提起があり、TC68としての対応策について検討が開始された。そこで、日本がその技術的な検討を分担し、1996年8月のTC68年次総会で研究論文^{（注20）}を報告し、世界の金融業界がDES

からトリプルDESに移行するための理論的な根拠付けを行った。今回の2010年問題においても、2-keyトリプルDES、鍵長1024ビットのRSA、SHA-1については、既に学界や暗号技術の専門家の間では、その強度低下が当然のことと理解されているものの、金融業界の実務家の間では、今なお、そうした評価に懐疑的である先も多く、次世代の暗号技術への移行に躊躇する傾向がみられる。

こうした問題について、その研究成果をTC68に報告していくことは、世界の金融業界が利用する国際標準への信頼性を維持するための取組みに資するとともに、わが国の決済システムにおける暗号技術の選択において適切な判断を促すという意味で、重要な取組みと考えられる。

ハ. 金融業界に求められる対応

2010年以降、安全性に関する「お墨付き」を失った暗号アルゴリズムを使用し続けた場合、当該システムの安全性に関するレピュテーションが低下する惧れがある。また、万一、暗号アルゴリズムの安全性上の欠陥から何らかの金銭的な損害が発生した場合には、「お墨付き」を喪失した暗号アルゴリズムを使用し続けていたという点で批判を受ける可能性も否定できない。このため、より安全な新しい暗号アルゴリズムへ移行することが求められるが、多くのシステムにおいて利用されている現在の暗号アルゴリズムすべてを短期間で新しいものへ移し変えることは容易なことではない。それゆえ、2010年までに金融インフラの安全性や信頼性を確保しつつ、いかにして暗号アルゴリズムのスムーズな移行を実現するかが大きな課題となっている。

（注20）楠田浩二・松本勉による「A Strength Evaluation of Data Encryption Standard」と題する研究論文（Kusuda and Matsumoto〔1997〕）。

2010 年問題に適切に対処するためには、早急に企業レベルで移行方法についての議論を開始すべきであるとともに、暗号アルゴリズムの選定に重要となる各種リスクや運用上の問題についても検討を始めることが重要である。今後、NIST の新しい国際標準暗号の方針や、TC68 における推奨対応策の検討結果も参考にしつつ、暗号アルゴリズムを適切に選定し、移行を成功させる必要がある。

(2) 金融機関の情報セキュリティ対策に関する国際標準化

イ. 金融業務における公開鍵基盤 (ISO 15782、ISO 21188)

インターネットの普及に伴い、オープンなネットワークで金融サービスを提供する金融機関が増えているが、利用者の認証を行う際に公開鍵暗号による電子認証技術を利用することが多い。公開鍵暗号を利用する場合、各利用者は自分の秘密鍵と公開鍵のみを管理すればよいため、利用者が膨大となるオープンなネットワークにおいては、共通鍵暗号と比べて利便性が高いからである。ただし、各利用者の公開鍵が正当であることを確認するための仕組みとして、公開鍵基盤 (PKI) を構築することが必要となる。PKI はオープンなネットワーク上に構築されるため、複数のシステム間の相互運用性が大切であり、標準化が重要な役割を果たすことにな

る。「公開鍵証明書」に関する汎業界的な標準としては、ITU-T による X.509^(注21) 勧告が利用されており、これに基づく PKI の仕組みや利用方法を巡っては、世界中で様々な技術開発が進められ、デファクト、デジュール双方で、様々な標準化が進められている。

TC68 では、金融機関が金融業務に利用する目的で認証機関 (CA) を運営する場合に CA として果たすべき役割や責任、公開鍵証明書の管理や拡張方法等について技術的な観点から規定した ISO 15782 (金融サービスにおける公開鍵証明書の管理) を制定している。

本規格は米国規格である ANSI X9.57^(注22) をベースとして作成されたため、証明書ポリシー (CP: Certificate Policy) や認証機関運用規程 (CPS: Certification Practice Statement) の作成方法等については詳しく規定されていない。このため、TC68 では、別途、CP/CPS に関する国際規格として、米国規格である ANSI X9.79^(注23) を参考にして ISO 21188 (金融サービスのための公開鍵基盤 —— 運用と方針の枠組み) を策定している。

本規格は、金融業務に利用される CA を対象に採用すべき高度なセキュリティ要件を具体的に規定しているほか、金融機関が電子認証業務を行う場合の義務と責任範囲を明確にしておき、金融機関が認証機関として PKI の運営に参画する際に有用な規格である。

(注 21) X.509: ITU-T (ITU の電気通信標準化部門) が 1988 年に勧告した公開鍵証明書のデータ形式に関する規格。ISO 9594-8 としても規格化されている。現在広く用いられているのは 1996 年に勧告された X.509v3 で、これは証明書に拡張領域を設けて、証明書の発行者が独自の情報を追加できるようになっている。

(注 22) ANSI X9.57 (Public Key Cryptography for the Financial Services Industry: Certificate Management): ANSI /X9/X9F が 1997 年に制定した金融業務において利用される公開鍵証明書の管理方法について規定した米国規格。

(注 23) ANSI X9.79 (PKI Practices and Policy Framework for the Financial Services Industry): ANSI /X9/X9F が 2001 年に制定した金融機関が認証業務を行う際に作成する証明書ポリシーや認証機関運用規程 (CP/CPS) について規定した米国規格。

なお、わが国においても、全国銀行協会が制定した「全銀協 I C キャッシュカード標準仕様」に基づいて P K I が構築され、全銀協が運営する認証局によって、公開鍵証明書発行サービスが運用されている。

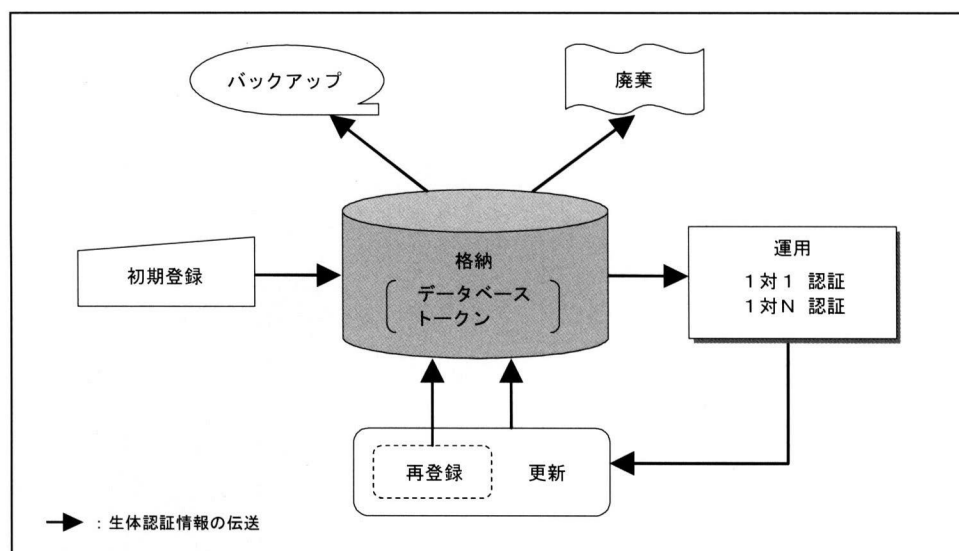
ロ. 金融業務における生体認証技術 (I S O 19092)

偽造・盗難キャッシュカード犯罪等へのセキュリティ対策として、金融業界では生体認証技術が活用されつつあるが、T C 68 では、金融業務に生体認証技術を適用する際のシステム設計・管理上の留意点に関するガイダンスについて、

T C 68 / S C 2 / W G 10 において標準化が進められている。

I S O 19092 は、米国からの提案により、米国規格 A N S I X 9.84 ^(注 24) をベースとして、国際標準化が行われているものである。I S O 19092 は、銀行の顧客および従業員の識別と認証を目的とする生体認証技術を利用する際の、生体認証情報のライフサイクル (図表 13 参照) の各局面における管理方法やセキュリティ要件を明確にし、セキュリティ要件を達成するための技術等について規定している。

(図表 13) I S O 19092 で規定される生体認証情報のライフサイクル



(注 24) A N S I X 9.84 (Biometric Information Management and Security) : A N S I / X 9 / X 9 F が 2001 年に制定したアメリカの金融業界において生体認証情報を安全に管理・運用するためのガイドライン。

ANSI X9.84をISO 19092として国際標準化するに当たって、「セキュリティの枠組み」と「メッセージ構文と暗号化に関する要件」の2つのパートに分割した。パート1では、①用語を含めた生体認証技術に関する基本的な説明、②生体認証機能に関する構成およびセキュリティ要件、③生体認証技術を金融サービスに実装する際の技術の紹介、④生体認証システムの運用を認証するための管理目標等が規定されている。また、パート2では、①ASN.1^(注25)を利用した生体認証情報の記述ルール、②生体認証情報の完全性や機密性を確保するための暗号技術の利用方法、③ISO 8583を拡張して生体認証情報を金融機関間で送受信する際のメッセージ書式等について規定されている。

本規格案は、現在、審議中（パート1は承認段階、パート2は委員会段階）であり、まだ正式な国際規格としては発行されていない状況である。わが国からは、JTC1/SC37国内委員会をはじめとしたリエゾン関係を強化しつつ、わが国の金融機関において、既に利用されてい

る静脈認証（Vein Biometrics）に関する記述を追加するよう要請するなど、積極的に審議に参加している。

（3）金融業務における通信メッセージ等に関する国際標準化

イ．金融取引用の通信メッセージに関する規格（ISO 20022）

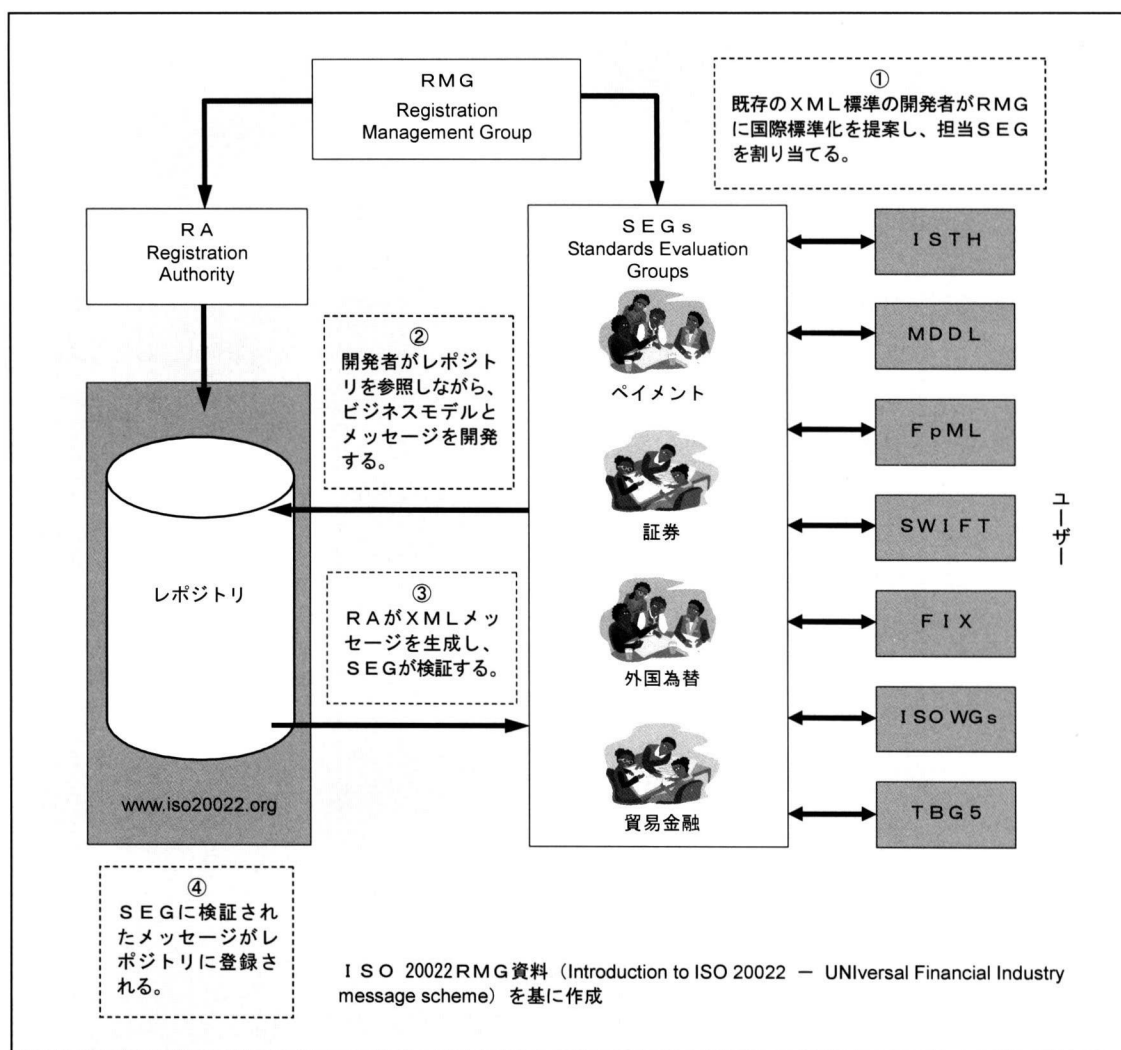
ISO 20022（UNIFI＜ユニファイ＞：UNiversal Financial Industry message scheme）とは、金融取引で利用される通信メッセージに関する国際規格である。通信メッセージ・フォーマットを拡張性に優れたXML^(注26)ベースとするなど、新しい要素技術を取り入れながら、ユーザーに通信メッセージを利用しやすくするための改善が図られている。また、通信メッセージ標準を開発する過程で、ユーザーのニーズを適切に反映し、その後の利用を促すための手続き上の仕組みが備わっている^(注27)（図表14参照）。

（注25）ASN.1（Abstract Syntax Notation One＜抽象構文記法1＞）：特定のコンピュータ構造や表現形式に依存せずにデータ・タイプを表現するための表記法である。主にコンピュータ同士の通信プロトコルを規定するために使用される。ASN.1はISOとITU-Tによって規定され、1987年12月にISO 8824として国際規格化された。

（注26）XML（Extensible Markup Language）：マークアップ言語（文字等の情報とともに、その情報に関する様々な属性情報を併せて文書中に記述する方式の言語）の1つ。インターネットで利用されるHTMLの簡便性と、その基となったより精緻な方式であるSGMLの柔軟性という2つのマークアップ言語の利点を兼ね備え、インターネットとの親和性も高いとされている。

（注27）標準化された通信メッセージ・フォーマットは、「レポジトリ」と呼ばれるデータベースに登録され、誰でも容易に閲覧することができる（<http://www.iso20022.org/>）。

(図表 14) I S O 20022 (U N I F I) の登録プロセス



本規格は、当初、TC68/SC4が所掌するISO 15022（証券取引用通信メッセージ・スキーム）の改訂版（2nd edition）として検討が進められてきたが、証券業務に限らず、銀行業務にも利用しうる汎用性を有していることから、金融取引全般における幅広い利用を想定した通信メッセージに関する規格としての位置付けを

与えられることになった。これを受けて、2004年にISO 20022という新たな番号が付され、TC68における担当も、SC4からTC68の直轄に変更された。

欧米の金融業界では、XML Web サービス^(注28)を利用して、複数のサービスをシームレスに提供するシステムをXMLベースで構築する動き

(注28) XML Web サービス：XML、HTTP、SOAPなどのインターネット標準技術を利用して、異なるプラットフォーム上のアプリケーションとも統合することが可能なソフトウェアの総称。

が広がっている。こうした動きに加え、欧州のリテール金融取引の分野では、域内での小口決済の内外格差を解消した単一ユーロ支払地域（SEPA）^{（注 29）}の構築に向け、2010 年の本格稼働開始を目指して、域内の小口決済インフラの共通化を進めている。そうした取組みの中で、銀行間ネットワークの広範なSTP化を実現するため、域内の銀行取引で利用する通信メッセージの開発にISO 20022を採用することを決定している。同様に、欧州の証券分野でも、投資家保護等の観点から、従来の投資サービス指令（ISD：Investment Services Directive）に代わる新しい証券業務規制として金融商品市場指令（MiFID：Markets in Financial Instruments Directive）が採択され、2007 年から施行されることを受けて、証券取引用通信メッセージの標準化団体がISO 20022を活用した標準化を進めつつある。このほか、最近では、外国為替や

貿易金融の分野でも、ISO 20022に準拠した通信メッセージの標準化を進める動きもみられ始めている。

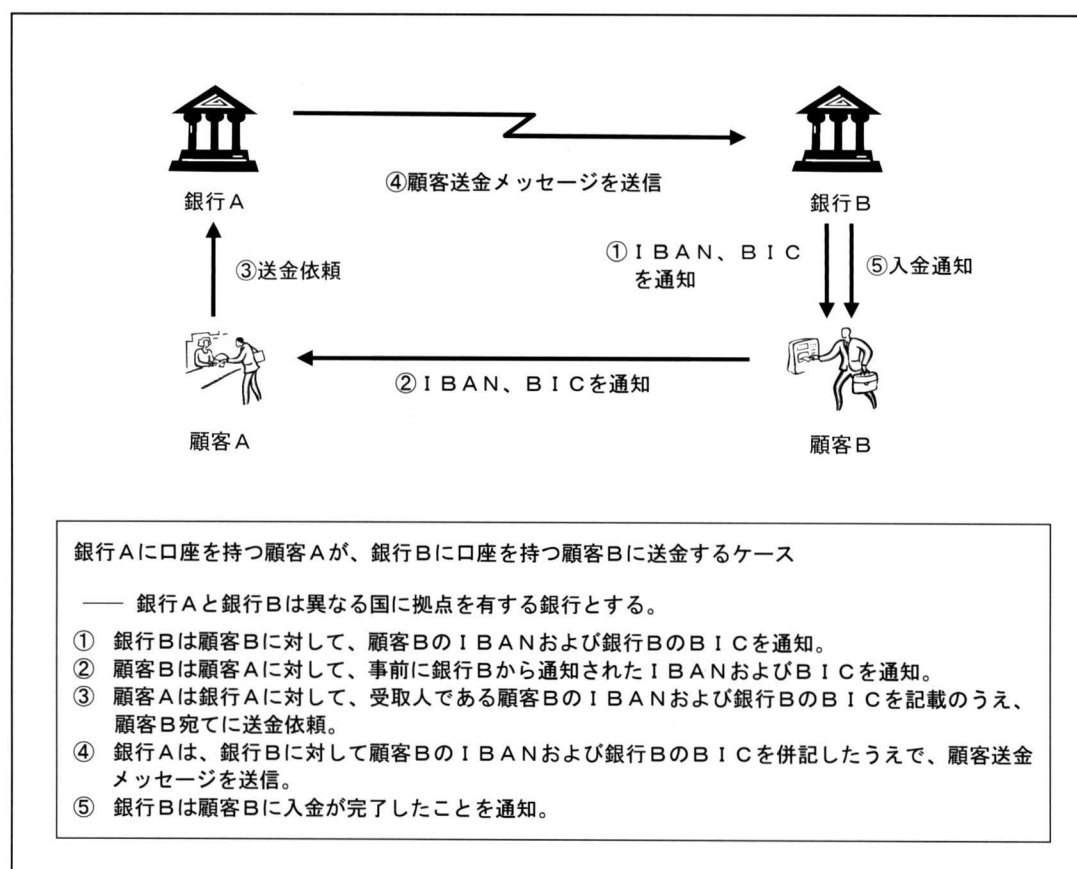
今後、わが国の金融業界としても、こうした標準化の動きをフォローしつつ、どのような対応を図っていくべきかについて、戦略的見地から、十分な検討を行っていく必要があると考えられる。

ロ. 国際的な銀行口座番号IBAN（ISO 13616）

IBANとは、International Bank Account Number（国際的な銀行口座番号）の略称で、ISOおよびECBSが、外国送金のエラー削減、処理の迅速化およびコスト面での効率性促進等を主な目的として制定した金融機関顧客（企業、個人）の口座を特定するための国際規格である（図表 15 参照）。

（注 29）SEPA（Single Euro Payment Area）：欧州域内での国境を越えたクレジットカードやデビットカード、自動引落とし等、電子決済システムを利用した支払いを、国内での取引と同じように、容易、安全かつ安価に行えるような基盤整備を目指すプロジェクト。欧州の銀行業界が設立したEPC（European Payments Council）が中心となり、2010 年の本格稼働開始を目指して関係者間の調整が進められている。

(図表 15) クロスボーダー取引における I B A N の利用例



T C 68 / S C 7 / W G 1 では、I S O 13616 の定期見直しのタイミングに合わせて、より様々な国々で共通して利用可能となるように I B A N の規定内容に関して調整を行っていたが、今般、関係国間で合意が得られた。このため、今後、国際標準化手続きを経たうえで、I S O 13616 の改訂版が発行される予定である。

I B A N の導入状況をみると、欧州諸国では、2004 年 7 月以降、E U 指令により、欧州域内のユーロ建てクロスボーダー為替取引においては、顧客を特定するために I B A N を用いることが義務付けられたため、現状広く利用されている。

一方、わが国では、2005 年 10 月に、日本スイフトユーザーグループが日本版 I B A N を制定したものの、本 I B A N の導入は、各金融機関の自由判断との位置付けにとどまり、必要に応じて送金事務処理円滑化等の一手段として、各社が任意に使用可能という位置付けであるため、現時点では、あまり普及していない。とはいえ、今後の技術革新や金融取引の国際化の進展に伴い、わが国でも I B A N を利用するニーズが高まる可能性もある。このため、海外における I B A N の利用状況についても注視しておく必要があると考えられる。

5. おわりに

冒頭に述べたとおり、金融情報技術に関する国際標準化を推進することは、単に金融機関の情報システムが相互に接続可能となるだけでなく、金融機関の事務合理化や顧客の安全性、利便性向上にも資するものである。

各国の金融業務の進め方は、各国の法令や金融制度、商慣習等を踏まえて形作られたものであるため、一律に国際標準に収斂していくものではない。しかし、わが国の金融業界においても、今後、情報通信ネットワークを利用した国

際的な金融ビジネスを展開するうえでの国際競争力を高めていくために、I S O / T C 68 における金融情報技術に関する国際標準化動向への理解を深めておくことが、ますます重要となつてこよう。

日本銀行としても、I S O / T C 68 の国内事務局を務める立場から、金融情報技術に関する国際標準化の動きを適切にフォローするとともに、関連情報を積極的に国内の金融業界に還元していくことにより、そうした理解の深化に貢献していきたいと考えている。

[参考文献]

- 岩下直行・谷田部充子、「金融分野における情報セキュリティ技術の国際標準化動向」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年、33～56頁
- 、「金融分野における情報技術の国際標準化動向 —— I S O / T C 68 における最近の議論を中心に」、第8回決済システムフォーラム（2004年11月5日）におけるプレゼンテーション資料、2004年（<http://www.boj.or.jp/type/release/zuiji/kako03/data/set0411b5.pdf>）
- 宇根正志、「金融分野におけるP K I：技術的課題と研究・標準化動向」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年、227～284頁
- ・神田雅透、「暗号アルゴリズムの2010年問題について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、31～72頁
- 栗原史郎・竹内修、『21世紀標準学』、日本規格協会、2001年
- 情報処理学会、「特集 バイオメトリック認証システム」、『情報処理』Vol. 47 No. 6通巻496号、2006年、569～615頁
- 情報処理推進機構（I P A）セキュリティセンター、『本人認証の現状に関する調査報告書』、2002年（<http://www.ipa.go.jp/security/fy14/reports/authentication/authentication2002.pdf>）
- 谷口文一、「金融業界におけるP K I・電子認証について —— 技術面、標準化に関する最近の動向を中心に —— 」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年、15～54頁
- 奈良好啓、『国際標準化入門』、日本規格協会、2004年
- 日本規格協会、『I S O規格の基礎知識（改訂2版）』、日本規格協会、2000年
- 、『J I Sハンドブック 2006（55）国際標準化』、日本規格協会、2006年
- 日本工業標準調査会（J I S C）、『第8次工業標準化推進長期計画』、日本工業標準調査会、1998年（http://www.jisc.go.jp/newsttopics/1998/chokei_8.htm）
- 日本工業標準調査会（J I S C）標準部会、『国際標準化活動基盤強化アクションプラン』、日本工業標準調査会、2004年
- 宮田慶一、「証券取引のS T P化を巡る動きについて」、『日本銀行調査月報』、日本銀行、1999年10月号
- International Organization for Standardization (ISO), “ISO TC68 SC2 Cryptographic Algorithms Position Paper on Symmetric Algorithms prepared for ISO TC68 SC2 in compliance with Resolution 05/280 2nd July 2006,” ISO, 2006.
- , and International Electrotechnical Commission (IEC), *ISO/IEC Directives, Part1, Procedures for the technical work, 5th edition*, ISO, 2004.
- , and ——, *ISO/IEC Directives, Part2, Rules for the structure and drafting of International Standards, 5th edition*, ISO, 2004.
- Koji Kusuda, and Tsutomu Matsumoto, “A Strength Evaluation of the Data Encryption Standard,” IMES Discussion Paper Series, 97-E-5, Bank of Japan, 1997.