■11 群（社会情報システム）－ 7 編（金融情報システム）

8 章 金融情報技術の国際標準化

（執筆者：岩下直行）［2009 年 3 月 受領］

■概要■

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．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，無秩序化する物や事柄を，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 [1]．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．

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，金融業務が情報通信ネットワークを経由してシステム的に処理されるようになると，通信メッセージ・フォーマット，コード体系などの情報通信技術が新たな標準化の対象に加わった．更に，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，生体認証技術など，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．

我が国の金融業界においても，こうした標準化の取り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．我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などもあって，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，我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．我が国の金融機関は，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．

本章では，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としての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．

【本章の構成】

本章では，8-1 節で金融情報技術の国際標準化の枠組みについて整理した後，8-2 節で金融分野における情報セキュリティ技術標準，8-3 節で金融分野における通信メッセージ標準の動向について述べる．

■11 群 － 7 編 － 8 章

8-1 金融情報技術の国際標準化の枠組み

（執筆者：岩下直行）［2009 年 3 月 受領］

金融情報技術の国際標準化は，国際標準化機構（ISO）の活動の一部として行われている．ISO は，本部をジュネーブに置く非政府機構であり，各国 1 機関のみに会員資格が認められている．日本からは，日本工業標準調査会（JISC）が 1952 年に会員団体として加入している．

ISO の標準化担当分野は多岐にわたり，分野ごとに専門委員会（TC：Technical Committee）が設置されており，金融情報技術の国際標準化は，その一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．TC68 の配下には SC2，SC4，SC7 の三つの分科委員会（Sub-Committee：SC）が設置され，SC ごとに国際規格立案や審議が行われている．TC68 において制定される国際標準は，金融取引の電子化の進展を反映し，通信メッセージの標準化やコード体系といった情報通信技術に関するものと，そうした電子化された取引の安全性確保のための情報セキュリティ技術が多くを占めている．

SC2 は，電子化された金融取引の情報セキュリティについての国際標準化を担当し，暗証番号（PIN）や生体認証システムとその管理手順，メッセージ暗号化のための手順などを制定している．SC4 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している．国際的な証券識別コードや事業体識別コード，金融商品の分類や短縮名称などを制定している．SC7 は，コア銀行業務に関連する国際標準化を担当しており，国際的な銀行口座や銀行識別コード，通貨表示コードを制定している．これら三つの SC とは別に TC68 直轄として，金融取引の通信メッセージに関する国際標準である ISO20022 の登録・管理を行う ISO20022RMG（Registration Management Group）が設けられている（**図 8･1**）．

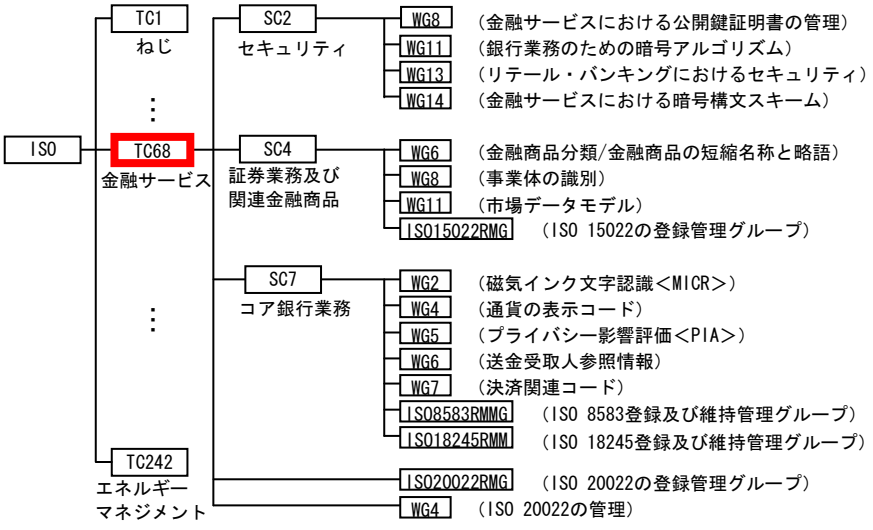


図 8･1 ISO/TC68 の組織及び標準化内容

日本国内においては，JISC からの委嘱を受けて，日本銀行が事務局として ISO/TC68 の国内審議団体の運営を行っている[2]．また，SC2，SC7，ISO20022RMG については日本銀行が，SC4 については日本証券業協会が国内委員会の事務局を運営している．

現在，ISO/TC68 によって策定されている主な国際標準を，担当する SC ごとに整理すると，**表 8･1** のとおりである．

表 8・1　ISO/TC68 が策定している主な国際標準

SC2：**金融情報のセキュリティ**
ISO9564 シリーズ　**暗証番号（PIN）管理とセキュリティ** 銀行取引カード（キャッシュカード，クレジットカード，デビットカードなど）とともに利用される暗証番号（PIN：Personal Identification Number）について，その設定，保管，入力，送信などに関する一般的な規則を定めた標準．PIN を暗号化に利用するアルゴリズム，暗号化の際のパディング方法といった暗号技術上の詳細な規定を含んでいる．
ISO15782 シリーズ及び ISO21188　**金融システムにおける公開鍵基盤（PKI）** ISO15782 シリーズは，金融機関が金融業務に利用する目的で PKI を構築し，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などについて定めた標準．ISO21188 は，ISO15782 シリーズを補う形で，PKI を利用する際の認証ポリシー及び認証機関運用規程の作成方法について規定した標準．
ISO19092　**生体認証のセキュリティと管理** 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た標準．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などを網羅した，生体認証技術のセキュリティに関する詳細な技術規格となっている．
SC4：**証券業務及び関連金融商品**
ISO6166　**国際的な証券識別コード（ISIN）** 株式，国債，社債などの有価証券を識別するための世界共通のコード体系，及びその管理手順について定めた標準．我が国では，証券コード協議会の事務局を務める東京証券取引所が ISIN の付番機関に指定されている．
ISO16372　**国際的な事業体識別コード（IBEI）** 銀行以外の法人格を有する金融取引参加主体（発行会社，証券会社，法人顧客，政府・地公体など）を識別するためのコードとその管理手順についての標準．
SC7：**コア銀行業務**
ISO4217　**通貨の表示コード** 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標準．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（最初の 2 文字は ISO 3166 で定義された国名コード，残りの 1 文字は通貨のイニシャル．日本円は JPY）と数字 3 桁からなるコードを定めている．
ISO9362　**国際的な銀行識別コード（BIC）** 国際的な金融取引に利用される，国際的に銀行を唯一に識別するコードについて規定した標準．銀行（4 文字），国，所在地（各 2 文字），支店（3 文字）から構成されている．
ISO13616 シリーズ　**国際的な銀行口座番号（IBAN）** 欧州で広く利用されている国際的な銀行口座のフォーマットを規定した標準．当初，欧州域内の標準として制定された後，ISO 標準に採用された．
TC68 **直轄**
ISO20022　**汎用金融取引メッセージの作成手続き** 銀行業務・証券業務両分野で利用される通信メッセージに関する国際標準．通信メッセージ・フォーマットを従来の固定長から拡張性に優れた XML に変更するとともに，システムやアプリケーションから独立した業務モデルを UML で記述し，そのモデルを基にプログラム・コードを生成するという新しいシステム開発手法を導入することにより，従来よりも柔軟かつ迅速なシステム構築を可能とすることを企図している．

■11 群 － 7 編 － 8 章

8-2 金融分野における情報セキュリティ標準

（執筆者：岩下直行）［2009 年 3 月 受領］

8-2-1 暗号アルゴリズムの 2010 年問題への対応

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．そのなかでも現在特に広く利用されている 2-key トリプル DES，1024 ビット RSA，SHA-1 については，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．この問題は，「暗号アルゴリズムの 2010 年問題」と呼ばれている（2 章参照）．

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まとめた．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 [3] 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を取りまとめたスタンディング・ドキュメント [4] が公表された．この検討結果に基づき，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．1994～5 年当時，共通鍵暗号の事実上の国際標準であった DES の安全性低下について，TC68 の場で問題が提起され，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 [5] 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．

こうした問題に関する研究成果を 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に対する信頼性の維持に資するとともに，我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，重要な取り組みと考えられる．

8-2-2 金融業務における生体認証技術

偽造・盗難キャッシュカード犯罪など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，TC68 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，SC2/WG10 において標準化が進められた．ISO 19092 は，米国からの提案により，米国規格 ANSI X9.84 をベースとして，国際標準化が行われているものである．ISO 19092 は，銀行の顧客及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などについて規定している．本規格の審議に当たっては，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，我が国の金融機関において利用されている静脈認証（Vein Biometrics）に関する記述を追加するなど，我が国からも積極的に議論に参加している．

■11 群 － 7 編 － 8 章

8-3 金融分野における通信メッセージ標準

（執筆者：岩下直行）［2009 年 3 月 受領］

8-3-1 ISO20022 による通信メッセージの国際標準化

ISO 20022 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 ベースとするなど，新しい要素技術を採り入れながら，ユーザ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上の仕組みが備わっている．

ISO 20022 は，ほかの多くの国際標準とは異なり，標準化の対象である通信メッセージそのものを文書に記述するというアプローチを採用していない．これは，そのようなアプローチが迅速な標準メッセージの開発とメンテナンスを妨げてきたと認識されているためである．

その代わりに，①利用される基本的なデータ項目の辞書を整備し，②市場参加者のグループに標準を開発させ，③それをレポジトリと呼ばれるデータベースに登録させる，という手続きをとることで,「各市場の実情に合った業務モデルと標準メッセージをタイムリーに開発し，広く普及させる」というアプローチを採用している．

こうした迅速な標準化を進めるために，**表 8･2** に示す組織が構成されている．

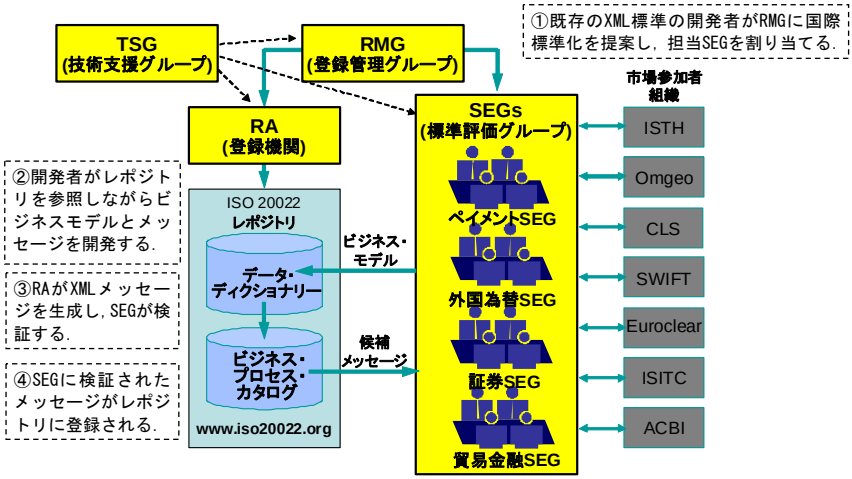
表 8・2　ISO 20022 の標準登録に関与する組織

① RMG（Registration Management Group，登録管理グループ）	ISO 20022 全体に関する意思決定機関．SEGs の任命・所掌範囲の確定，RA 及び SEGs の活動の監視など，登録手続全般を管理する役割を担う．年に 2 回，会合が開催されている．
② RA（Registration Authority，登録機関）	レポジトリの登録管理事務を実際に行う機関で，SWIFT がその事務を担っている．
③ SEGs（Standards Evaluations Groups，標準評価グループ）	登録依頼のあった通信メッセージの内容が業務上のニーズを満たすかを検証する役割を担う，各業務分野の専門家から構成された組織．
④ TSG（Technical Support Group，技術支援グループ）	RMG，RA 及び各 SEG に対して ISO 20022 における XML 実装やモデル構築に関する技術的支援を行う組織．

これらの組織が連携して行う，国際標準の登録プロセスは，**図 8･2** に示すとおりである．

欧米の金融業界では，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）の構築に向け，域内の小口決済インフラの共通化を進めている．そうした取組みのなかで，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，市場参加者が 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．

現在，ISO 20022 に基づくアプローチは，金融分野の幅広い領域で採用されている．ISO 20022 を採用したプロジェクトがすべて順調に進捗しているわけではないが，国際標準構築の新しい方向性として，広く根付きつつあるものと評価できる．今後，我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，戦略的見地から検討を行っていく必要がある．



"Introduction to ISO 20022 – UNIversal Financial Industry message scheme"(2008)を一部修正

図 8・2　ISO 20022 の登録プロセス

8-3-2 金融情報技術の国際標準化を巡る今後の課題

各国の金融業務の進め方は，各国の法令や金融制度，商慣習など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．また，我が国の金融機関においては，従来型のシステム開発技術によって，既に，完成度の高い金融情報システムが構築されており，それは国際標準を意識した設計になっていないという問題がある．このため，現段階で短期的にみれば，我が国の金融業界は，「国際標準に対応することが利益に繋がりにくい構造」となっている．

しかし，中長期的にみれば，国際的な金融情報システムは一つの方向に収斂していくものと考えられ，そうした潮流に我が国の金融業界もいずれはその影響を受けざるを得ないものと考えられる．我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，ISO/TC68 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，ますます重要となってくるものと考えられる．

■参考文献

1) 日本工業標準調査会（JISC），“第８次工業標準化推進長期計画，”日本工業標準調査会，1998.
2) 日本銀行，“金融情報技術の国際標準化について，”日本銀行調査季報，秋(10 月)号，2006.
3) 宇根正志・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，vol.25，no.s1，pp.31-72，日本銀行金融研究所，2006.
4) International Organization for Standardization (ISO), “Financial services—Recommendations on cryptographic algorithms and their use—Standing Document,” ISO, 2007.
5) Koji Kusuda and Tsutomu Matsumoto, “A Strength Evaluation of the Data Encryption Standard,” IMES Discussion Paper Series, vol.97-E-5, Bank of Japan, 1997.