IMES DISCUSSION PAPER SERIES

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

岩下直行・谷田部充子

Discussion Paper No. 98-J-29

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所
〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 98-J-29
1998 年 11 月

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

岩下 直行[*1]・谷田部充子[*2]

要　旨

金融業界においては、従来から、様々な金融業務に関する「標準化」が行われてきた。伝統的な紙ベースの金融業務では、手形、小切手の様式の統一が行われ、最近の電子的な金融業務では、金融ネットワークで利用されるデータ通信フォーマットやコード体系が標準化されている。こうした業務の標準化は、金融取引における不要な多様性を排除し、事務の合理化、安全性の向上に資するものである。

「標準化」は、情報セキュリティ技術の観点からも大きな意味を持っている。例えば、DES は、米国政府標準暗号（FIPS）に認定された結果、広く普及することができた。暗号アルゴリズムや情報セキュリティ技術は、高度な数学理論に基づくものが多いので、一般の利用者がその安全性や強度を見通すことは難しい。信頼できる機関が、安全性を十分に吟味した上で標準としてお墨付きを与えることによって、一般の利用者もその技術を安心して利用できるようになるのである。

国際標準化機構の金融専門委員会（ISO／TC68）では、金融業務に利用される国際標準を策定しているが、その多くは金融分野で利用される情報セキュリティ技術に関するものである。また、ISO／TC68 では、金融業務に利用される情報セキュリティ技術の安全性や標準化のあり方に関する検討も行っている。本検討作業の一環として、ISO／TC68 では、1994 年頃から DES の安全性に対する懸念を認識し、技術的な研究を進めると同時に、DES の後継暗号の必要性を訴えるポリシー・ステートメントを作成・発表してきた。こうした金融業界からの働きかけの効果もあって、米国では DES の後継として Triple DES の国内標準が策定され、米国政府も AES の標準化を開始した。

わが国の金融業界においても、ネットワーク上で金融業務の安全を確保する手段として、情報セキュリティ技術の重要性が高まってきている。わが国の金融業界が新しい情報セキュリティ技術の採用を検討する場合には、金融業務における国際標準化動向を踏まえて、国際的に整合性、説得性のある技術を採用していくことが必要と考えられる。

キーワード：国際標準化、情報セキュリティ技術、ISO、**暗号技術、**DES、Triple DES、AES
JEL classification: L86、L96、Z00

*1 **日本銀行金融研究所研究第** 2 **課**（E-mail: iwashita@imes.boj.or.jp）
*2 **日本銀行金融研究所研究第** 2 **課**（E-mail: mitsuko.yatabe@boj.or.jp）

本論文は、1998 年 11 月 4 日に日本銀行で開催された「金融分野における情報セキュリティ技術に関するシンポジウム」への提出論文に加筆・修正を加えたものである。

目　次

Ⅰ．はじめに

金融業界においては、従来から、様々な金融業務に関する「標準化」が行われてきた。伝統的な紙ベースの金融業務では、手形、小切手や各種帳票類の様式の統一という標準化が行われていた。最近の電子的な金融業務では、金融機関間のデータ通信フォーマット、金融機関コード、銀行取引カードのフォーマット等が標準化されている。こうした標準化は、金融機関間および金融機関－顧客間の金融取引において、不要な多様性を排除し、業務を円滑に行うために必要不可欠なものであり、金融機関の事務の合理化、安全性の向上や顧客サービスの向上にも資するものである。

ただ、従来のわが国で進められてきた金融業務の標準化は、国内・業界内を念頭に置いた標準化であり、国際標準との整合性に注意が払われることはあまりなかった。伝統的に、金融業務は各国の金融制度や取引慣行を反映した各国各様の書類や通信フォーマットが用いられているため、国際標準に合わせにくいという面がある。また、わが国の金融機関においては、国際的な金融取引を担当する特定の部署以外は、直接海外と金融取引を行うことは殆どなかったため、金融業務に関する海外との調和を意識する必要もあまりなかったものと思われる[1]。

しかし、情報技術革新に伴う内外市場の統合化、グローバル化の影響を受けて、わが国の金融業界においても、「国際標準」（グローバル・スタンダード）に対する認識が徐々に高まっている。わが国の金融機関は、信用リスクに対する銀行の自己資本比率規制の国際統一基準、IASC による国際会計基準、ISO 9000 や ISO 14000 による品質管理や環境管理の国際標準等、様々な領域において、グローバル・スタンダードへの対応が求められるようになっている。

金融業務面でも、金融の国際化、電子化の進展に伴い、「国際標準」の重要性が高まっている。手形や小切手の様式のような紙ベースの業務はともかく、コンピュータ・ネットワークを利用した金融機関間のデータ送受信や、磁気カード・IC カード等を用いたリテール金融取引等の分野については、既に海外との相互接続が可能となっているサービスもあり、金融ネットワークがオープンなものになっていけば、国際的な相互乗り入れが今後更に進むものと考えられる。わが国の金融業界における標準化に当っては、海外との調和、整合性を考慮する必要性が今後ますます高まってこよう。

「標準化」は、情報セキュリティ技術の観点からも大きな意味を持っている。代表的な共通鍵暗号である DES（Data Encryption Standard）や、その後継として選定作業が進んでいる AES（Advanced Encryption Standard）が「Standard」と名付けられていることからも明らかなように、暗号アルゴリズムなどの情報セキュリティ技術の普及においては、公的機関による標準化が大きな影響力を持つ。暗号アルゴリズムや情報セキュリティ技術は、高度な数学理論に基づくものが多いので、一般の利用者がその安全性や強度を容易には測定できない。信頼できる機関が安全性を十分に吟味した上で標準としてお墨付きを与えることによって、利用者がその技術を安心して利用できるようになるのである。DES は、米国政府が標準暗号（FIPS：Federal Information Processing Standards）に認定したことによって、安全な暗号として信頼され、広く普及することができた。次世代の米国政府標準暗号として選定作業が進められている AES の標準化においては、世界中の暗号学者が暗号アルゴリズムの提案やその評価に参加し、オープ

[1] 金融機関の国際部門における外為、貿易金融、外国証券取引等については、SWIFT の電文フォーマット等、デファクトの国際標準に基づいて業務が行われている。しかし、国際金融業務と国内金融業務とは切り離されており、国際標準に合わせて国内標準を変更していくとか、国内標準を国際的に利用可能なように働きかけるといった動きは見られてこなかった。

ンな議論を戦わせている。一般の利用者にとっては、専門家が策定した標準技術を利用することによって、高いセキュリティ水準を達成することが期待できる。

金融分野で利用される情報セキュリティ技術等の国際標準化は、国際標準化機構・金融専門委員会（ISO／TC68）が担当している。ISO／TC68 では、金融分野で利用される暗号アルゴリズムやそれを利用したプロトコル、鍵管理方式、IC カード、認証機関の業務の進め方等について国際標準化が進められている。従来、ISO／TC68 は、国際的な資金証券取引に利用されるコード体系やメッセージ・フォーマット、国際クレジットカードに利用される磁気ストライプ･カードの仕様といった金融機関の業務面について、国際的な相互運用性を確保するために国際標準化作業を進めていたが、最近は情報セキュリティ技術に関する国際標準化に軸足を移しつつある。

日本銀行は、通産省・工業技術院から委嘱を受け、ISO／TC68 の国内審議団体を務めている。本稿では、この ISO／TC68 における国際標準化活動を中心に、金融業務に利用される情報セキュリティ技術の国際標準化を巡る動向を整理したものである。

Ⅱ．国際標準を取り巻く環境の変化

１．標準化とは何か

「標準化」とは、何らかの技術について、その定義や仕様の統一を図ることを指す。一般には、業界内の複数の企業が協力して、「標準」あるいは「規格」と呼ばれる技術文書を作成し、それに基づく当該技術の実施が普及することにより達成される。標準化の目的は様々なものがあるが、主なものを整理すると以下のとおり。

①相互理解	関係者の間で、当該技術に関する用語や概念について、共通の理解を持つ。
②互換性の確保	同じ技術を用いて異なる生産者が製造した製品の間の互換性、相互運用性を保ち、異種機材間のインターフェースを確保する。
③多様性の調整	放置しておくと製品の仕様が不必要に多様化してしまう場合に、その種類を単純化してコントロールする。
④消費者利益の確保	標準に準拠していれば一定の性能や品質が保証される仕組みとすることにより、消費者の利益を確保する。
⑤新技術の普及	新しい技術を普及させるために、技術仕様を公開する。
⑥安全・環境の保護	製品が一定の安全規格、環境規格を満たしていることを保証することにより、消費者の安全を守り、環境を保護する。

２．様々な標準とその分類

「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順によって、次のような分類が可能である。

（強制規格、任意規格）

遵守することが法律などで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、電気用品取締法、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 などで定められている国際標準、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。

（国際標準、国内標準、業界標準）

当該標準が想定している対象地域が、世界全体か、特定の国家内か、特定の国家の特定の業界かによって、国際標準、国内標準、業界標準等に区分される。通常、国際標準とか国内標準という場合、デジュール標準を指すことが多い。

（デジュール標準とデファクト標準）

標準策定手続きに着目した分類。「デジュール標準（de jure standard、公的な標準）」とは、ISO や JIS 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より制定された標準を言い、「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言う。

	デジュール標準（公的な標準） de jure standard	デファクト標準（事実上の標準） de facto standard
定義	標準化機関により制定された標準	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
特徴	①策定プロセスが透明で標準内容が明確でオープン ②原則的に単一標準が提供される ③メンバーシップが比較的オープン	①策定プロセスの速度が迅速 ②標準の普及と製品の普及が同時 ③標準の一本化は市場での競争に委ねられる ④自規格を標準化できた者が市場を独占できる
欠点	①標準開発の速度が遅い ②標準の普及と製品の普及にタイム・ラグが存在 ③技術のフリーライドの発生	①情報公開が不完全 ・全インターフェイスの公開の保証なし ・技術情報の未開示のため複数方式の比較が困難 ・開発企業による競争限定的な囲込みが行われ、追随企業が不利な立場に置かれる懸念 ②メンバーシップが閉鎖的になりがち ③改正手続が不透明

出典：「今後の我が国の国際標準化政策の在り方」（日本工業標準調査会国際部会答申）、平成 9 年 11 月

３．デジュール国際標準の役割

VTR（VHS 対ベータ）、パソコン用 OS（マイクロソフト社対アップル社）などに代表される「規格戦争」は、通常はデファクト標準を巡る企業間の主導権争いである。電子機器業界や通信業界では、デファクト標準を制することが、市場シェアの拡大を通じて企業業績に直結する仕組みとなっている。このため、各企業にとって、デファクト標準を目指した製品開発を行うことが極めて重要となっている。

一方、ISO、JIS 等のデジュール標準は、関係者のコンセンサスを重視して標準の策定が進められ、標準化作業に長い時間が掛かることから、技術革新のスピードの速い産業においてはその実用性が低下しているとの指摘がある。しかし、産業分野や用途によっては、デジュール標準も引き続き広く利用されており、むしろその重要性が増大している分野も多い。例えば、消費者の安全保護対策や環境保護といった分野では、法令に基準の細目を定める代わりに、既存の国際標準の遵守を法令で義務付けることにより、国際標準を強制規格として活用しようとする動きがある。また、品質管理システム（ISO 9000 シリーズ）、環境管理システム（ISO 14000 シリーズ）のように、業種横断的に適用される管理システム標準が策定され、その適合性の有無を公共事業の入札等における取引先選定の条件に採用する動きがあり、こうした分野でデジュール標準の用途は拡大している。

また、電子商取引のように、広範な分野を対象とし、かつ、多様な利害関係者を含む場合には、構想の初期段階からデジュール標準の策定手続に基づいて標準化を進めることが必要となっている。国際標準化機関におけるデジュール標準策定は、デファクト標準と比べ標準策定に長期間かかるものの、策定プロセスが透明かつ公平であり、広範なメンバーのコンセンサスが得られるというメリットがあるため、デジュール標準の枠組みを活用して進められるケースが増えている。また、逆に ISO 等の国際標準化機関においても、コンソーシアム規格等のデファクト標準をデジュールの国際標準とする手続きが検討されるなど、国際標準策定の迅速化を図っている。このように、デジュール標

準とデファクト標準は、相互に補完し合いながらその重要性を増してきている。

本稿で紹介する ISO／TC68 における金融業務向けの情報セキュリティ技術関連のデジュール国際標準も、同様の意味で重要性が増加している国際標準といえる。

４．国内標準の国際標準への統合の動き

同じ技術分野で国毎に内容の異なる国内標準や国内標準が存在すると、国境を越えた物やサービスの貿易が阻害されてしまう。以前から、規格制度は、国際貿易における代表的な非関税障壁として問題となってきた。1967 年、欧州電気規格調整委員会（CENEL）が実施しようとした電子部品に対する閉鎖的な規格制度に対し、米国規格協会（ANSI）が非関税障壁となり得ることを指摘し、米欧間の貿易紛争に発展した事件が起こった。この事件を嚆矢として、東京ラウンド、ウルグアイ・ラウンドを通じて交渉が行われ、規格制度を貿易制限的に運用することを禁止する WTO（World Trade Organization）の国際貿易ルールが制定された。これが、WTO・TBT 協定[2]である。本協定では、WTO 加盟国に国際標準化の推進と基準・認証制度[3]の国際的調和を図ることを求めているほか、ある産品についてデジュールの国際標準が存在する場合、国内標準を策定する際には、当該国際標準をデジュールの国際標準を基礎とすることが義務付けられている。仮にこの協定に違反して、国内で独自の標準を策定、運用した場合、それによって損害を受けた国は、WTO に提訴することができる仕組みとなっている[4]。

こうした動きを背景に、わが国においても、国内標準の国際標準への統合が図られつつある。すなわち、新しい JIS（日本工業規格）等の国内標準の策定においては、原則として ISO 等の国際標準を基礎として行われることとなったほか、既存の国内標準のうち国際標準と整合的でないものについては、国内標準の改正が順次行われている。この結果、国際標準として規定された内容が、国内標準としてわが国の国民生活や産業活動に直ちに影響するようになっている。

---

[2] WTO･TBT 協定（Agreement on Technical Barriers to Trade）：WTO 協定の附属書 1A に含まれる協定類のひとつ。産品の規格及び規格への適合性の評価が、貿易に対する不必要な障害とならないことを確保することを目的としている。1979 年に GATT 東京ラウンドの一環として調印された後、ウルグアイ・ラウンドによって加盟国の義務を明確化する改定が加えられ、1995 年 1 月、現在の協定が発効している。

[3] 基準・認証制度：産品の特性（品質、性能、安全度、寸法など）を規定する規格および産品が規格に適合していることを、文書やマークの形で保証するための制度。

[4] 但し、TBT 協定はモノの貿易を対象としているため、現在のところ、金融などサービス分野には直接は適用されない。WTO 協定にはサービス貿易に関する一般協定（GATS、附属書 1B）が含まれているが、GATS には TBT 協定に相当する協定は置かれていない。

Ⅲ．金融業務の国際標準化の枠組み

１．金融業務の国際標準化のための機関

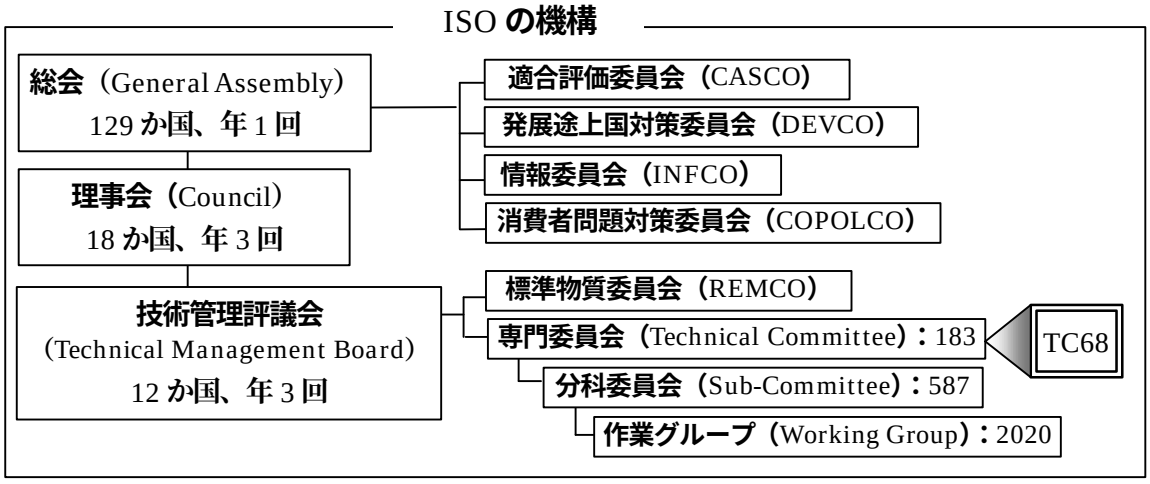
デジュール国際標準を策定する国際標準化機関には、
① 国際標準化機構（ISO：International Organization for Standardization）、
② 国際電気標準会議（IEC：International Electro-technical Commission）、
③ 国際通信連合（ITU：International Telecommunication Union） 等が存在する。

これらの機関の間の役割分担は、電気・電子工学関係を IEC が、通信関係を ITU が担当し、その他の分野を ISO が担当することとなっている。最近では、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を含む「情報技術」の標準化のウェイトが高まる傾向にあるが、この分野は、ISO と IEC とが共同で設立した共同専門委員会（JTC1：Joint Technical Committee 1）が国際標準化を担当している。金融業務に関する標準化は、ISO の活動の一部として行われている。

ISO は、工業製品やサービスに関する世界的な標準化活動を行うために 1947 年に設立された非政府間機構（本部はジュネーブ）であり、現在 129 か国が加入している。ISO の担当分野は、機械、化学、材料、建築等多岐にわたっており、各分野毎に専門委員会（TC：Technical Committee）が設置され、標準化作業を進めている。現在のところ、設置順に TC1（ねじ）から TC218（製材）まで 183 の専門委員会が活動している。

金融業務に利用される情報通信技術、特に情報セキュリティ技術に関する国際標準化は、こうした ISO の専門委員会の 1 つである TC68 において行われている。

ISO の機構



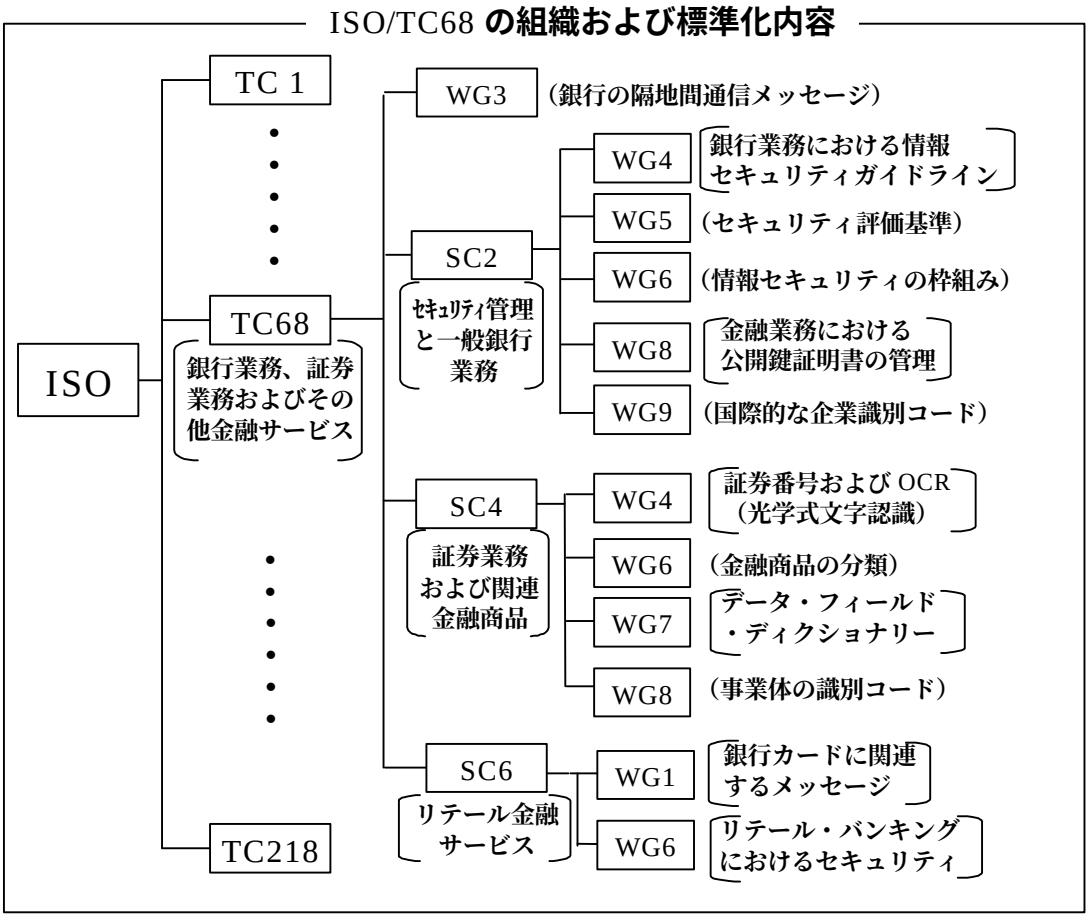
２．ISO/TC68 の組織

(1) TC68（銀行業務、証券業務およびその他金融サービス）

TC68 は、「銀行業務、証券業務およびその他金融サービス（Banking, Securities and Related 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に関する国際標準化を担当している。TC68 の下には、３つの分科委員会（SC：Sub-Committee）と１つの直属の作業グループ（WG：Working Group）が設置され、各分科委員会の下にも作業グループが設けられている。委員長は米国 CyberCash 社の Mark Zalewski 氏、事務局は ANSI（米国規格協会）が務めている。

TC68 への参加状況をみると、日本、米国、英国、フランス、ドイツ、オランダ、スウェーデン、韓国など２０か国が P メンバー（投票権を持つメンバー）となっており、ギリシア、中国など３０か国が O メンバー（投票権を持たないオブザーバー）となっている。このほか、ECBS（European Committee for Banking Standards）、国際決済銀行（BIS）、国際通貨基金（IMF）、SWIFT、Euroclear、国連欧州経済委員会（UN/ECE）、VISA インターナショナル、MasterCard インターナショナルなど１８機関がリエゾン団体（連携関係にある団体）となっている。

ISO/TC68 の組織および標準化内容



(2) SC2（セキュリティ管理と一般銀行業務）

SC2 は、「セキュリティ管理と一般銀行業務」を担当する分科委員会であり、下部組織として５つの作業部会を持つ。委員長は米国 Citicorp の Daniel Schutzer 氏、副委員長は米国 NSA[5]の Jerry Rainville 氏、事務局は ANSI（米国規格協会）が務めている。

主として、ホールセール・バンキングにおけるメッセージ暗号化の手順と暗号アルゴリズム（ISO 10126）、メッセージ認証の手順と使用アルゴリズム（ISO 8730、8731）、鍵管理の手順と使用アルゴリズム（ISO 8732、11166）、認証機関による公開鍵証明書の管理（ISO 15782）、情報セキュリティ・ガイドライン（ISO／TR 13569）等の国際標準を策定している。従来は、磁気インク文字の形状や通貨コードなど業務手続の標準化を行なっていたが、最近では金融ネットワークのセキュリティ面を中心に標準化を進めている。

SC2 への参加状況をみると、日本、米国、英国、フランス、ドイツ、オランダ、スウェーデン、など１４か国が P メンバーとなっているほか、ECBS（European Committee for Banking Standards）、VISA インターナショナル、SWIFT など１３機関がリエゾン団体となっている。

TC68
（金融業務専門委員会）

SC2（セキュリティ管理と一般銀行業務）		
	メンバー	日米英独仏蘭加ほか７か国
	委員長	Daniel Schutzer (Citicorp, US)
	副委員長	Jerry Rainville (NSA, US)
	事務局	ANSI (US)

WG4	作業項目	Information Security Guidelines for Banking
	主査	Jerry Rainville (NSA, US)
WG5	作業項目	Security Evaluation Criteria
	主査	Paul Faulkner (Barclays, UK)
WG6	作業項目	Framework study into IT Security
	主査	Duaf Oudheusden (De Nederlandsche Bank)
WG8	作業項目	Certificate Management for Financial Services
	主査	Blake Greenlee (US)
WG9	作業項目	International Business Entity Identifier
	主査	John Pritt (Dito International, Luxembourg)

[5] NSA（National Security Agency）：国家安全保障局。国防総省の下部機関で、米国の暗号政策の企画立案や標準策定に強い影響力を持つと言われている。

(3) SC4（証券業務および関連金融商品）

SC4 は、「証券業務および関連金融商品」を担当する分科委員会であり、下部組織として４つの作業部会を持つ。委員長はスイス UBS の Marcel Achermann 氏、事務局は SNV（スイス規格協会）が務めている。

主として、国際的な証券識別コード（ISO 6166）、証券取引に利用される電文メッセージ（ISO 7775、ISO 15022）など証券業務に関する国際標準を策定している。

SC4 への参加状況をみると、日本、米国、英国、ドイツ、フランス、スイス、イタリア、スペイン、ベルギー、スウェーデン、トルコ、など１５か国が P メンバーとなっているほか、SWIFT、Euroclear、Cedel など 8 機関がリエゾン団体となっている。

TC68
（金融業務専門委員会）

SC4 (証券業務および関連金融商品)		
	メンバー	日米英独仏加ほか９か国
	委員長	Marcel Achermann (UBS, Switzerland)
	事務局	SNV (Switzerland)

WG4		
	作業項目	Certificate Numbers and Optical Scanning
	主査	John Pritt (Dito International, Luxembourg)

WG6		
	作業項目	Classification of Financial Instruments
	主査	Nourredine Yous (Telekurs Financial Information, Switzerland)

WG7		
	作業項目	Data Field Dictionary
	主査	Patrick Brown (ISMA, UK)

WG8		
	作業項目	Identification of Business Entities
	主査	John Pritt (Dito International, Luxembourg)

(4) SC6（リテール金融サービス）

SC6 は、「リテール金融サービス」を担当する分科委員会であり、下部組織として 2 つの作業部会を持つ。委員長はフランス Credit Lyonnais の Alain Cohen-Aloro 氏、事務局は AFNOR（フランス標準化協会）が務めている。

主として、金融取引用の IC カード仕様 （ISO 9992、ISO 10202 等）や、クレジットカード取引用の通信メッセージ・フォーマット（ISO 8583 等）の国際標準を策定してきたが、最近ではリテール金融業務における情報セキュリティ技術や電子商取引の標準化に力を入れている。

SC6 への参加状況をみると、日本、米国、英国、フランス、ドイツ、オランダ、スウェーデン、など１５か国が P メンバーとなっているほか、SWIFT、VISA インターナショナルなど５機関がリエゾン団体となっている。

TC68
（金融業務専門委員会）

SC6 （リテール金融サービス）	メンバー	日米英独仏加ほか９か国
	委員長	Alain Cohen-Aloro (Credit Lyonnais, France)
	事務局	AFNOR (France)

WG1	作業項目	Financial transaction cards originated messages
	主査	Bonnie Howard(American Express, US)

WG6	作業項目	Security in Retail Banking
	主査	Mark Zalewski (CyberCash, US)

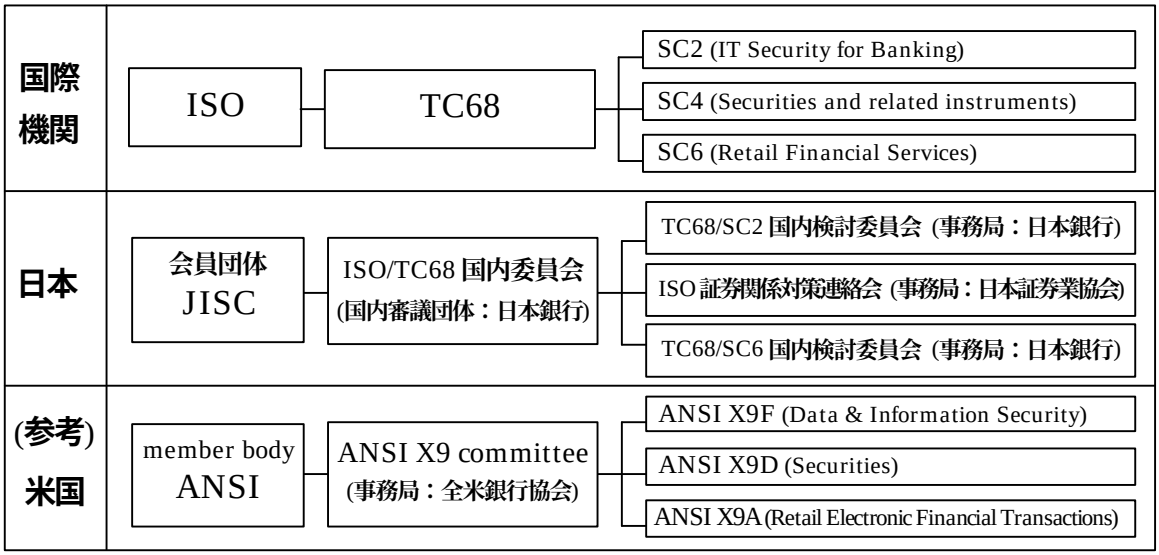
３．ISO／TC68 に対応するわが国の国際標準化活動

(1) ISO／TC68 国内委員会の活動

ISO には、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、わが国からは日本工業標準調査会（JISC）[6] が 1952 年に加入している。

JISC は、ISO の各専門委員会（TC）毎に研究団体、業界団体等に国内意見の取りまとめ等を行う国内審議団体を委嘱している。金融業務に関する TC68 については、日本銀行が国内審議団体の委嘱を受けている（事務局は金融研究所）。日本銀行は、国内の銀行、証券会社、金融界の諸団体・機関、メーカー、通信事業者、学者、官公庁等をメンバーとする ISO／TC68 国内委員会（委員長：南部鶴彦学習院大学教授）を定期的に主催しているほか、関連する国際会議への出席や、国内意見の取りまとめ等を行っている。

ISO／TC68 の下に設置された３つの分科委員会（SC2、SC4、SC6）についても、対応する国内検討委員会ないし連絡会が組成されている。３つの分科委員会のうち、SC4（証券業務）については、日本銀行から国内における事務局事務の委嘱を受けた日本証券業協会が、連絡会の事務局を務めており、SC2 と SC6 については日本銀行が国内委員会の事務局を務めている。これら３つの国内検討委員会、連絡会では、国内の金融機関、メーカー等の参加を得て、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。



[6] 日本工業標準調査会（JISC）：工業標準化法に基づき、通商産業省工業技術院に設置された通商産業大臣の公的諮問機関。240 名の専門家からなる委員会構成の組織で、日本工業規格（JIS）制定のための調査・審議を行うほか、ISO、IEC 等の国際機関の会員団体として国際標準活動に参加する機能を持つ。実際の JIS 原案の作成や国際標準化対策活動は、産業分野毎に JISC から委嘱を受けた標準化委員会、国内審議団体に委ねられている。

(2) 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 関連で、国内でリエゾン関係を持っているのは、ISO／IEC JTC1[7]の分科委員会である SC27 と SC17／WG4 である。

① JTC1／SC27

JTC1／SC27 は、汎業界的な情報セキュリティ技術の国際標準化を担当している。その国内委員会である SC27 専門委員会は、JTC1／SC27 の国内審議のために情報処理学会が事務局となって組成された委員会で、国際標準原案に関する投票や国際会議への対応方針を討議している。委員長は、慶応大学環境情報学部の苗村憲司教授が務め、国内主要電機メーカーや通信機事業者が委員となっている。

SC27 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 WG1、暗号技術を担当する WG2、セキュリティ評価基準を担当する WG3 の３つの WG があり、SC27 専門委員会は、各 WG に対応する国内委員会での審議を取り纏め、日本としての案件審議を担当している。

TC68 と SC27 は国際レベルで密接な提携関係にあり、毎年、主要メンバーによる共同会合を開催している。国内レベルでも、ISO／TC68 国内委員会から SC27 専門委員会へのリエゾン（連繋役）として日本銀行（ISO／TC68 国内審議団体）の委員が参加しているほか、暗号技術を担当する SC27／WG2 検討委員会へもリエゾン参加している。

② JTC1／SC17／WG4

JTC1／SC17 は、識別カードの国際標準化を担当しており、その作業部会である WG4 は、外部端子付きの IC カードの国際標準化を担当している。その国内委員会である SC17／WG4 国内委員会は、JTC1／SC17／WG4 の国内審議のために日本事務機械工業会が事務局となって組成された委員会で、国際標準原案に関する投票や国際会議への対応方針を討議している。主査は、富士通(株)の松本勉氏が務め、IC カードおよび読取機の国内主要メーカーとユーザーが委員となっている。

ISO／TC68 国内委員会からは、SC17／WG4 国内委員会にリエゾンとして日本銀行の委員が参加している。

[7] ISO/IEC JTC1：ISO（International Organization for Standardization）と IEC（International Electro-technical Committee）が共同で設立した、情報技術の国際標準化を担当する技術専門委員会（JTC1：Joint Technical Committee 1）。JTC1 では、プログラミング言語からシステム・デバイスまで、様々な技術標準を策定している。

４．国際標準策定のプロセス

ISO の国際標準は、次のような策定プロセスを経て作成される。

① 新たな国際標準の作成を希望する参加国またはリエゾン団体は、「NP（新業務項目提案）」を提案することができる。NP は、郵便による投票、もしくは会議（専門委員会または分科委員会）の決議により、P メンバーの過半数による同意が得られ、かつ最低５か国以上が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。

② 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・リーダーが指名され、作業グループにおいて「WD（作業原案）」の作成が進められる。

③ WD の作成作業が完了すると、専門委員会または分科委員会に回付され、「CD（委員会原案）」として中央事務局に登録される。委員会原案は賛否の意見を問うため、全ての参加国（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郵便による投票を行なう。

④ CD の国際会議における審議により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３分の２以上の賛成が得られた場合には、「DIS（国際標準案）」として登録される。

⑤ DIS は全ての参加国（P メンバーおよび O メンバー）に回付され、投票を行い、必要に応じて原案を修正する。委員会審議に参加する国の 2/3 以上の賛成、かつ反対が投票総数の 1/4 以下であることが承認の要件となる。

⑥ DIS が承認されると、「FDIS（国際標準最終案）」として、全ての国に回付され、２ヵ月間投票を行う。この段階では、標準内容の修正は不可能であり、賛成か反対かのみを回答する。委員会審議に参加する国の 2/3 以上の賛成、かつ反対が投票総数の 1/4 以下であることが承認の要件となる。承認された場合、「IS（国際標準）」として中央事務局から発行される。

⑦ CD または DIS としての投票は、反対意見との調整を行なうため、原案に修正を加えつつ、複数回行われることもある。

このように、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、各国の意見を盛込むための修正が加えられるプロセスでコンセンサスが形成され、国際標準が完成する仕組みとなっている。なお、全ての国際標準は、発行後の技術進歩や情勢変化に対応するため、５年毎に定期的な見直しが行なわれるほか、制定されてから 10 年以上経過した国際標準を見直す場合は、技術の変化に伴って標準化の必要性がなくなっていないかを確認する仕組みとなっている。

プロジェクトの段階	関連文書	
	名称	略号
1. 提案段階	新業務項目提案 (New work item Proposal)	ＮＰ
2. 作成段階	作業原案 (Working Draft)	ＷＤ
3. 委員会段階	委員会原案 (Committee Draft)	ＣＤ
4. 承認段階	国際標準案 (Draft International Standard)	ＤＩＳ
5. 最終投票段階	国際標準最終案 (Final Draft International Standard)	ＦＤＩＳ
6. 発行段階	国際標準 (International Standard)	ＩＳ

５．TC68 で策定された情報セキュリティ関連の国際標準の概要

ISO／TC68 では、以下のような情報セキュリティ関連の国際標準を策定している。

国際標準の名称	概要説明
メッセージ認証のための必要案件（ISO 8730）	大口金融取引において、送信者がメッセージに MAC（Message Authentication Code、共通鍵暗号を用いて計算した認証子）を付加して送信し、受信者が MAC を確認する方法が規定されている。
メッセージ認証のためのアルゴリズム（ISO 8731）	ISO 8730 において用いられる MAC 生成のための暗号アルゴリズムが規定されており、ANSI X3.92 を引く形で DES が国際標準化されている。
暗号鍵の管理（ISO 8732）	大口金融取引において、共通鍵暗号による秘密通信の安全性を確保するための暗号鍵の管理方式について、運用管理の原則や手順を規定している。
PIN 管理とセキュリティ（ISO 9564-1）	銀行カードによるリテール金融取引で PIN（暗証番号）を利用する場合のセキュリティの原則について規定した国際標準。PIN の長さ（4 桁～12 桁）、PIN を転送・保管する場合には、ISO9564-2 に規定された暗号アルゴリズムで暗号化すること等が規定されている。
PIN 管理とセキュリティ：暗号ｱﾙｺﾞﾘｽﾞﾑ（ISO 9564-2）	ISO 9564-1 において用いられる PIN の秘匿のための暗号アルゴリズムが規定されており、ANSI X3.92 を引く形で DES が国際標準化されている。
IC カードと端末間のメッセージ（DIS 9992）	IC カードをリテール金融取引に用いるための、カードと端末の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）とメッセージを規定したもの。
メッセージ暗号化手順（ISO 10126-1）	大口金融取引においてメッセージの内容を部外者から秘匿するための暗号化の手法につき規定している。暗号化のプロセス等の一般原則、暗号化するデータのパディング方法等を規定している。
メッセージ暗号化手順：暗号ｱﾙｺﾞﾘｽﾞﾑ（ISO 10126-2）	ISO 10126-1 において用いられるメッセージ秘匿のための暗号アルゴリズムが規定されており、ANSI X3.92 を引く形で DES が国際標準化されている。
IC カードを利用した金融取引システムのセキュリティ対策（CD 10202）	リテール金融取引に用いられる IC カードのコピー、改竄、偽造等を防止するために、IC カード、端末、ネットワーク、ホスト・コンピュータ等を含めたシステム全体におけるセキュリティ確保のあり方について規定したものである。
サイン・オン認証（ISO 11131）	金融機関のシステムに対し、取引先等が回線を通じてアクセスする際に、それが正当な端末または権限者であるか否かを確認する相手認証の手法につき規定している。
公開鍵ｱﾙｺﾞﾘｽﾞﾑの利用による鍵管理（ISO 11166-1）	SWIFT が USE（User Security Enhancement）で採用したセキュリティ機構を標準化したもので、大口金融取引において公開鍵アルゴリズムを利用して暗号鍵の配送を行う方式について規定している。
公開鍵ｱﾙｺﾞﾘｽﾞﾑの利用による鍵管理：RSA 暗号ｱﾙｺﾞﾘｽﾞﾑ（ISO 11166-2）	ISO 11166-1 において用いられる鍵配送のための公開鍵暗号アルゴリズムが規定されており、RSA 暗号方式の仕様と鍵ペアの生成方法等が規定されている。
安全な暗号装置（ISO 13491）	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（SCD）に要求される機能について規定している。

Ⅳ．ISO／TC68 における情報セキュリティ標準化を巡る話題

１．DES の強度低下と金融業界の対応

(1) DES 問題の背景

DES は、現在、世界で最も広く普及している共通鍵暗号であり、特に金融分野においては、欧米を中心に幅広い業務において DES が利用されてきた。しかし、DES はその鍵長が 56bit と短く、近年のコンピューター技術の発達とコスト・パフォーマンスの改善により、全数探索法による攻撃の脅威が深刻化してきている。また、従来 DES を利用する上での「信用状」と考えられてきた米国政府標準暗号（FIPS）としての認定が、本年限りで終了することが確実な情勢となり、その後継暗号の選択が深刻な問題となっていた。

現在、TC68 で制定されている国際標準にも、ホールセール分野で利用される MAC（ISO 8730）、鍵管理（ISO 8732）から、リテール分野で利用される PIN（暗証番号）の暗号化（ISO 9564）まで、DES の使用を前提としたものが多数存在するが、DES への信任の低下を受けて、これらの標準を「アルゴリズムを特定しない標準」に改正していくことが必要となっている。

(2) ISO／TC68 における DES 問題への取り組み

ISO／TC68 では、1994 年 6 月の ISO／TC68／SC2 総会において、米国代表より、DES の強度低下に関する問題提起が行われて以来、DES の後継暗号問題が最大の論点のひとつとなった。ISO／TC68／SC2 では、金融分野で利用可能な DES の後継暗号の必要性を訴える政策ステートメント「ISO／TC68 Cryptographic Development Policy」を 1995 年 4 月に作成・発表し、DES 後継暗号に対する金融機関のニーズを関係方面に働きかけてきた。こうしたの作業の一環として、日本からは、1996 年秋に、DES の強度評価に関する技術レポートを ISO／TC68 宛に提出した。当該技術レポートでは、DES に対する攻撃法を網羅的に分析した上で、遅くとも 2000 年までには、現実的な費用で、専用解読装置を用いた全数探索法によって短時間のうちに DES を解読することが可能となることを指摘している（本レポートは、後に Kusuda, Matsumoto [1997]として刊行された）。

こうした提言を積み重ねた結果、DES 以外の暗号技術の標準化が進むとともに、1997 年には米国政府が AES（Advanced Encryption Standard）の標準化を開始するなど、金融業務で利用できる暗号技術の選択肢は広がりつつある。特に、DES から AES に移行するまでの中継ぎとしてその有用性が広く認識されている Triple DES について、米国金融業界による国内標準化作業において ANSI X9.52 としての標準化がほぼ完了している。この Triple DES 標準は、今後 FIPS に認定される見通しであるほか、ISO／TC68 において国際標準化が行われる予定である。

(3) DES の強度低下と欧米の金融機関業務への影響

ISO／TC68 に参加する委員は、各国で金融機関の情報セキュリティ対策の実務に携わっており、国際会議において、標準化された技術に関する各国の対応状況を報告し合っている。そうした各国報告によれば、従来、DES に大きく依存していた欧米の金融機関の情報セキュリティ対策は、DES の信頼性の低下に伴い大きな変化が生じており、従来の DES から、Triple DES や公開鍵暗号を利用するものに移行しつつある。

米国では、全米銀行協会と主要民間銀行が中心となって、経営レベルで DES 問題へ

の対応が討議されている。米国では、ホールセール分野における EFT や証券取引のための銀行間通信に DES が利用されているほか、リテール分野でも、CD、ATM、POS 端末と銀行のホスト・コンピューターとの間で PIN（暗証番号）を送受信する際に、DES による暗号化が施されている。1998 年 7 月にハードウェアによる DES 解読装置の開発が報道され、DES の強度に対する信頼性の低下が決定的なものとなった結果、米国銀行業界では、ホールセール分野、リテール分野の双方で、現在 DES が利用されている部分を Triple DES に移行することが急務と認識されるようになった。特に、リテール分野では、全米の CD、ATM、POS 端末のうち、1/3 は新しいソフトウェアをダウンロードすることで、1/3 は機器の補修により Triple DES への対応が可能であるものの、残る 1/3 については機器の更新が必要であり、Triple DES 化には膨大な費用が必要と見積もられている。

欧州でも、ホールセール、リテールとも、Triple DES への移行が盛んに行われている。例えば、英国では、銀行間の決済ネットワークである CHAPS[8]について、DES から RSA による鍵配送と Triple DES による回線暗号を組合せた方式に移行している。ドイツでも、1997 年末までに、CD、ATM で PIN の暗号化に利用する暗号を DES から Triple DES に変更している。

[8] CHAPS（Clearing House Automated Payment System）：英国における銀行間のポンド建て大口資金の振替を行うネットワークシステムで、英国の 14 の決済銀行が共同設立した CHAPS and Town Clearing Company によって運営されている。CHAPS で取引された為替の資金決済はイングランド銀行の決済口座によって実行されており、1 日の平均為替取扱高（1996 年）は約 1 千億ポンドである。

２．金融機関による認証業務の国際標準化

(1) 金融業務と公開鍵インフラ

従来の金融業務の電子化は、金融機関間のクローズドなネットワークを利用するものが多く、参加者の数も限られていたため、情報セキュリティ技術としては、主に DES 等の共通鍵暗号が利用されてきた（ISO 8730、10126 等）。SWIFT 等、一部の金融ネットワークにおいて公開鍵暗号が鍵配送のために利用される例はあったが（ISO 11166）、数年前までは、金融業務で電子署名が利用される例は世界的にも多くはなかった。

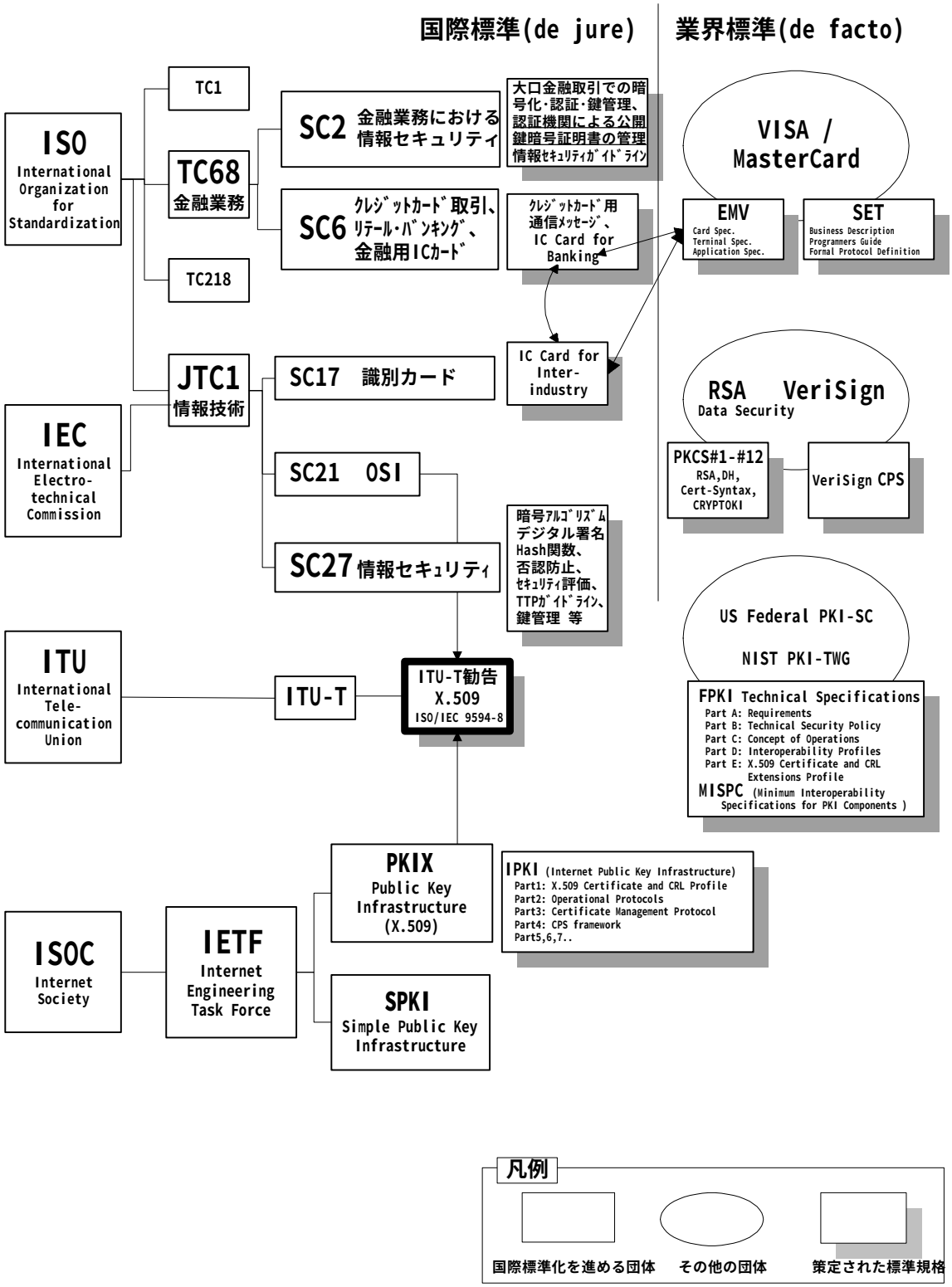
しかし、最近のインターネットの発達に伴い、オープンなネットワークで金融サービスを提供する金融機関が急速に増えている。これらのケースでは、利用者の認証に公開鍵暗号による電子認証技術を利用することが多い。公開鍵暗号を利用する場合、各利用者は自分の秘密鍵と公開鍵のみを管理すればよいため、利用者が膨大となるオープンなネットワークにおいては、伝統的な共通鍵暗号と比べて利便性が高いからである。ただし、各利用者の公開鍵が正当であることを確認するための仕組みとして、公開鍵インフラを構築することが必要となる。

公開鍵インフラ（PKI：Public Key Infrastructure）とは、認証機関（CA: Certification Authority）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。

公開鍵インフラはオープンなネットワーク上に構築されるため、多くのシステム管理者による相互運用性が大切であり、標準化が重要な役割を果たす。「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 勧告が存在するほか、PKI を巡っては、世界中で様々な技術開発や標準策定が進められている（関連する国際標準、国内標準、業界標準との関係については、次ページ「情報セキュリティ技術、認証技術に関する国際標準化活動の鳥瞰図」参照）。

ISO／TC68 では、こうした公開鍵インフラを金融機関が業務に利用する際に、CA が果たすべき機能、責務等を技術的な観点から規定として、「認証機関による公開鍵暗号証明書の管理」（ISO/CD 15782）の標準化を進めている。

情報セキュリティ技術、PKI技術に関する国際標準化活動の鳥瞰図



(2) 認証機関運営における情報セキュリティ技術の重要性

電子認証については、その法的効力の問題や、CA への公的規制の導入の是非等を巡って、わが国でも様々な議論が行われており、「電子決済に係る電子認証業務を電子決済サービスの一環として銀行が担うべき」[9]といった意見もある。しかし、こうした議論の基礎となる CA の業務内容、特にその技術的側面については、これまで十分には検討されてきていない。例えば CA の担い手の適格性について、「適切な認証サービスの提供ができる技術的な能力」が必要[10]という点ではコンセンサスがあるものの、具体的にどのような技術的能力が必要とされるのかは明確ではなかった。

わが国の金融機関のシステムは、クローズト・ネットワーク環境において、システムへの物理的なアクセスを制限することを主たるセキュリティ対策と位置付けてきたため、CA を利用した電子認証業務を行おうとする場合、従来と同じ手法ではシステムの安全性を守ることはできない。金融機関は、新しい環境・技術を正確に理解して、適切なセキュリティ対策を講じることが必要となる。そのような適切な対応の可否が、電子認証業務の担い手の「技術的能力」を形成するものと考えられる。

(3) ISO/CD 15782 の特徴

ISO/CD15782 は、金融業務における電子認証の実用化を念頭に策定されているもので、以下のような特徴を持つ。本国際標準原案は、現在 CD 段階であり、今後１～２年の時間を掛けて、国際標準化が進められる予定である。

① リスクの高い金融業務において利用される CA を想定し、採用すべき高度なセキュリティ技術を具体的かつ詳細に規定している。
   —— 例えば、CA の秘密鍵を安全に保管するために耐タンパー性を持ったハードウェア装置を利用することや、採用する電子署名アルゴリズム、ハッシュ関数の詳細仕様の標準化、鍵生成等におけるパラメータの特定等が規定されている。
② 技術的な観点から電子認証業務に関わる各主体の義務と責任とを明確化している。
   —— 具体的には、CA の業務内容が業務の手順毎に詳細に規定され、各段階で CA が実施すべきこと、証明書利用者が実施すべきこと等が明確にされている。
③ 米国の銀行業界が中心となって、実務的な要請から企画された標準であり、今後 ISO 標準として国際的に利用されていく蓋然性が高い。
   —— インターネットを利用した CA 業務の場合、インターネットが国境のないオープンなネットワークであるだけに、その中で提供されるサービスやセキュリティの基準について国際的な調和が必要とされるケースが多く、ISO 等のデジュール標準の枠組みが利用される可能性も高いと考えられる。
④ 暗号技術の専門家が標準策定に参画しており、最新の情報セキュリティ技術を十分考慮した規定内容となっている。
   —— 米国金融業界からの依頼により、暗号技術、情報セキュリティ技術を専門とする複数のベンチャー企業が、直接標準策定作業に参加している。

---

[9] 「電子マネー及び電子決済に関する懇談会」報告書　第６章 電子マネー・電子決済の担い手 ２．電子決済に係る認証機関 (3)金融機関による認証サービス

[10] 「電子マネー及び電子決済に関する懇談会」報告書　第６章 電子マネー・電子決済の担い手 ２．電子決済に係る認証機関 (1)ネットワークにおける認証機関の役割と適格性

３．金融機関の情報セキュリティに関するガイドラインと評価基準

(1) 金融機関の情報セキュリティ対策の実践と評価

金融機関の情報セキュリティ対策は総合技術であるため、それを円滑に実践するための行動指針や、実施したセキュリティ対策を評価するための枠組みが必要である。ISO／TC68 では、金融機関の行動指針として、情報セキュリティ・ガイドライン（ISO/TR 13569、Information security guideline）を用意している。また、セキュリティ対策を評価する枠組みについては、欧米主要国の策定した情報セキュリティ評価基準の国際標準である Common Criteria の利用や、英国の国内標準である BS 7799 の利用が提案されている。

(2) 情報セキュリティ・ガイドライン（ISO/TR 13569）

ISO/TR 13569 は、ISO／TC68／SC2／WG4 が作成し、常時アップデイトしている「技術報告書（TR: Technical Report[11]）」であり、ISO／TC68 で規定された情報セキュリティ対策の国際標準をサーベイする形で、金融機関が業務を進める上で必要となる情報セキュリティを確保するための指針を提供している。

具体的には、金融機関が情報を適切に管理するための手段として、①情報管理の方針を明確に規定したセキュリティポリシーの策定、②情報セキュリティ管理責任者の設置、③セキュリティ・プログラムに関する研修の実施等が列挙されている。また、暗号技術の利用についても、利用すべき標準を明示した上で、その詳細な手引きが記載されている。

また、最近の DES の信頼性の低下を受けて、より信頼できる暗号アルゴリズムへの移行を進める観点から、次回の改定において、「TC68 が推奨する最短鍵長」について本ガイドラインに記述することとなっている。本件については、1998 年 7 月の TC68／SC2 総会において検討が行われ、既に 56bit の共通鍵暗号に対する信任が揺らいでいること、今後の技術進歩を織り込んでいく必要があることから、共通鍵暗号 80bit、楕円曲線暗号 160bit、その他の公開鍵暗号 1024bit を「推奨最短鍵長」として、本ガイドラインに織り込むこととなった。

(3) 情報セキュリティ評価基準

情報セキュリティ評価基準とは、コンピュータのハードウェアやソフトウェアに関する情報セキュリティの水準を、統一化された基準書に基いて、第三者機関が評価・認定するための基準のことである。セキュリティ評価に関する取り組みは、欧米主要国で特に進んでいたが、そこで利用される評価基準やその運用が各国別に区々[12]であるため、国際的な相互運用性に欠けるとの批判があった。そこで、1994 年から、米国、カナダ、英国、フランス、ドイツ、オランダの６か国のセキュリティ評価担当機関が CCIB（Common Criteria Implementation Board）と呼ばれる協議会を組成し、これらの評価基準を統一しようとする「Common Criteria プロジェクト」が開始された。1998 年 5 月には、Common Criteria Version 2 が完成し、インターネット上で公開されている。

---

[11] Technical Report：ISO で策定される技術的な情報で、ISO の国際標準とはなりにくいが、情報として公表することが適当と判断された場合に公表、発行される技術報告書。

[12] 現在、米国では、国防総省の下部機関である NCSC（National Computer Security Center）が TCSEC（Trusted Computer Security Evaluation Criteria）に基いてコンピューター機器のセキュリティ評価を担当している一方、欧州では、英独仏の評価基準を統一した ITSEC（Information Technology Security Evaluation Criteria）に基いて民間のコンサルタント会社等がセキュリティ評価・認定ビジネスを営業している。

現在、ISO/IEC JTC1/SC27 では、Common Criteria を SC27 の国際標準（ISO/IEC 15408）として認定することが提案されている。

ISO／TC68 では、金融業務に利用可能な情報セキュリティ評価基準の要否を、ISO／TC68／SC2／WG5 において検討していたが、Common Criteria の国際標準化作業が円滑に進んでいることから、金融業界独自の基準を設けるのではなく、Common Criteria における IC カードの Protection Profile[13]等について、金融業界としての要件を検討していく方針に変わりつつある。

また、金融機関等によるセキュリティ・マネージメントについて、第三者機関がチェックする枠組みとしては、主に欧州の金融機関の間で、英国の国内標準である BS 7799（Code of Practice for Information Security Management）が利用されている。この標準は、情報セキュリティ技術の利用者である企業が、各種の情報セキュリティ技術を組み合わせて金融業務の安全対策を講じる場合、そのシステム全体の運営管理が適切であるかについて第三者機関が評価・認定する仕組み。現在、英国では、BS 7799 を一部改定して、ISO 9000 のように、認定に合格した企業を認証し、お墨付きを与えるための制度が構築されている。

[13] Protection Profile：Common Criteria を実際の情報機器に適用するために、その機器の種類（例えば、IC カード、firewall 等）毎に利用者が定めた詳細なセキュリティ保護要件。

Ｖ．おわりに

これまで、わが国の金融業界では、磁気カードの仕様、銀行間通信プロトコル等、業務に利用される技術規格を業界内の申合せとして策定してきており、国内における標準化はある程度進められてきたと言える。また、金融機関が利用する情報機器の安全対策については、通産省や金融情報システムセンターが基準を策定し、それを監査する仕組みも作られている。

しかし、こうした技術規格や安全対策基準では、ISO／TC68 などで策定されている国際標準を意識したものは少なかった。これは、そもそも ISO 等の国際標準が欧米諸国の主導により作られたものであり、わが国での利用には適さないと考えられてきたことも大きいと考えられる。各国の金融業務の進め方は、法令や金融制度、顧客の商慣習等を踏まえて形作られてきたものであり、金融業務にローカルな部分が残る限り、一律に国際標準に収斂していくというものではない。実際、欧米諸国の金融業界でも、ISO／TC68 の国際標準をそのまま採用することはむしろ稀であり、自国用に修正して利用しているケースも多い。

わが国の金融業界の立場からすると、金融業務に関する国際標準のうち、最低限、情報セキュリティ技術に関連するものについては、最新の技術動向を注視しておく必要があると考えられる。国際的に相互接続されたネットワークの一部を構成するわが国の金融ネットワークの安全を守るという観点からは、国際的な整合性、説得性のあるセキュリティ対策を講じていく必要があるからである。こうした観点から、わが国の金融業界としても、今後の情報セキュリティ技術の国際標準化を意識しておくことが重要と考えられる。

以　上

【参考文献】

浅羽茂、『競争と協力の戦略』、有斐閣、1994 年

今井秀樹、『暗号のおはなし―情報セキュリティの新しい鍵―』、日本規格協会、1996 年

岩下直行、「金融業務に利用される暗号技術と国際標準化」、『金融財政』、時事通信社、1998 年 6 月

岩下直行・宇根正志、「キーリカバリー構想を巡る最近の情勢について」、日本銀行金融研究所ディスカッションペーパーシリーズ、No. 97-J-8、1997 年

宇根正志･太田和夫、「共通鍵暗号を取り巻く現状と課題― DES から AES へ」、日本銀行金融研究所 情報セキュリティ･シンポジウム提出論文、1998 年 11 月

宇根正志･岡本龍明、「公開鍵暗号の理論研究における最近の動向」、日本銀行金融研究所 情報セキュリティ･シンポジウム提出論文、1998 年 11 月

大蔵省銀行局･国際金融局、『電子マネー及び電子決済に関する懇談会報告書』、1997 年 5 月

大蔵省銀行局、『電子マネー及び電子決済の環境整備に向けた懇談会報告書』、1998 年 6 月

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準』、1998 年 7 月

金融情報システムセンター、『平成 10 年版 金融情報システム白書』、財経詳報社、1997 年 2 月

情報技術標準化研究会、『情報技術の標準化』、オーム社、1986 年

通商産業省、『コンピュータウイルス対策基準』、通商産業省告示第 429 号、1995 年 7 月

通商産業省、『コンピュータ不正アクセス対策基準』、通商産業省告示第 362 号、1996 年 8 月

通商産業省、『平成十年版 通商白書』、大蔵省印刷局、1998 年

電気通信技術審議会 標準化政策部会、「高度情報社会を展望した電気通信の標準化に関する基本方策」、1997 年

中北徹、『世界標準の時代』、東洋経済新報社、1997 年

中山靖司･太田和夫･松本勉、「電子マネーを構成する情報セキュリティ技術と安全評価」、日本銀行金融研究所 情報セキュリティ･シンポジウム提出論文、1998 年 11 月

名和小太郎、『技術標準対知的所有権』、中公新書、1990 年 2 月

日本銀行金融研究所「金融業務における国際標準化の動向」、『日本銀行月報』、1992 年 8 月

日本工業標準調査会国際部会、「今後の我が国の国際標準化政策の在り方」、1997 年

藤田昌宏・河原雄三、『国際標準が日本を包囲する』、日本経済新聞社、1998 年

松本勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、日本銀行金融研究所情報セキュリティ・シンポジウム提出論文、1998 年 11 月

溝口道郎・松尾正洋、『ウルグアイ・ラウンド』、日本放送出版協会、1994 年 7 月

山田英夫、『デファクト・スタンダード』、日本経済新聞社、1997 年

American National Standards Institute, "X3.92 ― 1981, Data Encryption Algorithm," 1981.

American National Standards Institute, "X9.52 ― 1998, Triple Data Encryption Algorithm Mode of Operation," 1998.

Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation, Version 2.0," May 1998. (http://www.radium.ncsc.mil/tpep/library/ccitse/)

D. Coppersmith, C. Holloway, S. M. Matyas, and N. Zunic, "The Data Encryption Standard," Information Security Technical Report, Vol. 2, No.2, pp. 22-24, ZERGO, 1997.

D.W. Davies and W.L. Price, “Security for Computer Networks — An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,” Second Edition, John Wiley & Sons, 1989.

Electronic Frontier Foundation, “Cracking DES — Secrets of Encryption Research, Wiretap Politics & Chip Design,” O'Reilly & Associates, May 1998.

European Committee for Banking Standards, "Secure Banking over the Internet," March 1997

ISO／TC68／SC2, "ISO／TC68 Cryptographic Development Policy," April 1995.

ISO／TC68／SC2, ISO／TR 13569 "Banking and related financial services – Information security guidelines," October 1997.

ISO／TC68／SC2, ISO／CD 15782-1 "Banking — Certificate Management Part 1: Public Key Certificates," October 1998.

ISO／TC68／SC6, ISO 9564-1 "Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques," 1991.

ISO／TC68／SC6, ISO 9564-2 "Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment," 1991.

ISO／TC68／SC6, ISO 13491-1 "Banking – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods," May 1996.

ISO／TC68／WG3, ISO 7982-1 "Bank telecommunication – Funds transfer messages – Part 1: Vocabulary and universal set of data segments and data elements for electronic funds transfer messages," April 1998.

ITU Telecommunication Standardization Sector (ITU-T) Recommendation X.509 | ISO/IEC 9594-8
"Open Systems Interconnection - the Directory: Authentication Framework," June 1997. (ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc)

K. Kusuda and T. Matsumoto, "A Strength Evaluation of the Data Encryption Standard," Institute for Monetary and Economic Studies, Bank of Japan, DPS No. 97-E-5, 1997.

A. Menezes, P. van Oorshot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, New York, 1996.

National Institute of Standards and Technology, "Data Encryption Standard (DES) ," Federal Information Processing Standards Publication (FIPS PUB) 46-2, December 13, 1993.

National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, January 11,1994. (http://csrc.nist.gov/fips/fips1401.html)

National Institute of Standards and Technology, "AES — The First Advanced Encryption Standard Candidate Conference," The Proceedings of The First Advanced Encryption Standard Candidate Conference, August 20, 1998.

OECD, “Cryptography Policy: The Guidelines and the Issues — The OECD Cryptography Policy Guidelines and the Report on Background and issues of Cryptography Policy," March, 1997. (http://www.oecd.org//dsti/sti/it/secur/prod/)

William Burr, Donna Dodson, Noel Nazario, W. Timothy Polk, "MISPC: Minimum Interoperability Specification for PKI Components, Version 1," June 5, 1997

WTO, "Agreement on Technical Barriers to Trade," Agreement Establishing the World Trade Organization, ANNEX 1A: Multilateral Agreements on Trade in Goods, 1995. (http://www.wto.org/wto/legal/finalact.htm)