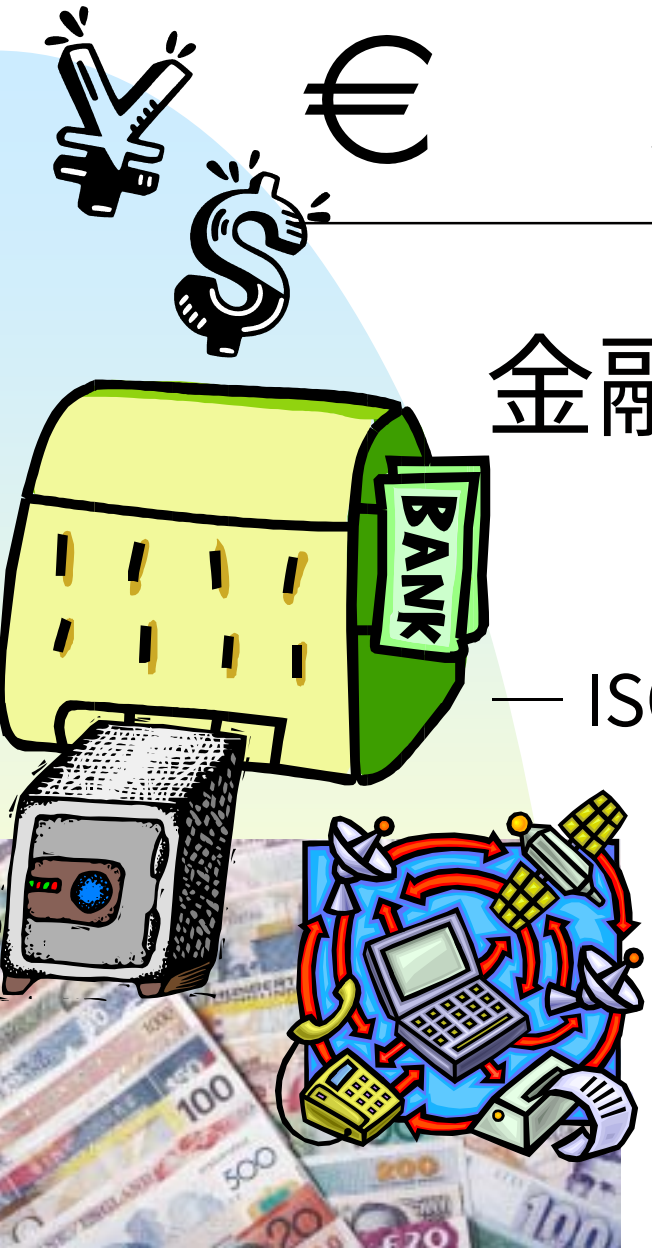


決済システムフォーラム

金融分野における情報技術の国際標準化動向

— ISO／TC68における最近の議論を中心に

日本銀行 金融研究所
岩下 直行
iwashita@imes.boj.or.jp

ISO：国際標準化機構

- 1947年設立の非政府間機構、本部ジュネーブ、148か国が加入
- 分野毎に専門委員会（TC：Technical Committee）を設置
- TC1（ねじ）からTC225（市場調査）まで188の専門委員会が活動

TC68：金融専門委員会

- 金融サービスを対象とする専門委員会
- 金融業務に利用される情報技術、情報セキュリティ技術に関する国際標準化を担当

ISO／TC68に対応する わが国の国際標準化活動

ISO/TC68国内委員会
―経済産業省の委嘱を受けて日本銀行が国内事務局を務める。

国際機関	ISO	TC68	SC2 (IT Security for Banking) SC4 (Securities and related instruments) SC6 (Retail Financial Services)
日本	会員団体 JISC	ISO/TC68 国内委員会 (事務局：日本銀行)	TC68/SC2 **国内検討委員会** (**事務局：日本銀行**) ISO **証券関係対策連絡会** (**事務局：日本証券業協会**) TC68/SC6 **国内検討委員会** (**事務局：日本銀行**)
(参考) 米国	member body ANSI	ANSI X9 committee (事務局：全米銀行協会)	ANSI X9F (Data & Information Security) ANSI X9D (Securities) ANSI X9A (Retail Electronic Financial Transactions)

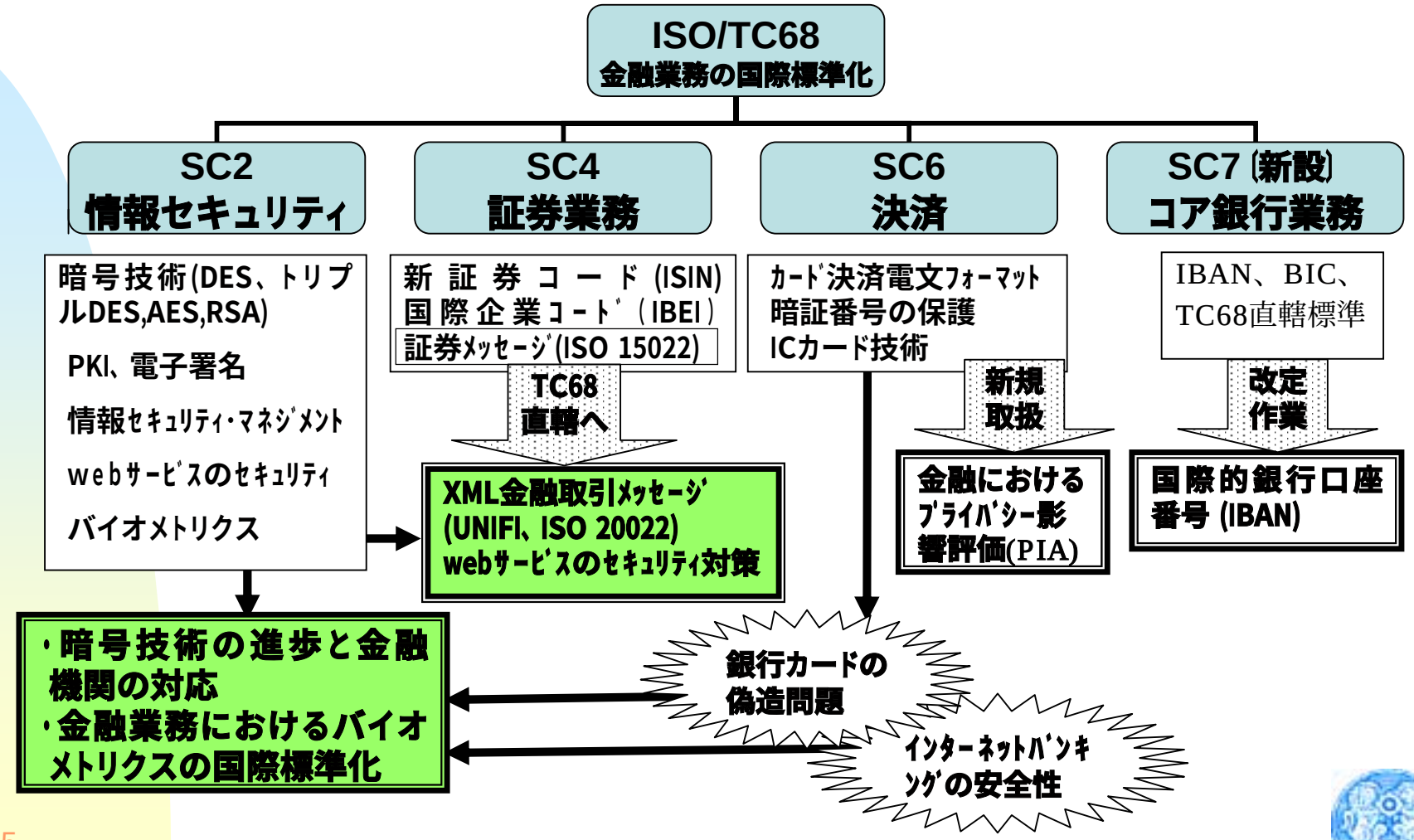
ISO/TC68の2004年国際会議

(1) TC68総会
(全体の管理、金融ﾒｯｾｰｼﾞのXML標準)
6月15日～16日、ブラッセルズにて開催
12か国、6リエゾン機関、合計 32人が参加

(2) TC68／SC2総会、SC6総会
(情報セキュリティ・決済業務)
9月9日～14日、東京にて開催
7か国、3リエゾン機関、合計 26人が参加

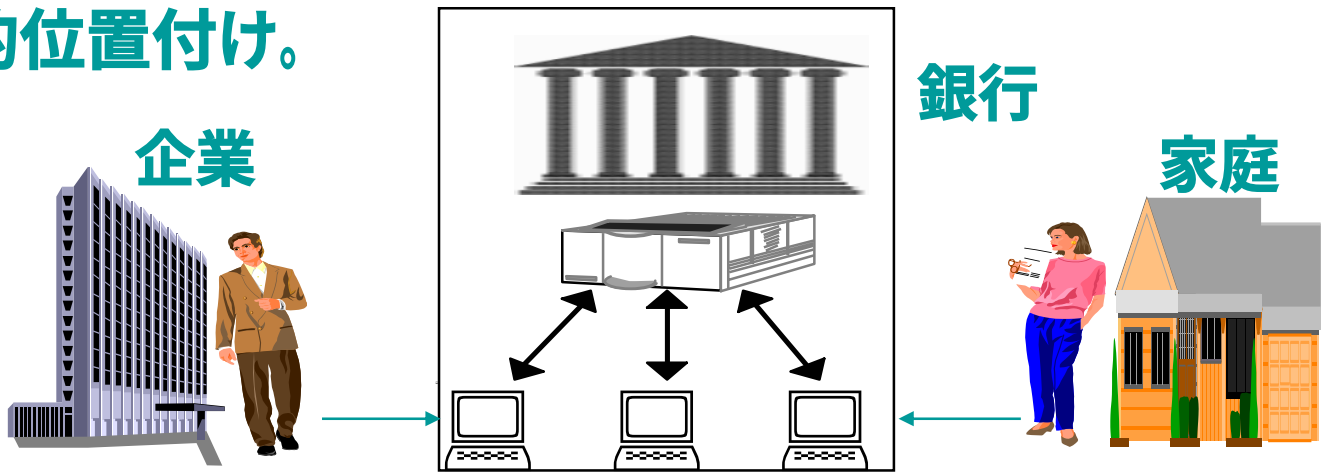
(3) TC68／SC4総会
(証券業務)
9月20日～21日、ソウルにて開催
13か国、6リエゾン機関、合計 31人が参加

ISO/TC68の活動概要と本日の話題



従来の決済システムの構造と情報技術の特徴

- 従来のポリシー：「閉じたシステム」「閉じたｱｰｷﾃｸﾁｬｰ」
- 外部から物理的に隔離された専用のコンピュータ･システム。異なるシステム間の連動はあまり考慮されない。
- ｾｷｭﾘﾃｨ対策としては、専用回線等による物理的なアクセス制御、バックアップ手段の充実などが中心。暗号技術は補完的位置付け。



・ﾋﾟﾗﾐｯﾄﾞ型　・閉鎖型　・集中ｼｽﾃﾑ

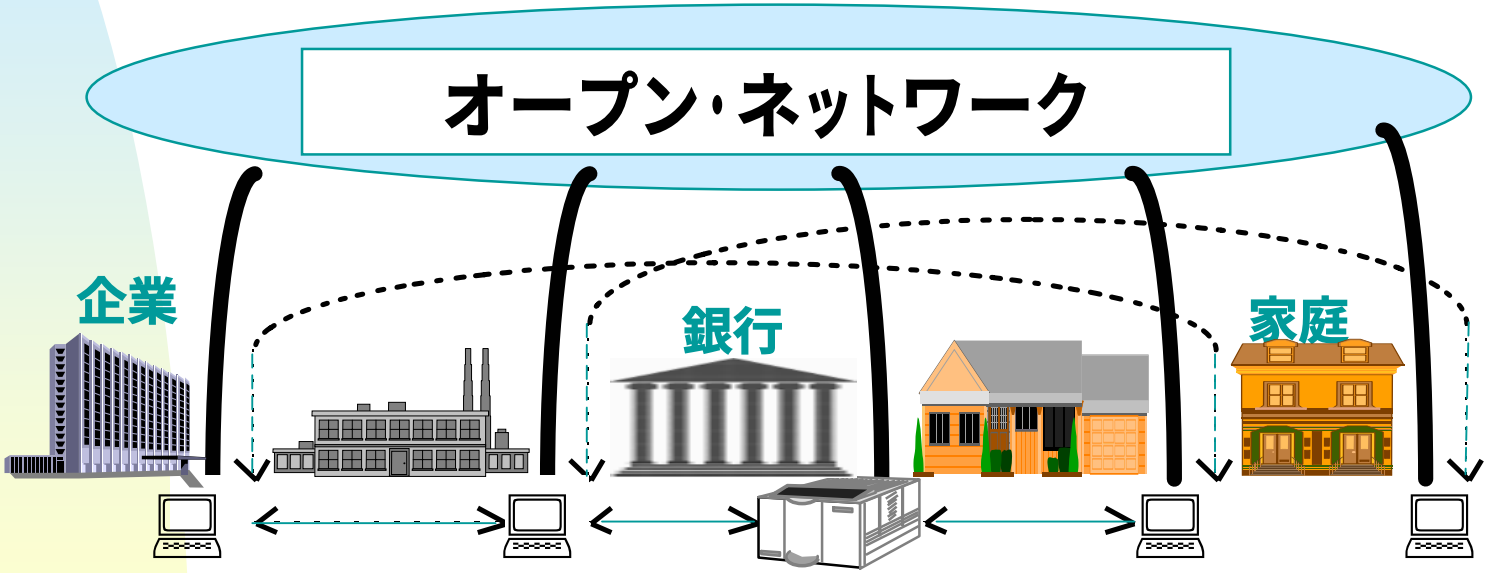
しかし、情報技術革新により、金融機関のシステム開発が直面する環境が大きく変わった。

- ダウンサイジング
- インターネットの普及
- 新しいシステム開発手法の進歩
- システム間連動ニーズの高まり
- オープンなネットワーク環境における新たな脅威の発生

情報技術の発達に伴い、従来の前提が崩れつつある。

例：STP化、EDI、インターネット・バンキングの普及。

オープン・ネットワークを介して、決済システムを含む様々なシステムが相互に連動することを前提に、グランドデザインを考え直す必要が生じている。



・水平型　・開放型（ｵｰﾌﾟﾝ・ｼｽﾃﾑ）　・分散ｼｽﾃﾑ

決済システムに生じつつある変化

【金融機関間取引における業務要件の変化】

ネットワーク化の進展と取引のグローバル化を受けて、複数の決済システムがリンクすることによる新しいニーズが生じた。

例：STP化―Straight-Through Processing

【対顧客取引における業務要件の変化】

インターネットの発達に伴い、顧客が直接、決済システムに接続することを希望するようになった。

例：インターネット・バンキング、金融EDI、国際CMS

【システム開発の基盤技術の変化】

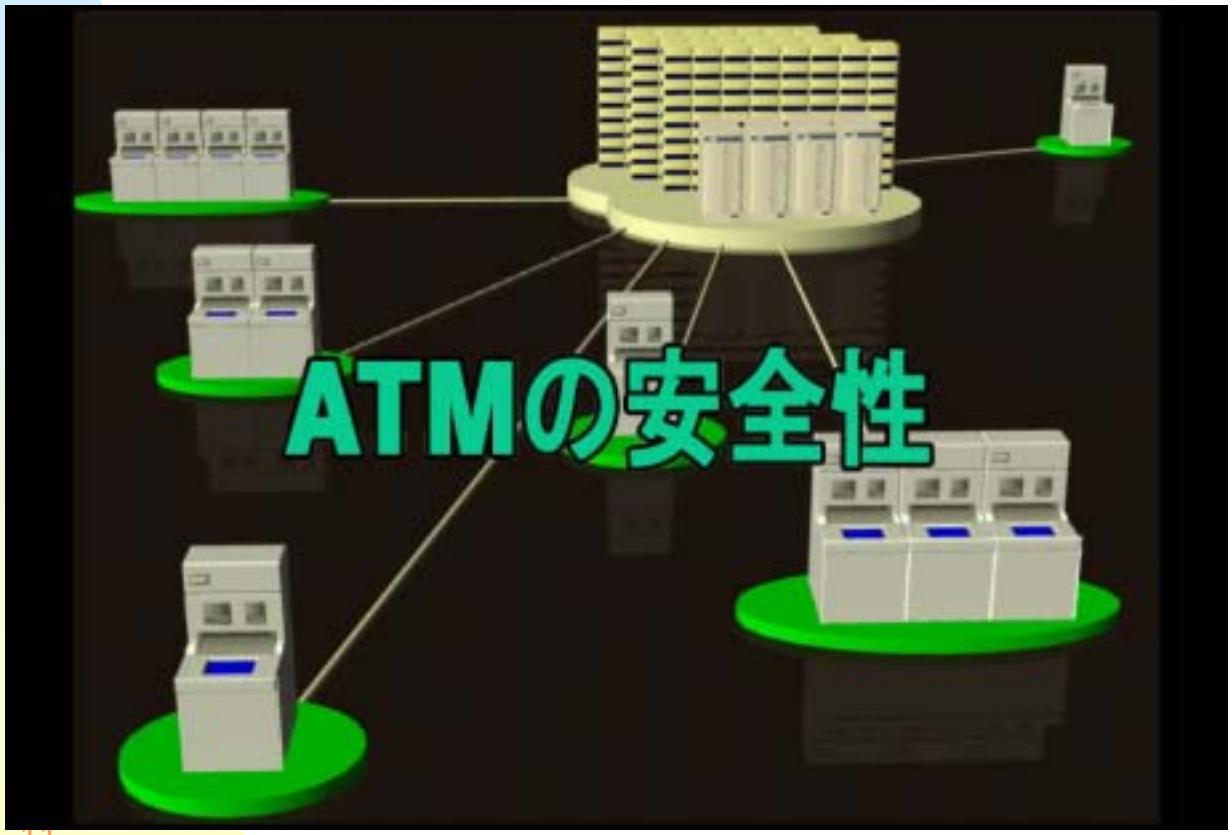
コスト効率に優れた新しいシステム開発技術の普及により、新しい開発手法に適応していく必要が生じた。

例：金融メッセージのXML化、web serviceの利用

第一の話題：情報セキュリティ

「ATMは専用線を使っているから安心」か?

中学校の技術家庭科教材
情報とわたしたちの生活　「ＡＴＭのしくみ」　より
http://kyoiku-gakka.u-sacred-heart.ac.jp/jyouhou-kiki/4203/



「ＡＴＭと銀行のコンピュータをつなぐネットワークに関しては、専用回線を使いますのでハッキングなどの心配はありません。」

某銀行のATMセキュリティに関するFAQ

「ホストコンピューターと繋がる回線は
機密性の高い回線を使用しており、
セキュリティもプライバシーも安全です。」

幾つかの疑問

- その回線が「機密性が高い」ことをどのようにして確認したのか？
- 既に、物理的な意味での「専用線」は少数派になっているが、それでも安全と言えるのか？
- そもそも、セキュリティ・プライバシーは、回線だけで解決できる問題だろうか？

わが国の決済システムにおいても、高度な情報セキュリティ技術が利用されるようになった

- インターネットを利用した銀行取引：
  ⇒SSLを利用してパスワードを保護
- キャッシュカード／デビットカード：
  磁気ストライプカード⇒ICカードに移行
- 暗証番号による保護⇒ﾊﾞｲｵﾒﾄﾘｸｽに移行
- 銀行の勘定系システムの安全性の拠り所：
  専用線利用のクローズドシステム
  ⇒暗号や電子認証の利用へ

⇒暗号、電子認証，ICカード等の情報セキュリティ技術がわが国でも金融機関の実務に利用されるようになってきた。

⇒　問題は、情報セキュリティ技術を如何に「上手に」利用するかにある。

欧州における情報セキュリティリスク顕在化の事例

- **採用した情報セキュリティ技術が業務の安全性を左右**

⇒安全性が十分に確保できない場合

- **直接的リスク：業務の停滞や金銭的被害**
- **レピュテーションリスク：信用を失う**
- **リーガルリスク：訴訟**
- **経営的ダメージも**

フランス銀行カード協会 (Groupment des Cartes Bancaires) のICカード偽造事件

- **古い規格に準拠して製造されたICカードのRSA公開鍵暗号の鍵長が短かったことが原因。**
- **1999年、ある技術者がICカードとカードリーダを解析し、偽造カードを作成し、大きな事件となる。**
- **768bit鍵長の新しいICカードに移行が必要となった。**

ISO9796にもとづくドイツの電子署名用ICカードを巡る事件

- ISO9796に基づくメッセージ回復型のRSA電子署名を使用。
- 1999年 ISO9796に対する新しい署名偽造攻撃法の存在が明らかに。
  - 1999年4月、Coron、Naccache、Stern
  - 1999年8月、Coppersmith、Halevi、Jutla
- 潜在的な脅威によって、当該ICカードにより生成された電子署名の信認が揺らぐ

事件の教訓

- 単に「暗号を利用している」
  「ICカードを利用している」
  「ﾊﾞｲｵﾒﾄﾘｸｽを利用している」
  というだけでは不十分。
- 情報セキュリティ技術が、最新の評価基準によりきちんと評価された、信頼できるものであることが必要。

TC68策定の情報セキュリティ関連の国際標準

ISO番号	国際標準の名称	概要
ISO 8732	暗号鍵の管理	大口金融取引用の暗号鍵の管理方式。
ISO 9564	暗証番号(PIN)管理とｾｷｭﾘﾃｨ	暗証番号の送信に暗号を利用することを規定。ｱﾙｺﾞﾘｽﾞﾑとして3DESとRSAを指定。
ISO 10126	ﾒｯｾｰｼﾞ暗号化手順	大口金融取引の守秘目的の暗号化手法と利用するｱﾙｺﾞﾘｽﾞﾑを規定。
ISO 11131	金融機関のSign-on認証	金融ｼｽﾃﾑにｱｸｾｽする際の相手認証手法。
ISO 13491	安全な暗号装置(SCD)	ﾘﾃｰﾙ金融取引用暗号装置の要件を規定。
TR 13569	情報セキュリティガイドライン	金融機関が採用するｾｷｭﾘﾃｨ対策を詳述。
ISO 15782	公開鍵証明書の管理方法	金融機関がCAとなる際の留意点を規定。
ISO 16609	MACの必要条件	共通鍵暗号を利用した認証用ｺｰﾄﾞの要件。
TR 17944	金融ｼｽﾃﾑにおけるｾｷｭﾘﾃｨの枠組み	関連する国際/国内標準を集めたリスト集。
CD 19092	金融業務におけるバイオメトリクス	金融業務にﾊﾞｲｵﾒﾄﾘｸｽを適用する際のｼｽﾃﾑ設計･管理上の留意点、ｶﾞｲﾀﾞﾝｽ。
DTR 19038	トリプルDESの利用モード	米国金融業界による3DES標準の国際版。
ISO 21188	金融業務のためのPKIーCP/CPS	金融向けに書かれたCP/CPS枠組み標準。
NP 22011	金融取引電文に安全な電子署名を付与する際の要件	インターネットバンキング等において金融取引電文に安全に署名するための指針。

暗証番号(PIN)暗号化に関する標準

ISO 9564

Personal Identification Number management and security

- 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）等と共に利用される PIN について、その設定、保管、入力、送信等に関する一般的なルールを取り決め。
- 暗号化されないPINは、物理的に安全な環境に保管しなければならない。そうでない場合、規定された暗号アルゴリズムを用いて暗号化されなければならない。
- 従来は、DESの利用を想定。
  ⇒ DESの安全性低下を受け、トリプルDESに移行。
  ⇒ この結果、欧米の金融機関の利用するCD/ATMの改造が必要に。

DES暗号の強度の低下とISO/TC68の対応

1994年6月

- ISO/TC68/SC2総会において、米国代表がDESの強度低下について問題提起。

1995年4月

- ISO/TC68/SC2総会において、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を発表。

1996年10月

- ISO/TC68総会において、日本がDESの強度評価に関する技術レポートを提出。専用解読装置を用いた全数探索法の脅威を論証（IMES Discussion Paper Series 97-E-5）。

1997年1月

- 米国政府がAES（Advanced Encryption Standard）の標準化を開始。

1998年10月

- 米国金融業界によるTriple DESの国内標準化作業完了(ANSI X9.52)。

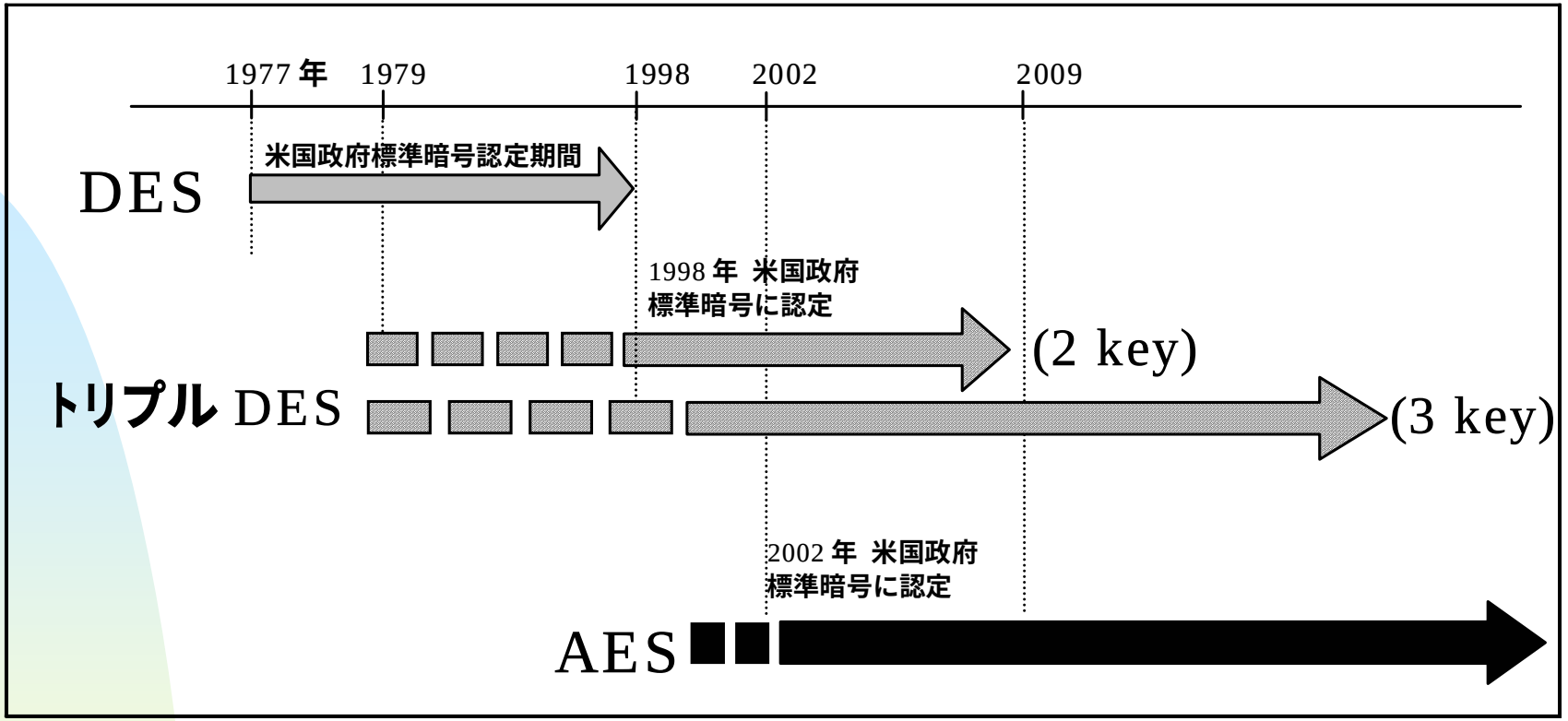
2000年10月

- 米国NISTが、RijndaelをAESに選定(FIPS 197の制定は2002年5月)。

2004年5月

- 米国NISTがFIPS 46-3（DES/ Triple DES）を廃止。2-key Triple DESの有効期限を2009年までとする文書（NIST Special Publication 800-67）を公表。

トリプル DESの有効期限を巡る議論



ISO/TC68/SC2総会における議論

・NISTによる2keyトリプルDES有効期限設定の妥当性。

・2keyトリプルDESの実装件数は多いため、早急な対応が必要。

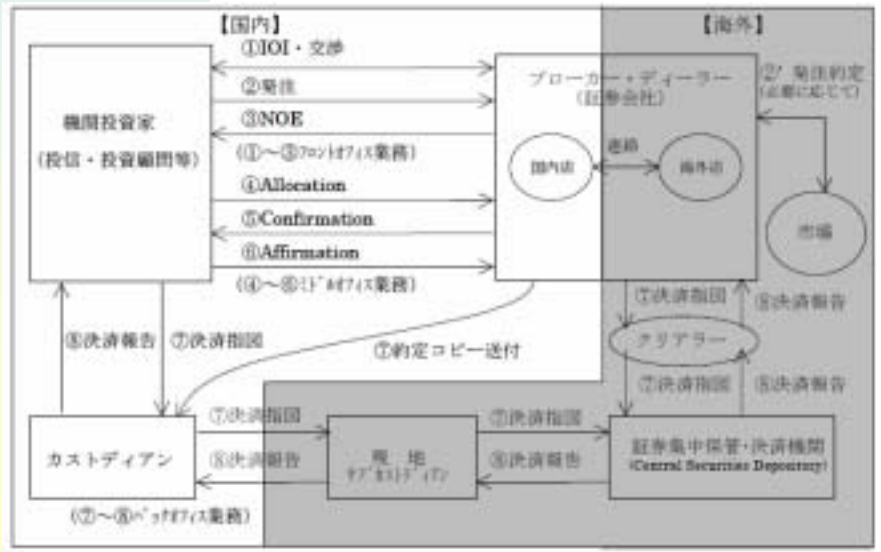
第二の話題：メッセージ標準

証券取引のSTP化とメッセージ標準

証券取引のSTP (Straight-Through Processing)化: 証券取引において約定から決済に至るプロセスを、標準化されたメッセージ・フォーマットによりシステム間を自動的に連動させ、人手を介さずに一連の作業をシームレスに行うこと。

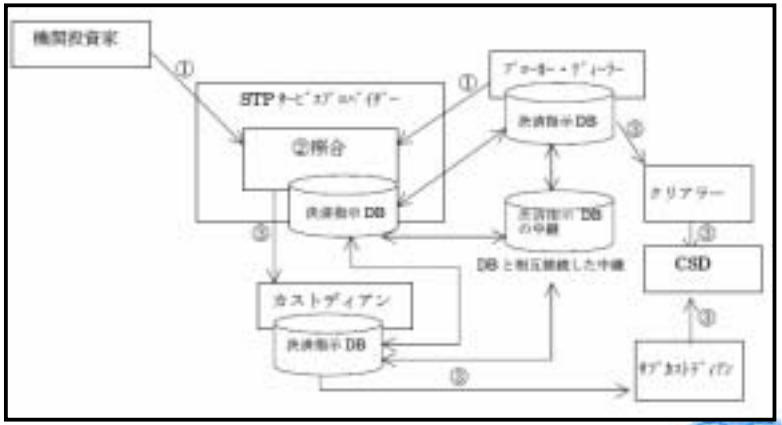
STP化前 (現行)

証券取引関係者間の情報のやり取りが、電話やTELEXを含む様々なネットワーク経由で行われ、事務フローが分断されている。データの再入力が必要なため、事務ミスによるフェイルが頻発し、決済期間の短縮にも限界がある。



STP化後

標準化された通信メッセージを用いてフロントオフィス・バックオフィス双方でシームレスな一貫処理が行われる。取引の早い段階から関係者間で情報が共有され、データの再入力が発生しないため事務ミスも少なく、決済期間の大幅な短縮が可能。



証券取引用メッセージの国際標準化を巡る様々な動き

ﾌﾟﾛｼﾞｪｸﾄ名	概　要
ISO7775	1984年に制定された最初の証券メッセージの国際標準。SWIFTのMT500番台として、バックオフィスでの決済業務に広く利用されている。1989年、G30から国際証券取引での採用を勧告された。
SSAB	1993年にISO7775の改訂のために組成された有識者会議。作業半ばで活動を停止。
ISITC	1991年に組成された英米の投資家、銀行の団体。 自主的に、各証券市場にマッチしたISO7775の拡張利用方式を提案し、グループ内で利用してきた。
FIX	1993年に米国で試行が始められたフロントオフィス用の証券メッセージ。主に、証券会社と機関投資家との間のオンライン取引で利用される。
ISO15022 (1st edition)	1999年にISO7775の後継として制定された国際標準。MTそのものを標準化するのではなく、MTの作り方を標準化することにより、従来のISO7775、ISITC等のメッセージとの互換性を保ちつつ、FIXとのマッチングが可能となった。

ISO15022のXML化を巡る新たな動き

2003年

ISO/TC68/SC4によるISO 15022 2nd editionの策定

——通信メッセージのフォーマットを、固定長からXMLに変更。

——証券取引のみならず、全ての金融取引がターゲットに。

——FixML（フロント事務）、FpML（デリバティブ取引）、MDDL（市場データ）、XBRL（財務データ）、Omgeo（ポスト・トレード）等金融XML標準の統合を企図。

2004年

ISO 15022 2nd editionに新番号を付番し、ISO 20022とする。

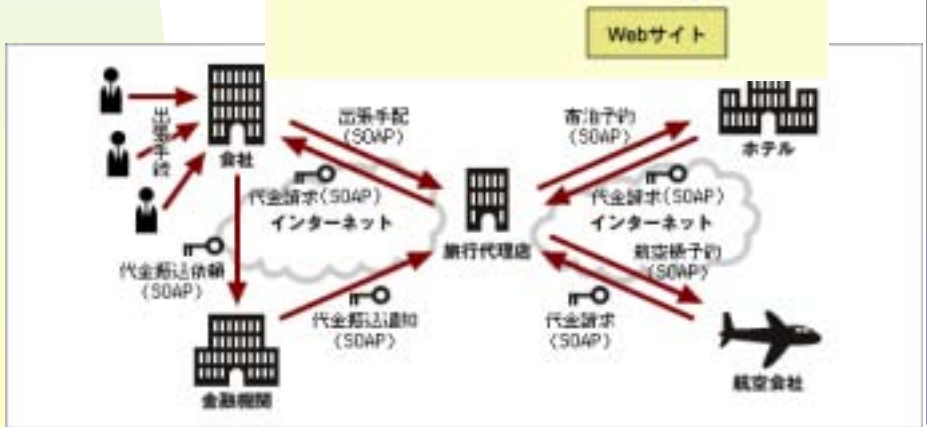
——ISO/TC68/SC4からISO/TC68直轄に。

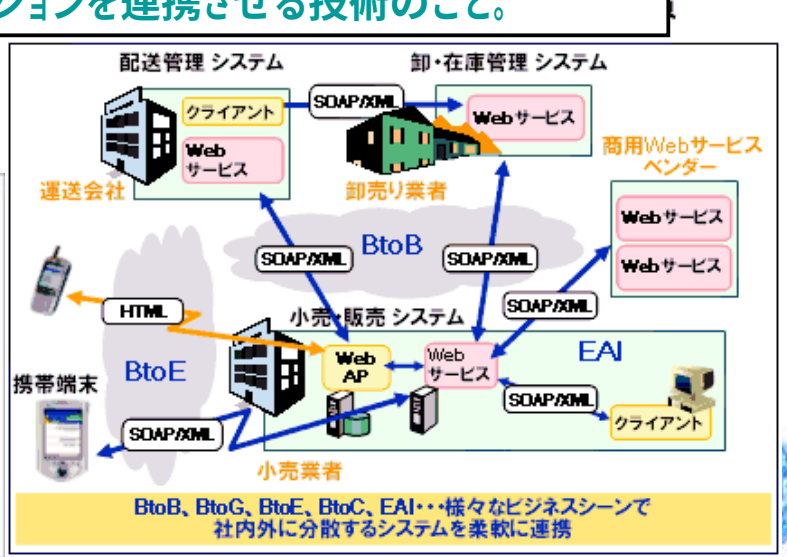
——銀行業務（ペイメント、財務情報、外為取引等）の取り込みを企図。

なぜ、欧米の金融機関は金融業務向け通信メッセージ標準のXML化を進めようとするのか?

・・・・・XML Webサービス*を利用してシームレスに連動するシステムを効率的に構築することが狙い。

*XML Webサービスとは、SOAP (Simple Object Access Protocol)/XML形式のメッセージ交換によって、ネットワーク上のアプリケーションを連携させる技術のこと。





ISO20022 のRAとRMG

ISO 20022では、XMLメッセージを一元的に管理するための実務は登録機関(RA)であるSWIFTが担当し、XMLメッセージの開発、承認、調整は、TC68参加各国が推薦した委員によって構成される登録管理グループ (RMG) が担当することとされている。

現在、各国ISO/TC68窓口に対し、ISO 20022 RMGに各国代表として参加するエキスパートを募集している。

2005年1月に、RMGの第一回会合を予定。

金融向け通信メッセージ標準を巡る今後の課題

- XML標準への対応の必要性、XML Webサービスの利用可能性等について、どのような評価を下すか。
- SWIFTや海外の金融機関が先行してXML標準を利用することになった場合の対応方針如何。
- 実際の利用が将来となるとしても、標準策定段階で、日本としての業務要件を織り込ませる必要はないか。