平成17年6月10日

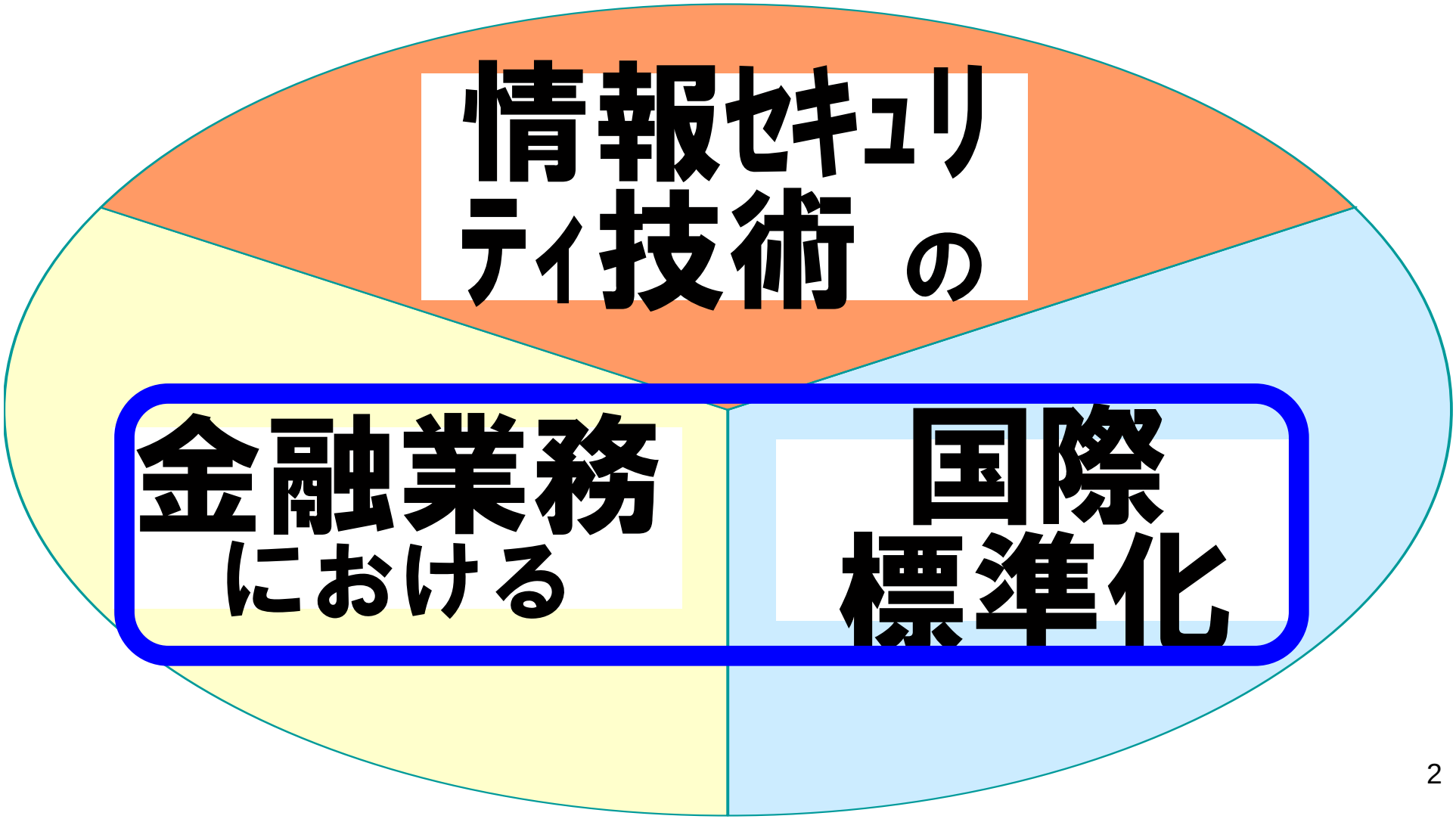
金融庁偽造キャッシュカードSG
プレゼンテーション

金融業務における情報セキュリティ技術の国際標準化

― ISO/TC68の活動を中心に

日本銀行 金融研究所
情報技術研究センター長
岩下 直行

1.金融業務における国際標準化



標準化とは何か

標準化とは、規格の制定と認証を通じ、自由に放置すれば複雑化、無秩序化する物や事柄を、人為的に単純化、秩序化すること。

業界内の複数の企業が協力して「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

①相互理解	用語や概念について、共通の理解を持つ。
②互換性の確保	異なる生産者が製造した製品間の互換性。
③多様性の調整	不必要に多様化してしまう仕様を単純化。
④消費者利益の確保	一定の性能・品質を標準により保証する。
⑤新技術の普及	新技術普及のために、技術仕様を公開。
⑥安全・環境の保護	安全規格、環境規格の制定。

様々な標準とその分類

【強制規格、任意規格】

「強制規格」：遵守することが法律で強制されているもの。

（例）：電気製品、自動車、薬品等の安全基準等

「任意規格」：遵守することが任意のもの。

（例）：ISOやJISなどの国際標準、国内標準

（それ自体が遵守を強制されるものではない）

【国際標準、国内標準、業界標準】

標準が想定している対象地域の範囲による。

国際標準、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

	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	標準を巡る競争の結果、事実上決定された標準
特徴	①策定プロセスの透明性 ②単一標準の提供 ③オープンなメンバーシップ	①策定プロセスの速度が迅速 ②標準普及と製品普及が同時 ③市場競争で標準が一本化 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製品普及と標準普及のラグ ③技術のフリーライド	①情報公開が不完全。開発企業による競争限定的行為の懸念 ②閉鎖的なメンバーシップ ③改正手続が不透明

わが国の産業界と国際標準化

かつては多くの産業で「国際標準」と「国内標準」が断絶していた。

- **国内で製造し、国内で消費するものが大半。**
- **わが国独自の言語、単位、慣習、業界ルール等々。**
- **輸出向け商品は、輸出先の規格を利用。**

しかし、グローバル化の中で、製造業を中心に、国際標準への対応の必要性が高まった。

GATT / Standard Code（1979年）⇒ WTO / TBT協定（1994年）

「工業製品等の各国の規格及び基準認証制度が不必要な貿易障害とならないよう、国際規格を基礎とした国内規格策定の原則を規定」

⇒ 過去に制定された国内標準（JIS）を改定し、国際標準（ISO等）に整合化させる作業が進捗

わが国の金融業界の国内における標準化

わが国の金融業界の標準化の実績

［紙の世界］手形、小切手、帳票類の様式の統一
［電子化後］金融機関間のデータ通信フォーマット、

金融機関コード、
磁気ストライプ・カード仕様　等

従来の国内金融分野における標準化の特徴

①業界内部での申し合わせの形態を取る。（JISではない）
②国際的な動向をあまり考慮しない。（ISOとも整合しない）

⇒（ICカード仕様など一部業務を除き）
従来は、「内向きの標準化」であった。

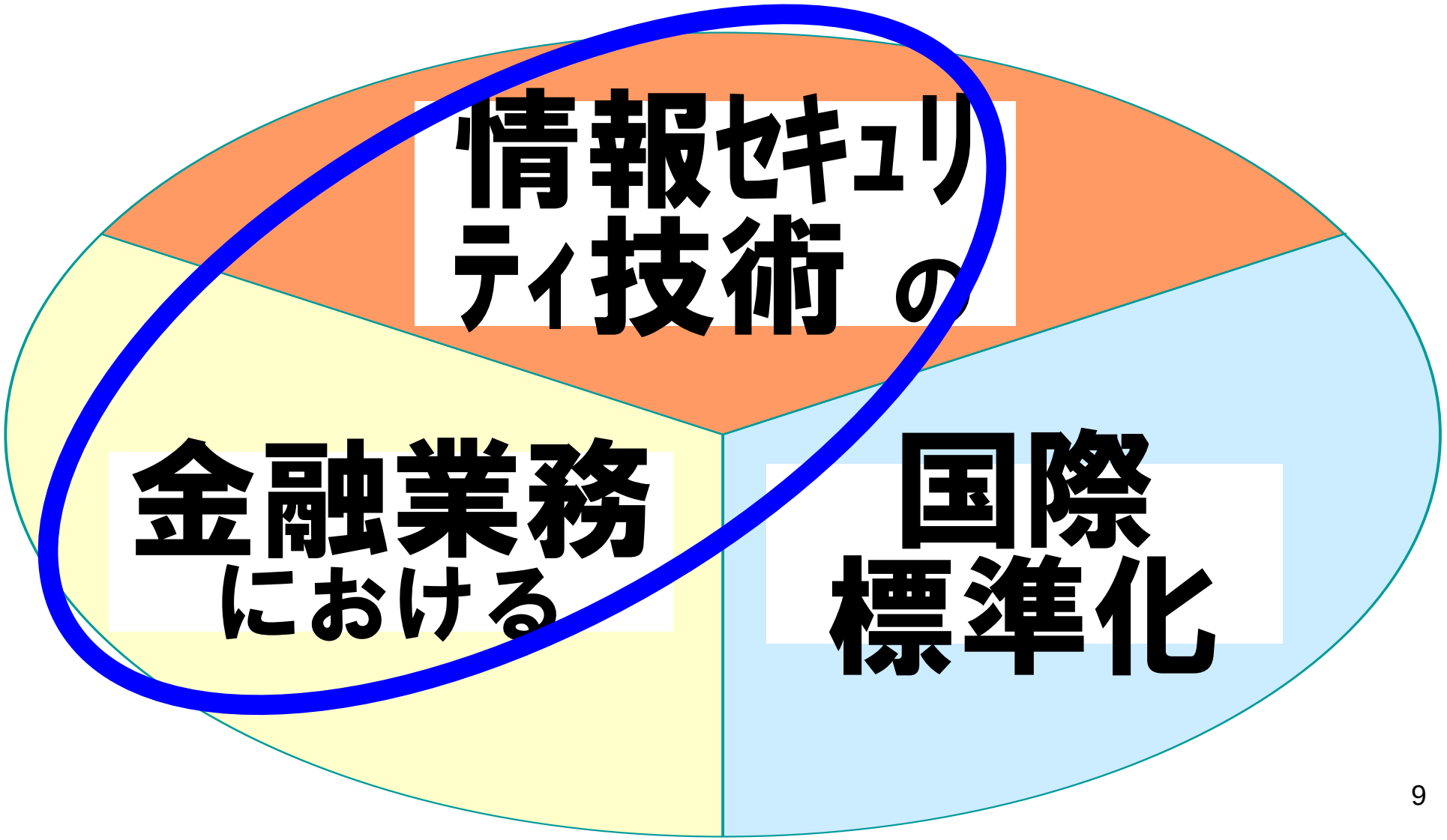
わが国の金融業界と国際標準化

- 国内金融については、「海外と整合させるために国際標準に準拠する」という必要性が希薄。
- 国内と海外では規制、言語、慣習等が異なる。
- 国際取引については、国内取引とは異なるシステムを用いるのが一般的であった。

⇒ わが国の金融業界は、国内金融において、国際標準を意識することはなかった。

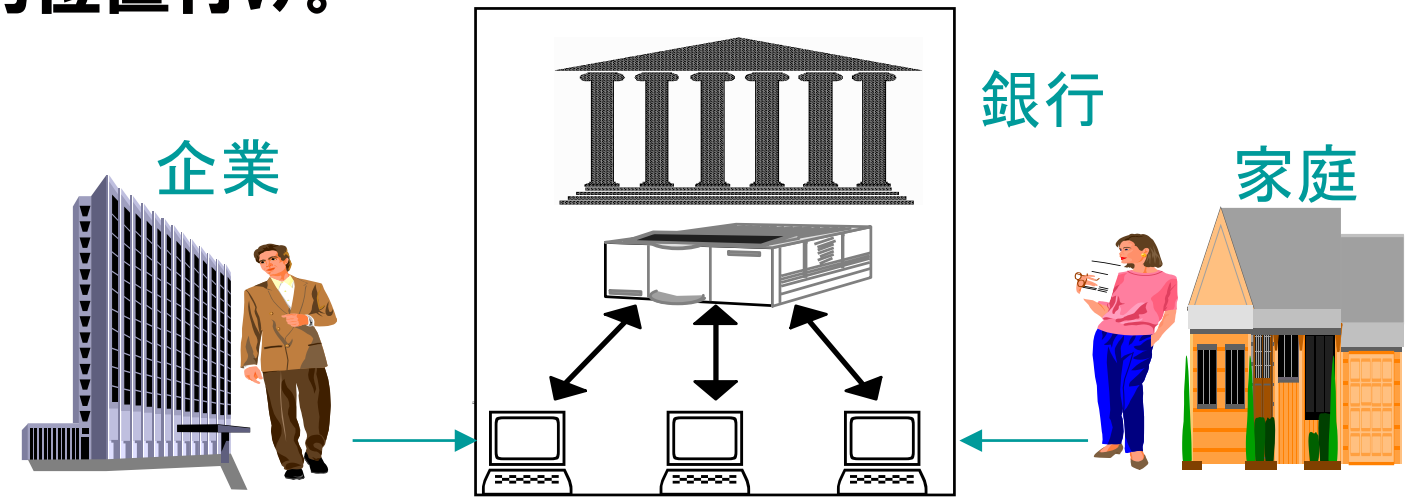
⇒ わが国の国内金融では、欧米の金融機関によって国際標準とされた情報セキュリティ技術が殆ど利用されていなかった。

2.金融業務と情報セキュリティ技術



わが国の従来の決済システムの構造

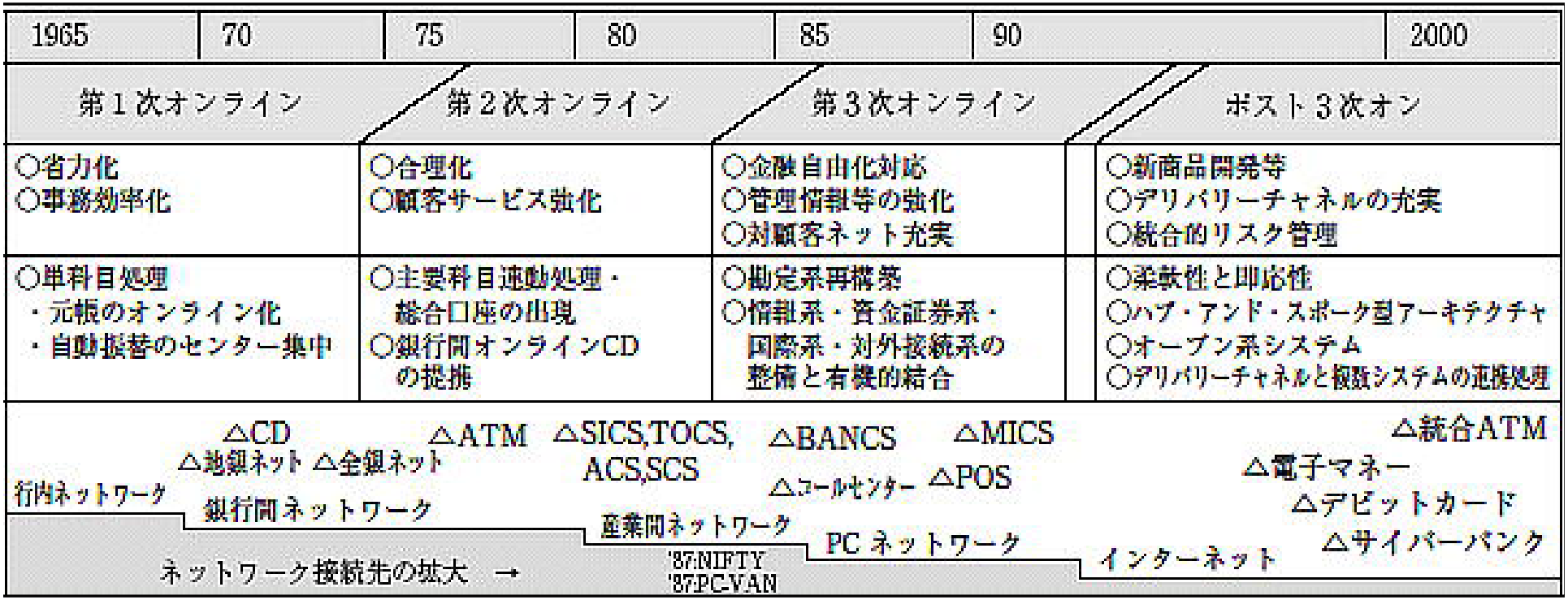
- 従来のポリシー：「閉じたシステム」「閉じたアーキテクチャー」
- 外部から物理的に隔離された専用のコンピュータ・システム。異なるシステム間の連動はあまり考慮されない。
- セキュリティ対策としては、専用回線等による物理的なアクセス制御、バックアップ手段の充実などが中心。暗号技術は補完的位置付け。



・ﾋﾟﾗﾐｯﾄﾞ型　・閉鎖型　・集中ｼｽﾃﾑ

10

金融業界は、コンピュータによるネットワーク・システムを最も早い時期に整備した業種であった



1970年頃に初めて導入されたキャッシュカードとCD/ATMの技術

基本設計を30年間にわたって維持

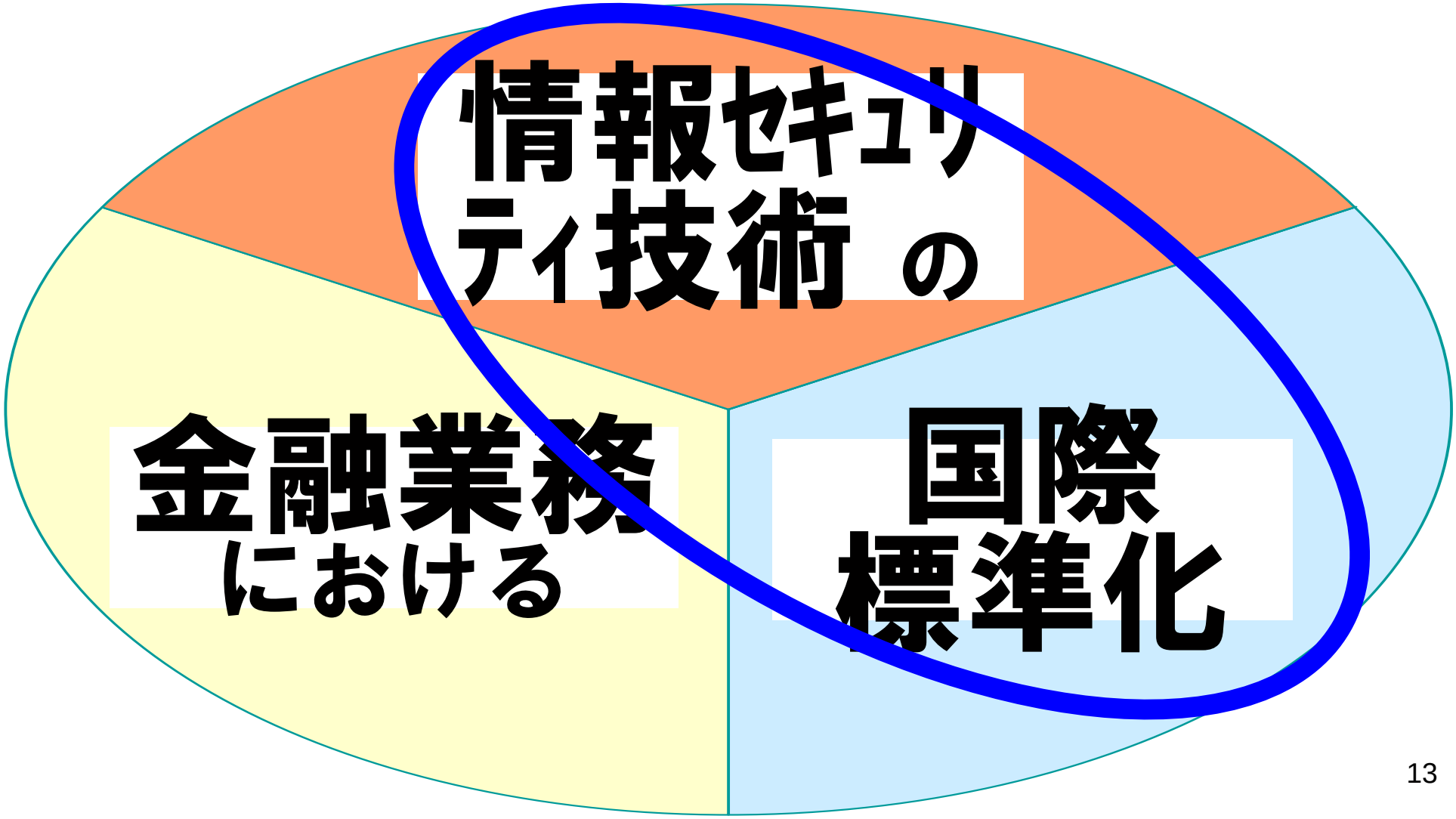
銀行のオンライン・システムの頑健性、安全性に疑いを持たれることはなかった。

しかし、金融ハイテク犯罪の増加により、銀行のセキュリティに対する顧客の信頼は揺らぎつつある。

- 銀行の提供するCD/ATMネットワークは、顧客利便を追及して提携、接続を繰り返した結果、セキュリティ管理上、複雑化し過ぎているのではないか？
- 通信情報（特に暗証番号）の通信経路における暗号化など、情報漏洩を防止する適切な対策が講じられていないのではないか？

⇒ 銀行の情報システムのセキュリティについて、顧客の信頼を維持するために、欧米で採用されている情報セキュリティ技術の国際標準を活用していくことが考えられる。

3.情報セキュリティ技術の国際標準化



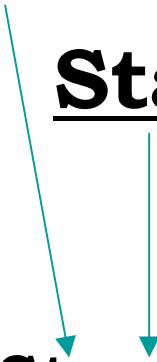
信頼できるセキュリティ技術を普及させるためには、

- 「様々な提案がなされ、互いに競争し、最終的に利用者に支持されたものが勝ち残る」しかない。しかし、
- 「結局どの技術も利用者に選択されず、従来の取引と変化がなかった」とか、
- 「安全性の低い技術が普及してしまい、将来に禍根を残す」ことは避けたい。
- 信頼できる優れた技術を普及させるために、どうすればよいか？

米国政府標準暗号:DESとAES

DES（Data Encryption Standard）

AES（Advanced　Encryption　Standard）



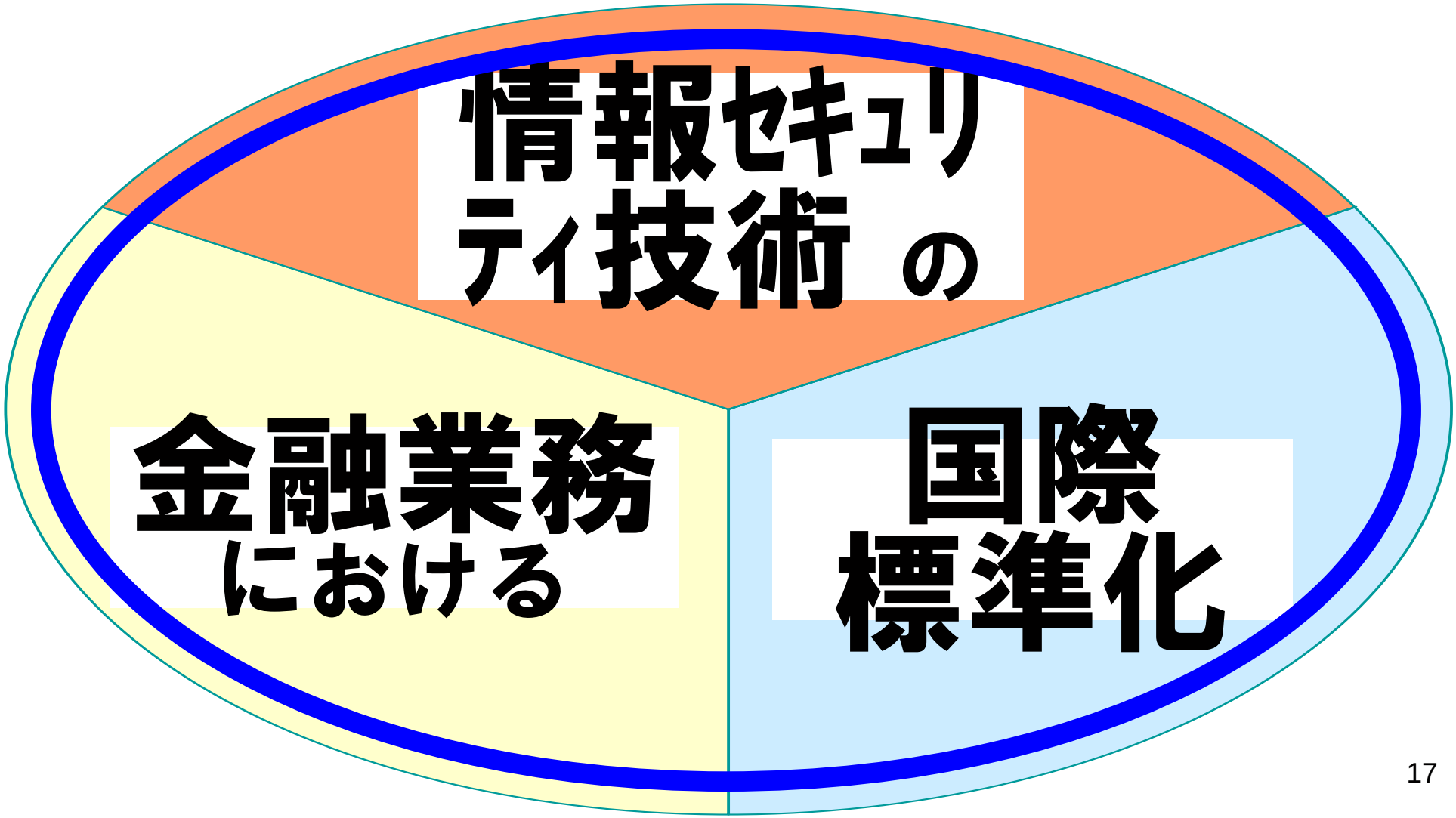
米国政府標準暗号
（FIPS:Federal Information Processing Standards）

情報セキュリティ技術の普及局面においては公的機関による標準化が安全性に対する「お墨付き」として機能する。

情報セキュリティ技術の普及と標準化

- 暗号などの情報セキュリティ技術は通信ネットワーク環境で利用されるため、標準化された技術を多数の利用者が利用することによって利便性が高まり、システム構築・運用コストを低減化できる。
  → 標準化によって実際に利用するプロトコルやアルゴリズムを絞り込みたいというニーズ。
- 信頼できる中立的な機関が安全性を十分に吟味した上で標準化を行うことによって、利用者がその技術を安心して使うことができる。
  → デジュール標準という「お墨付き」が普及を促す。

4. ISO/TC68の活動



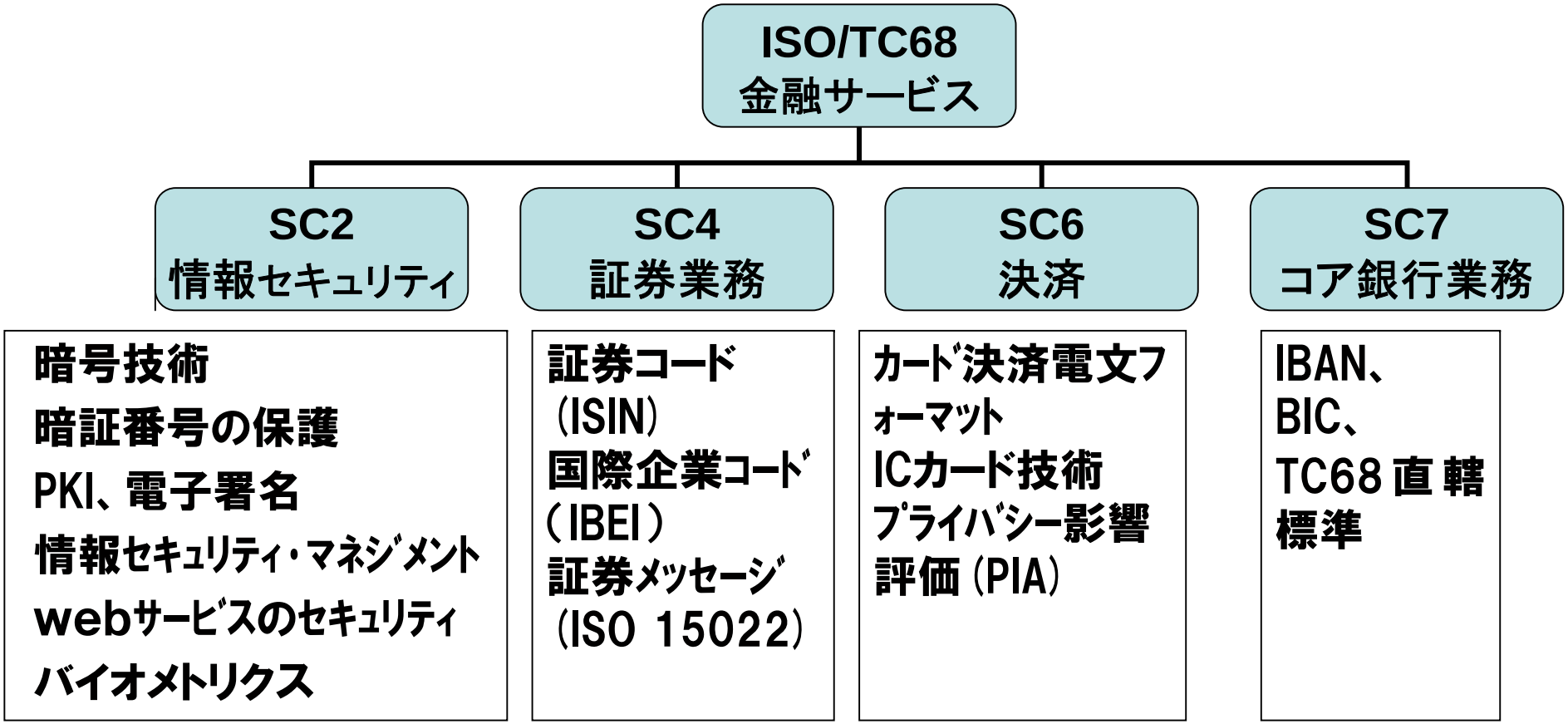
ISO：国際標準化機構

- 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の概要


ISO/TC68
金融サービス
SC2
情報セキュリティ
SC4
証券業務
SC6
決済
SC7
コア銀行業務
暗号技術
暗証番号の保護
PKI、電子署名
情報セキュリティ・マネジメント
webサービスのセキュリティ
バイオメトリクス
証券コード
(ISIN)
国際企業コード
(IBEI)
証券メッセージ
(ISO 15022)
カード決済電文フォーマット
ICカード技術
プライバシー影響
評価(PIA)
IBAN、
BIC、
TC68直轄
標準

ISO/TC68/SC2-6東京会合の模様

2004年9月9日～14日、日本銀行本店

8か国から、24人が参加。

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（委員長：南部鶴彦学習院大学教授）
― 経済産業省から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 (Security) SC4 (Securities and related instruments) SC6 (Payment) SC7 (Core Banking)
日本	**会員団体** JISC	**ISO/TC68 国内委員会** **（事務局：日本銀行）**	**TC68/SC2-6-7 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）**
（参考）米国	member body ANSI	ANSI X9 committee	ANSI X9F (Data & Information Security) ANSI X9D (Securities) ANSI X9A (Retail Electronic Financial Transactions)

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 8583	金融取引カードのメッセージ	カード取引に利用される電文フォーマットを規定。
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。アルゴリズムとして3DESとRSAを指定。
NP 10126	メッセージ暗号化手順	大口金融取引の守秘目的の暗号化手法と利用するアルゴリズムを規定。
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 11568	金融取引における鍵管理	PIN暗号化のための暗号鍵の管理方法を規定。
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ドの要件。
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。
DIS 19092	金融業務におけるバイオメトリクス	金融業務にバ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、ガイダンス。
TR 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－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）の取扱に関する国際標準: ISO 9564

Personal Identification Number (PIN) management and security

Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems

- 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（例えば、PINは4桁以上）。
- PINに関る機器・ソフトは、不正に改変できないことが必要（4a）。
- PINを平文で保管するには、物理的に安全な環境が必要（4e）。
- PINを暗号化する場合、暗号化方式を明らかにしないことによってではなく、暗号鍵の秘匿によってその機密性を守ること（4d）。
- PINを暗号化する場合、同じPIN、同じ暗号鍵でも、異なる暗号文となること（乱数等により適切にパディングすること、4c）。
- PINを暗号化する場合、ISO 9564-2に規定された暗号アルゴリズムで暗号化すること（6.2）。

ISO 9564-1におけるPINブロックの説明

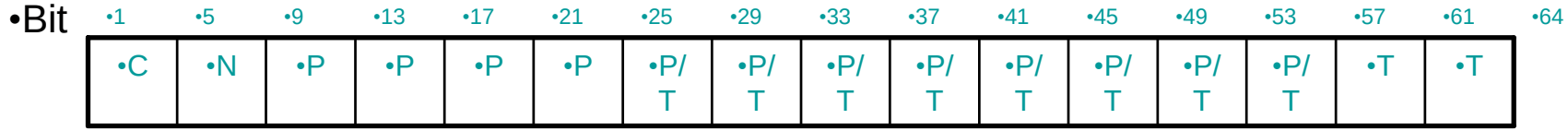
電文フォーマットに加え、適切なパディング方式まで規定

8.3.2. Format 1 PIN block

This PIN block is constructed by concatenation of two fields: the plain text PIN field and the transaction field.

The format 1 PIN block shall be reversibly enciphered when transmitted.

The format 1 PIN block shall be formatted as follows:



•

•where:

•C = Control field - Shall be binary 0001.

•N = PIN length - 4−bit binary number with permissible values 0100 (4) to 1100 (12).

•P = PIN digit - 4−bit field with permissible values 0000 (zero) to 1001 (9).

•P/T = PIN/Transaction digit - Determined by PIN length.

•T = Transaction digit - 4−bit binary number with permissible values of 0000 (zero) to 1111 (15).

The transaction field is a binary number formed by [56-(N* 4)] bits. This binary number shall be unique (ex-cept by chance) for every occurrence of the PIN block and can, for example, be derived from a transaction se-quence number, time stamp, random number or similar.

•NOTE The transaction field should not be transmitted and is not required in order to translate the PIN block to another format since the PIN length is known.

Personal Identification Number (PIN) management and security
Part 2: Approved algorithm for PIN encipherment

- かつては、米国国内標準(ANSI X3.92:1981)を引用して
  DES暗号のみを規定していた。
  ⇒ 欧米のCD/ATMでは、暗証番号の暗号化にDES暗号を
  利用していた。
  ⇒ 1990年代に入って、DES暗号の強度が低下。
  ⇒ 米国の金融業界が、DES暗号に代わる暗号アルゴリズムを
  自ら標準化(ANSI X9.52 トリプルDES)。
- 現在は、推奨アルゴリズムとしてトリプルDESとRSAのみを記載。
  ⇒ 欧米のCD/ATMは、DES暗号からトリプルDES暗号に移行。

米国の金融業界では、業界団体と主要銀行が中心となって、
経営レベルで暗号アルゴリズムの問題が討議されている。

DES暗号の強度の低下とISO/TC68の対応

1994年6月
- ISO/TC68/SC2総会で、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総会で、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。

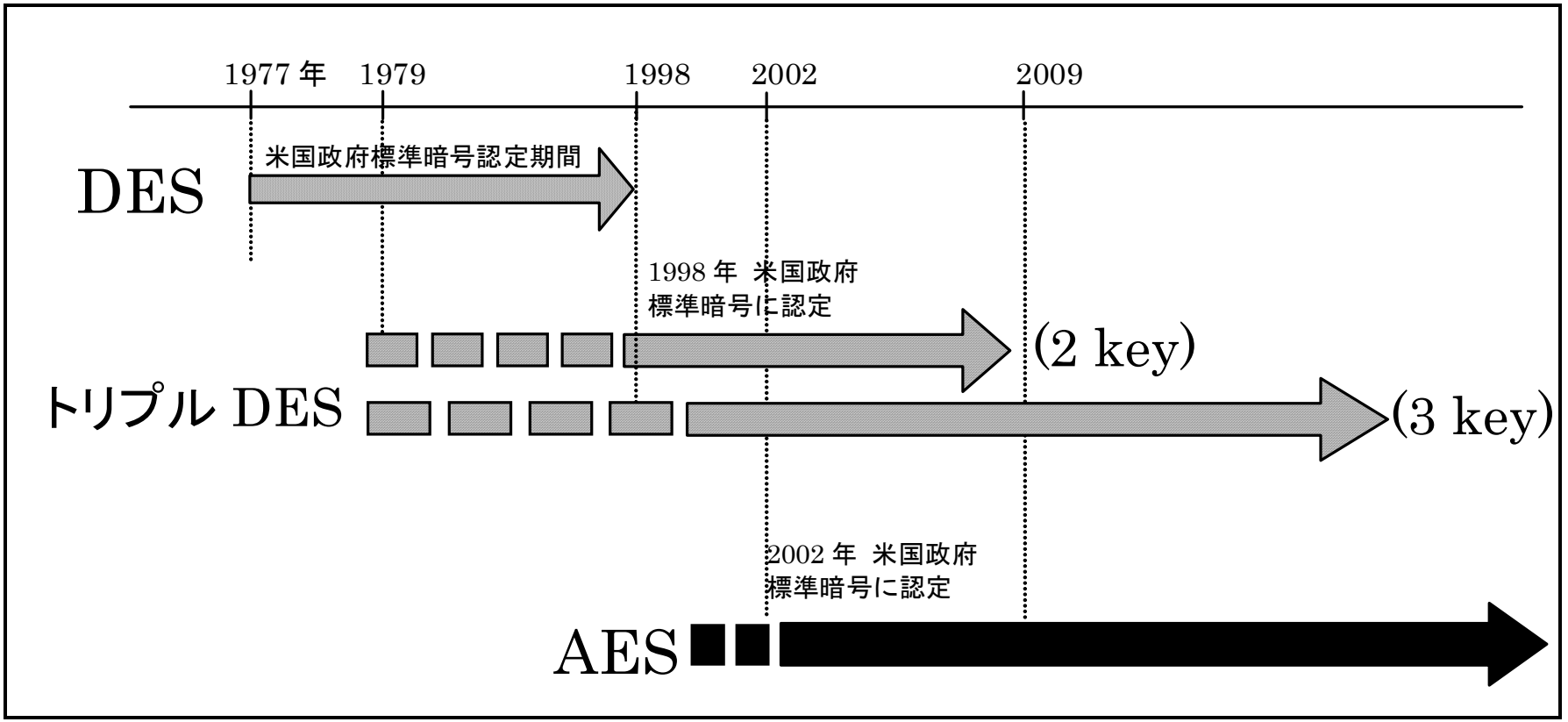
1998年10月
- 米国金融業界によるTriple DESの国内標準化作業完了(ANSI X9.52)。

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。

2005年5月
- 米国NISTがFIPS 46-3(DES/ Triple DES)を廃止。

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。

偽造キャッシュカード問題と国際標準

ISO/TC68(国際)が果たしていくべき役割

預金者の安全確保、金融システムの安定のために、金融機関が採用すべき適切なセキュリティ対策に関する各国金融業界の叡智を集め、国際標準の審議・検討を行い、その成果を対外的に示していくこと。

ISO/TC68国内委員会の役割

金融業界の情報セキュリティ対策に関する国際標準の審議に参画するとともに、その内容を国内に周知し、国内における望ましい対応の実現をサポートしていくこと。