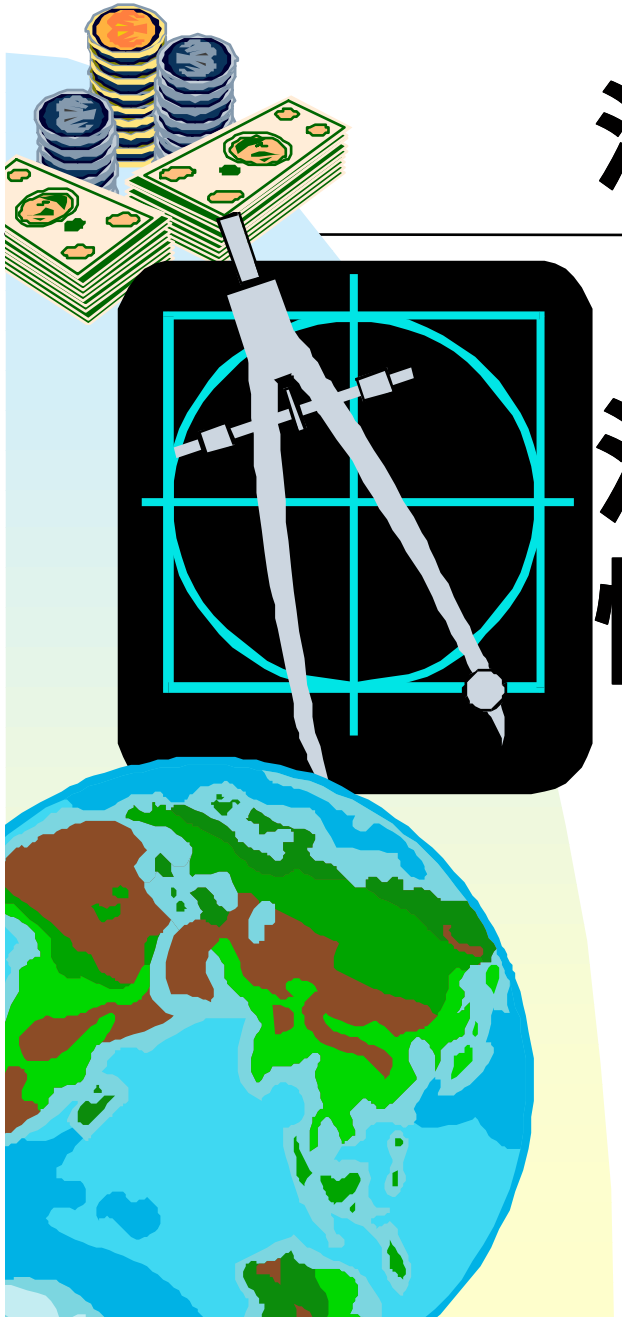
（別添２）

決済システムフォーラム



決済システムにおける情報セキュリティ

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

情報セキュリティ技術とは

- 情報セキュリティとは、機密情報の漏洩、情報の偽造や不正利用などを防止し、情報の安全性・信頼性を確保することをいう。具体的には、次の３つの観点から、情報を保護することを意味する。
  - ①機密性：慎重な取扱を要する情報が、権限のある者のみによって閲覧、変更可能となっていること。
  - ②完全性：情報およびその処理プロセスが、真正かつ完全な状態に保たれること。
  - ③可用性：情報が、権限のあるものによって、必要な時に有効に利用できる状態となっていること。
- 情報セキュリティを確保するための技術の基本となるものが「暗号技術」。

「金融業界や決済システムとは縁遠い？」

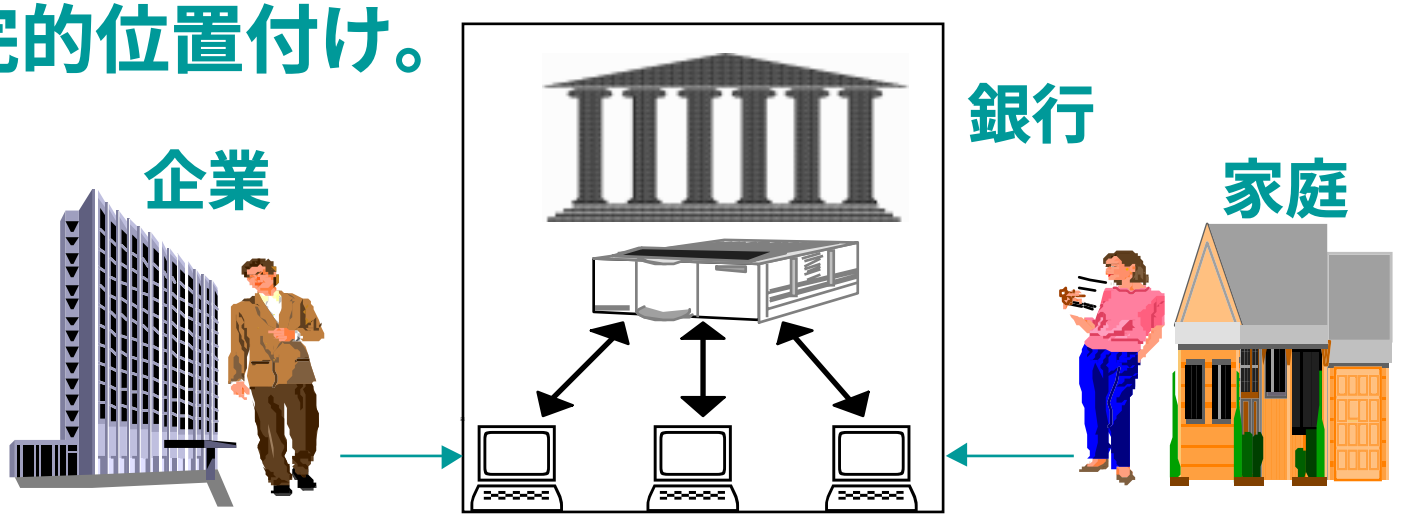
金融業界と情報セキュリティ
――日本と欧米のアプローチの違い

- **欧米諸国においては、従来から、金融業界は情報セキュリティ技術の最大のユーザーと位置付けられていた。**
  - 元々、お金というデジタル化し易い商品を取り扱う商売であり、セキュリティに対する要請も高く、また、他の産業に先駆けてネットワークを構築していたから。
  - **現代暗号の嚆矢**

    1977年に、DES暗号が米国政府標準に認定され、暗号の商用利用が開始された。その背景には、決済情報や顧客情報の情報セキュリティを確保したいという米国金融業界の強いニーズがあった。
- **一方、わが国では、金融機関や決済システムにとって、情報セキュリティ技術や暗号技術が重要という認識は少なかった。**

従来のわが国における決済システムの構造と情報セキュリティ対策

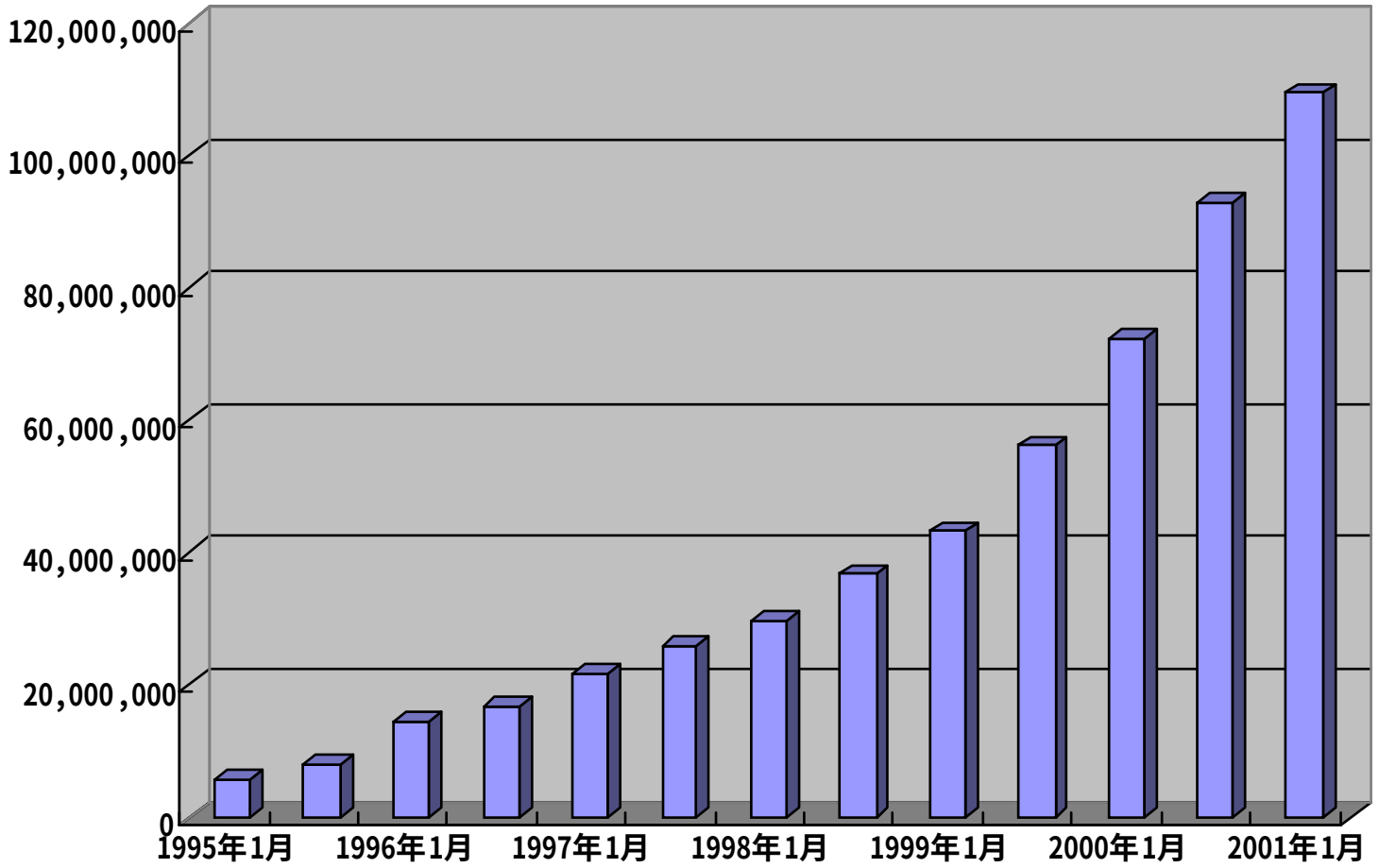
- 従来のポリシー：「閉じたシステム」
- コンピュータ・システムを外部から物理的に隔離することにより安全性を確保する。
- 対策としては、専用回線等による物理的なアクセス制御、バックアップ手段の充実などが中心。暗号技術は補完的位置付け。



・ﾋﾟﾗﾐｯﾄﾞ型　・閉鎖型　・集中ｼｽﾃﾑ

しかし、インターネットの普及に伴い、環境が大きく変わった。

インターネットに接続されたコンピュータ数の推移



データ：Network Wizard社Domain Survey

金融ネットワークのオープン化

【金融機関間取引の分野】

情報通信技術の急速な進歩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取引が増加。

例：STP**化**―Straight-Through Processing

【対顧客取引の分野】

インターネットの発達に伴い、顧客が決済システムへの接続を希望するようになった。

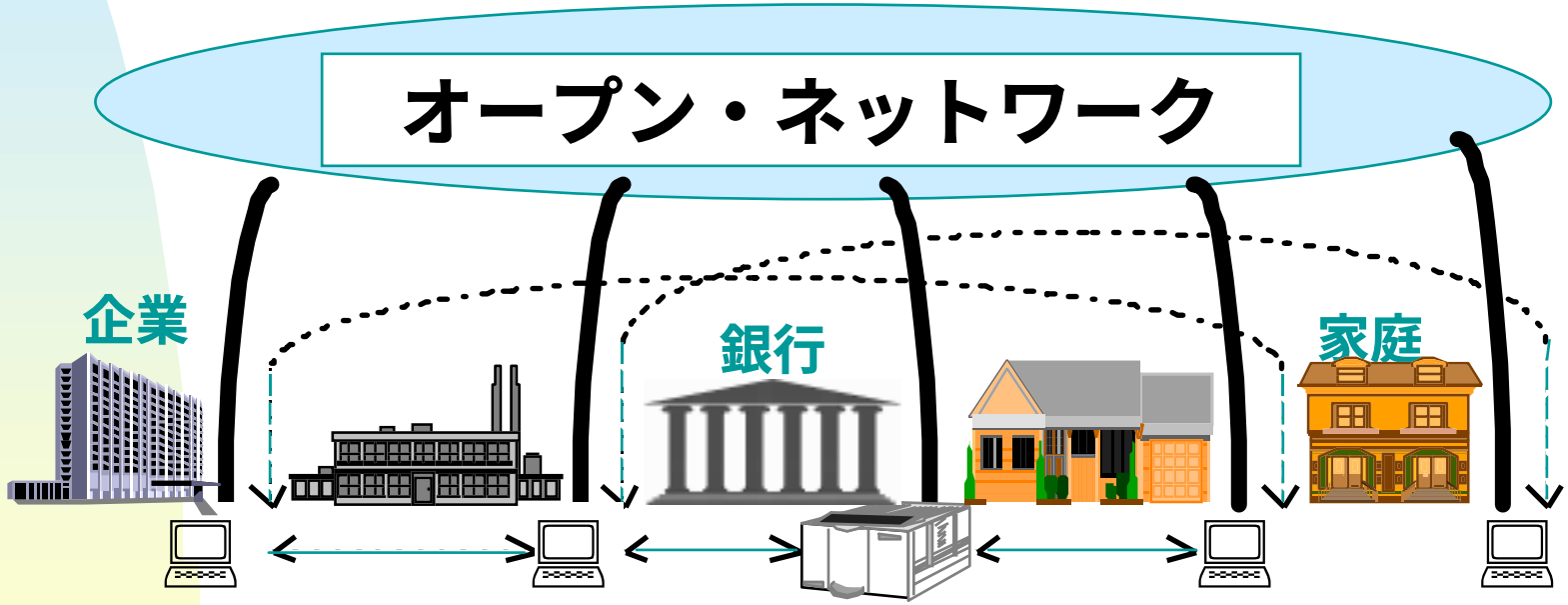
例：インターネット・バンキング、金融EDI**、国際**CMS

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・ネットワークの利用を前提に、金融機関のセキュリティ対策を考え直す必要が生じている。

⇒暗号技術を活用する必要性



・水平型　・開放型（ｵｰﾌﾟﾝ･ｼｽﾃﾑ）　・分散ｼｽﾃﾑ

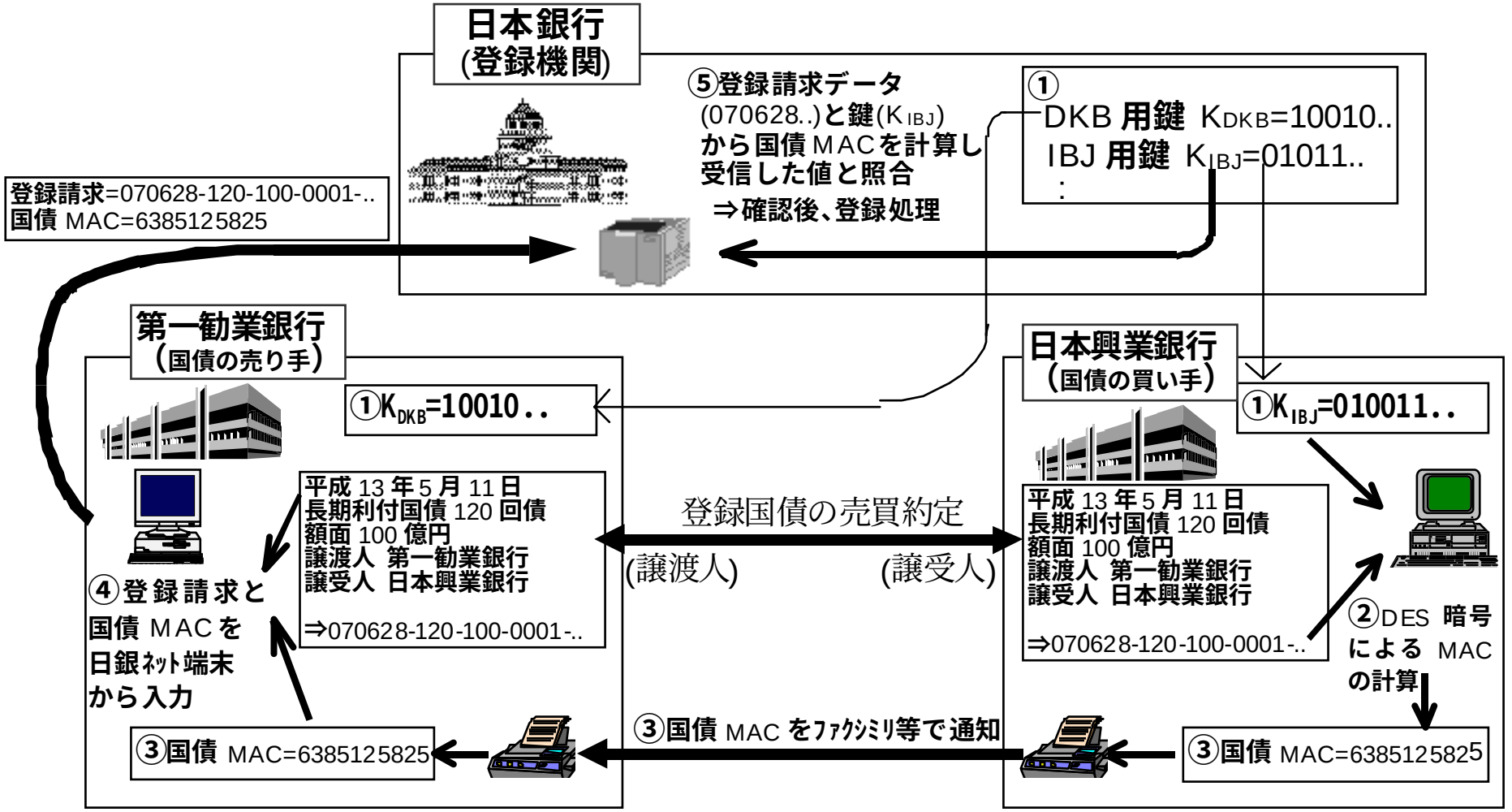
わが国の決済システムにおいても、情報セキュリティ技術が利用されるようになった。

- 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
- 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。

⇒情報セキュリティ技術の重要性の高まり。

日銀ネットにおける国債 MACの仕組み

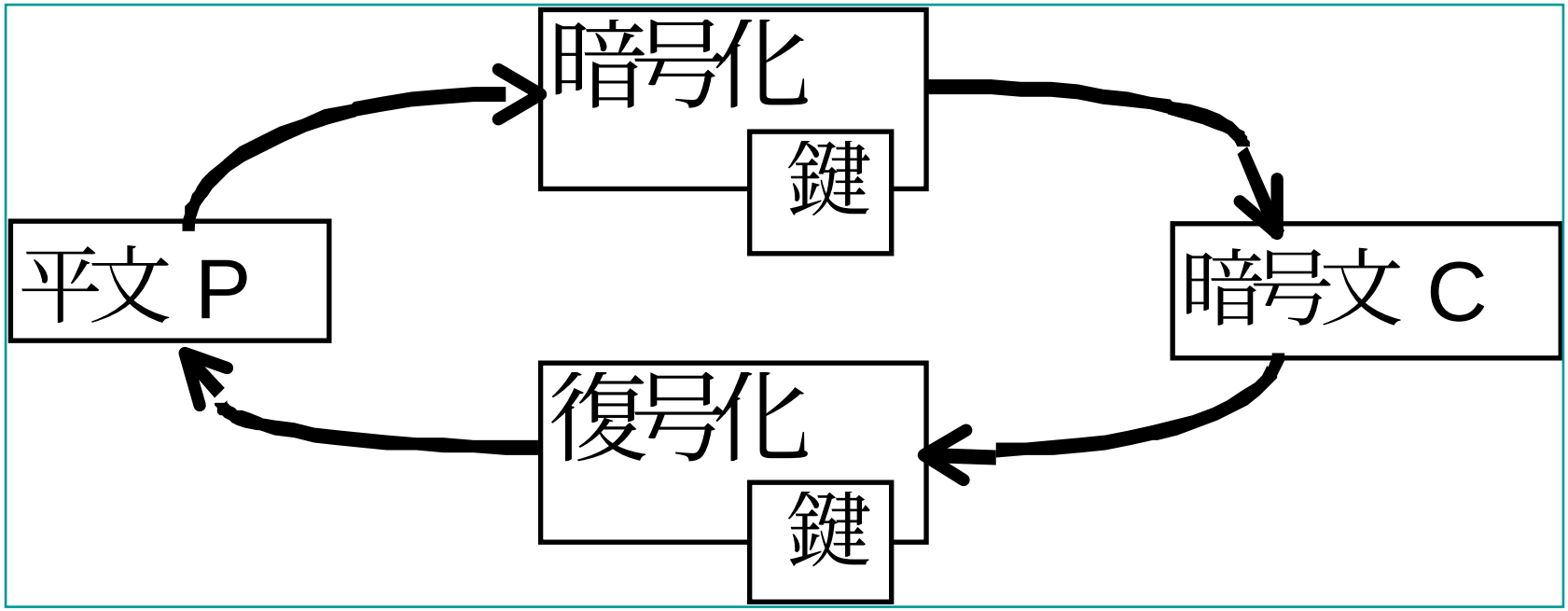


MAC：Message Authentication Code（メッセージ認証子）

暗号アルゴリズムの分類と代表例

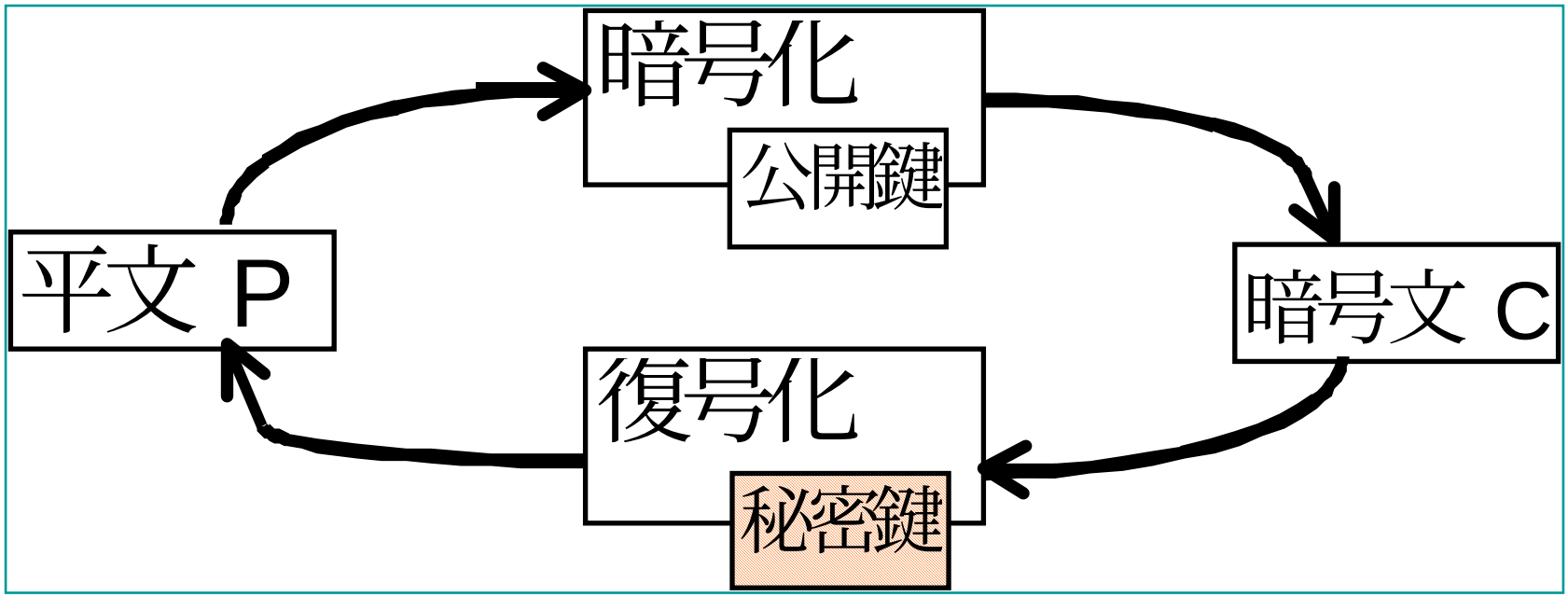
		利用者への鍵の配置の仕方	
		共通鍵方式	公開鍵方式
利用目的	守秘	共通鍵暗号 DES、 トリプル DES、 AES（Rijndael）など	公開鍵暗号 RSA 暗号、 ElGamal 暗号、 楕円曲線 ElGamal など
	認証	共通鍵認証方式 同上（共通鍵暗号アルゴリズムを利用して MAC 等を生成）	デジタル署名 RSA 署名、 ElGamal 署名、DSA、 ECDSA、ESIGN など

共通鍵暗号



①暗号化、復号化に共通の鍵を利用。
②鍵を秘匿することにより秘密を守る。

公開鍵暗号



①公開鍵と秘密鍵とは異なる。

②公開鍵は一般に公開、秘密鍵は鍵作成者が秘匿。

⇒暗号化はだれにでもできるが、復号化は鍵作成者しかできない。

③公開鍵から秘密鍵を推定できない。

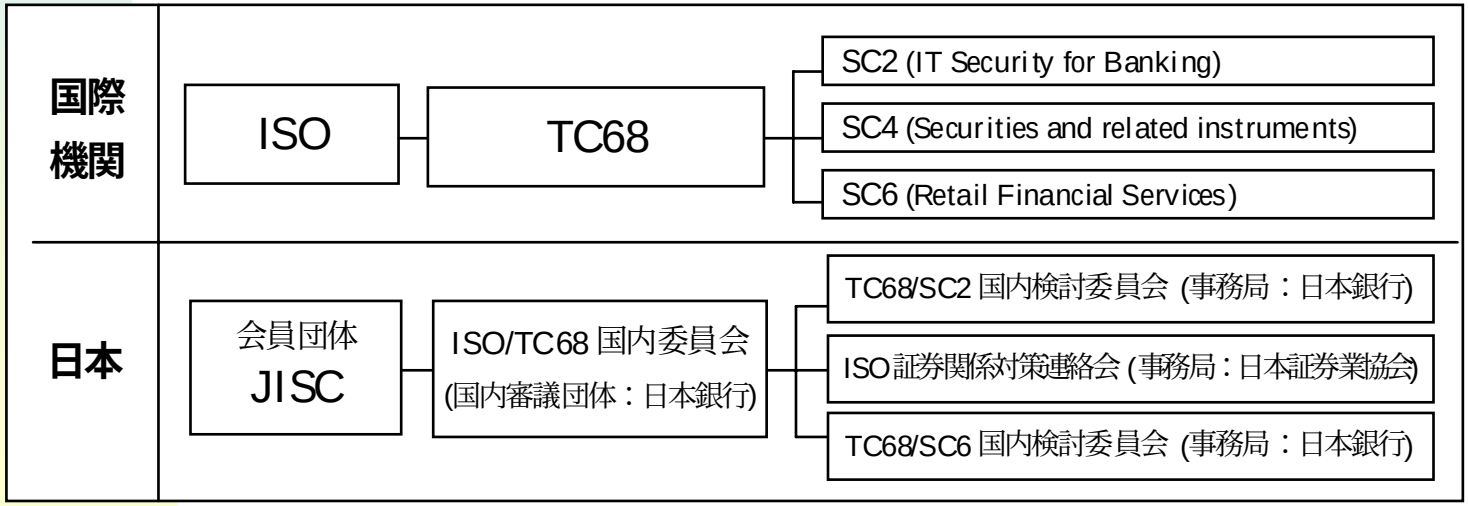
この機能を、守秘、認証の双方に活用可能。

金融分野における情報セキュリティ技術の国際標準化活動（ISO/TC68）

ISO：国際標準化機構（International Organization for Standardization）
―1947年設立の非政府間機構、本部ｼﾞｭﾈｰﾌﾞ、加盟137か国
―分野毎に専門委員会（TC：Technical Committee）を設置

TC68：金融専門委員会
―銀行業務、証券業務などを対象に、国際標準化を実施

ISO/TC68国内委員会
―経済産業省の委嘱により、日本銀行が国内事務局を務める。



DES暗号の強度の低下とISO/TC68の対応

1994年6月

- ISO/TC68/SC2総会において、米国代表が、DESの強度低下に関する問題を提起。DESの後継暗号問題について、TC68としての検討を開始。

1995年4月

- 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」を発表。

1996年秋10月

- 日本からDESの強度評価に関する技術レポートをISO／TC68宛に提出。専用解読装置を用いた全数探索法の脅威を論証。

1997年1月

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

1998年10月

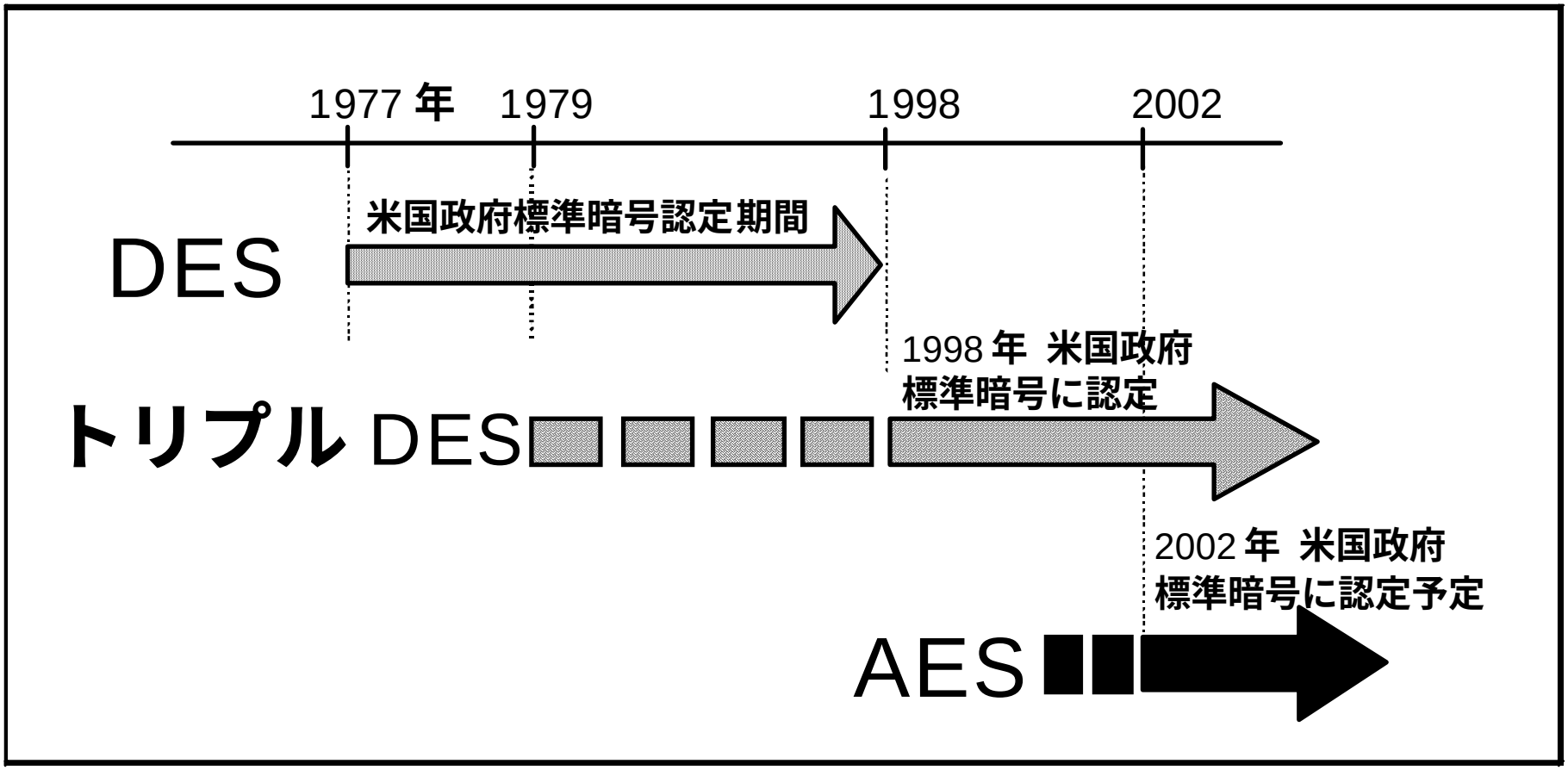
- 米国金融業界によるTriple DESの国内標準化作業完了(ANSI X9.52)。

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からトリプル DES、AESへ



情報セキュリティ技術の選択を誤ると...

- 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

- 直接的な影響：業務の停滞や金銭的被害
- レピュテーションリスク
- リーガルリスク
- 経営的ダメージも

⇒欧州の金融業界におけるリスク顕現化の事例

フランス銀行カード協会
(Groupment des Cartes Bancaires)
ICカードのセキュリティ侵害事件

- 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に起因。
- ハッカーが、ICカードとカードリーダーを解析して仕様を入手し、偽造カードを作成、使用。　⇒マスコミに大きく報道され、信用を失う。
- 2004年までに現行仕様を放棄し、デファクト標準であるEMV仕様を採用。

ドイツ銀行協会仕様のICカード

- ZKA signature card
  - 金融業界が発行する多機能ICカード
  - 電子署名、インターネット・バンキングにおけるユーザー認証、暗号通信、電子マネー（ゲルトカルテ）等に利用される。
  - ISO9796に基づくメッセージ回復型のRSA電子署名アルゴリズムが組み込まれている。
- 1999年、ISO9796に対する新しい署名偽造攻撃法が発見され、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頼性が揺らぐ。
- 2002年から、新しい仕様に移行。

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」
  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。

信頼できる情報セキュリティ技術を選択することの重要性

わが国の金融機関が信頼できる情報セキュリティ技術を見極め、適切に選択していくためには、どうすればよいか？

①情報セキュリティ技術の安全性評価と標準化

②第三者機関による情報セキュリティ機器や運用管理に関する評価・認定

情報セキュリティ技術の安全性評価：暗号技術検討会（CRYPTREC）

- 総務省及び経済産業省が、情報セキュリティの推進を図る観点から開催した、暗号技術の評価等を実施するための検討会。
- 暗号学者・研究者と関係省庁のオブザーバにより構成。座長は東京大学・今井秀樹教授。

【主な検討対象】

- 電子署名法等に基づいて利用される暗号技術の評価（電子署名に用いる暗号技術等への助言）
- 政府で利用される暗号技術の評価（政府認証基盤（GPKI）等で利用される暗号技術への助言）
- 国際標準化に関連する暗号技術の評価（ISO、ITU等における標準化活動の支援）

第三者機関による情報セキュリティ機器や運用管理に関する評価・認定

- 情報セキュリティ機器
- システムの運用管理　等の

具体的な情報セキュリティ技術の適用場面では、

第三者機関による評価・認定スキーム

①ISO15408

②BS7799　（ISO 17799）

が広く利用されつつある。