本資料について

- 本資料は下記著書を基にして作成されたものです。著書の内容は保障できないため、正確な知識を求める方は原本を参考にしてください。

  - 著者　　青木　隆一･稲田　龍　【著】
    村井　純　【監修】
  - 著書名　　PKIと電子社会のセキュリティ
  - 出版社　　共立出版
  - 出版日　　2001年10月25日

PKIと
電子社会の
セキュリティ

渡邊研究室

01J080　**坂野文男**

はじめに

- PKI (Public Key Infrastructure) とは
  - 現実社会における封書、印鑑、内容証明郵便、免許証に相当する機能を実現することができる
    ネットワークインフラストラクチャのための規約あり、
    それに基づくシステム、システムの運用者、
    システムの運用ポリシの総称でもある
  - 現在は、電子社会に包括的セキュリティを提供する最有力候補の地位を得ている

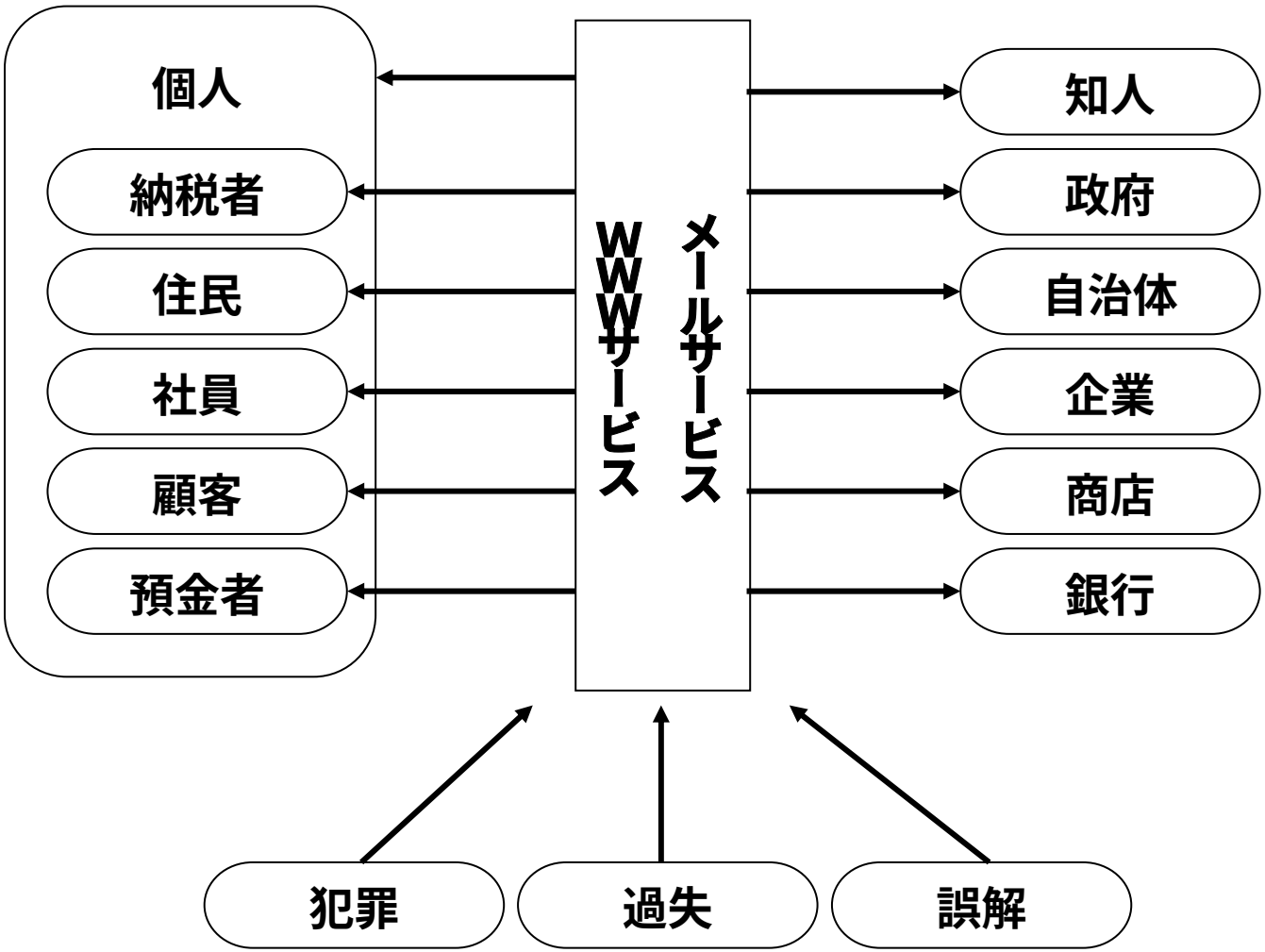
- ネットワークインフラストラクチャとは
  - ネットワークの基盤となるものを示す言葉

1．電子社会のセキュリティー

- 電子社会は、現実社会の人や企業間のコミュニケーションや契約をネットワークを介して行うという現実社会の代理社会である

- 電子社会では、相手の顔が見えない、また情報の偽造が容易である

電子社会の構造



電子社会のセキュリティ要件

- 現実社会に用いられる個々のセキュリティ機能から、対応する電子社会におけるセキュリティ要件をネットワークを介して電子情報を交換する形態を加味して類推する

電子社会のセキュリティ要件

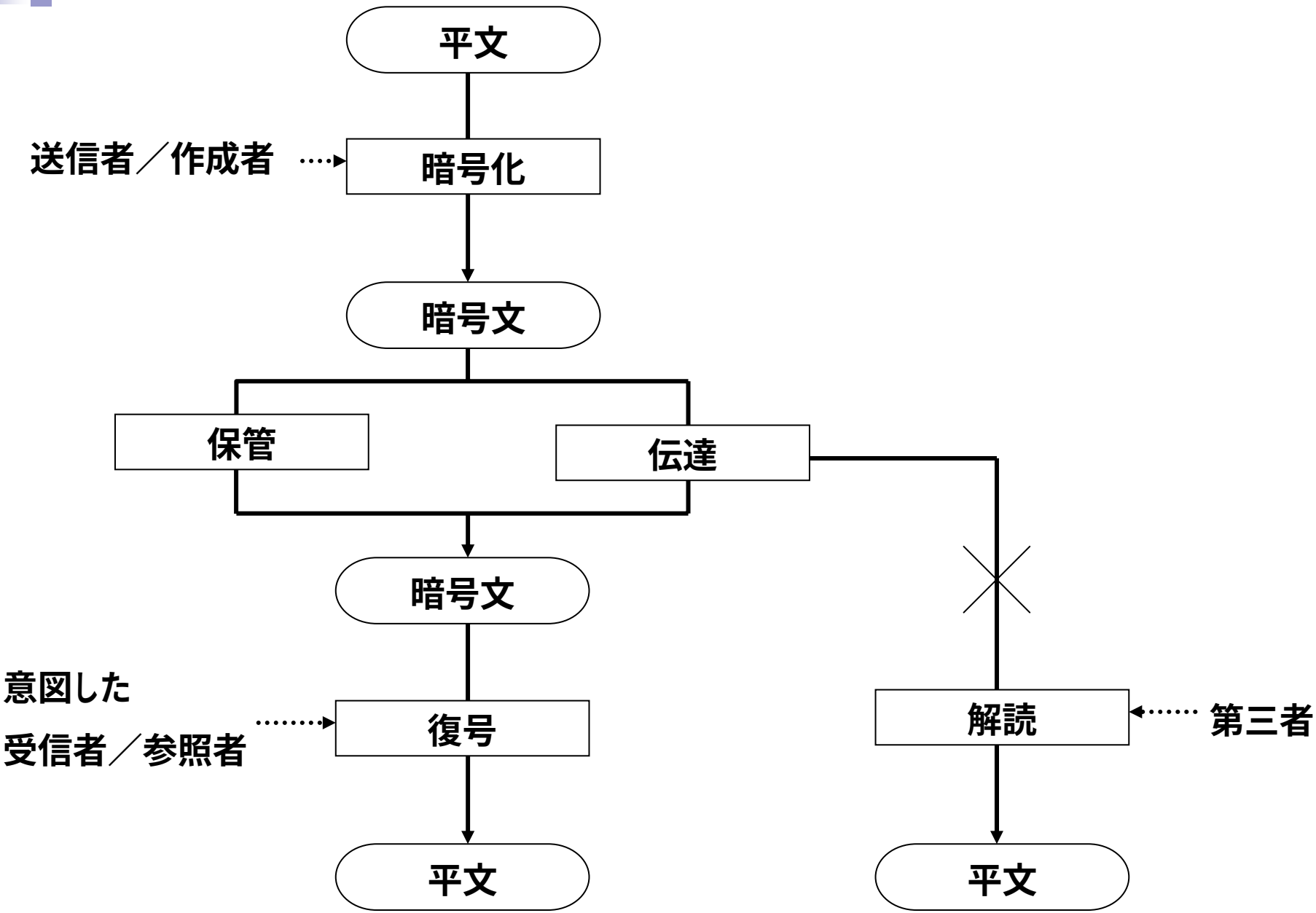
A) エンティティ識別
B) 秘匿
C) 資格証明
D) 権利制御
E) 身元証明
F) 身元保証
G) 物品保証
H) 意志証明
I) 記録
J) 事実証明
K) 保護
L) 防御
M) 規約
N) 裁定
O) 処罰
P) 保険
Q) 偽造防止

- エンティティとは

独立かつ自律的な存在で、個人やサービスに対応する

2．暗号技術の能力

- 暗号
  - 情報の秘匿性を確保するために、その情報を変換する技法である
  - 変換対象となる情報を**平文**
  - 変換後の情報を**暗号文**
  - 平文から暗号文への変換処理を**暗号化**
  - 意図した者による暗号文から平文への逆変換処理を**復号**
  - 意図しない第三者による暗号文から平文への逆変換処理を**解読**

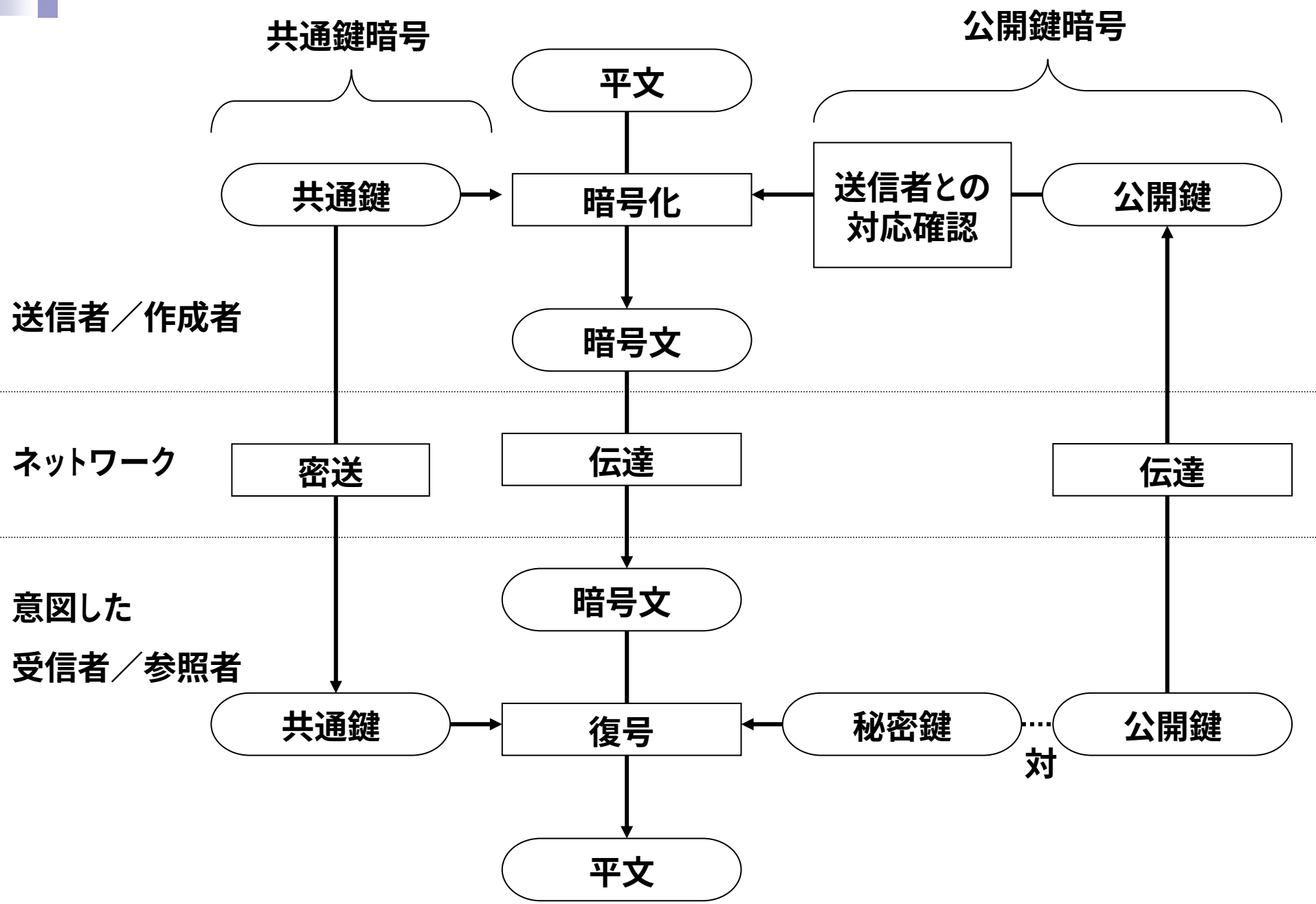

平文
送信者／作成者
暗号化
暗号文
保管
伝達
暗号文
意図した
受信者／参照者
復号
解読
第三者
平文
平文

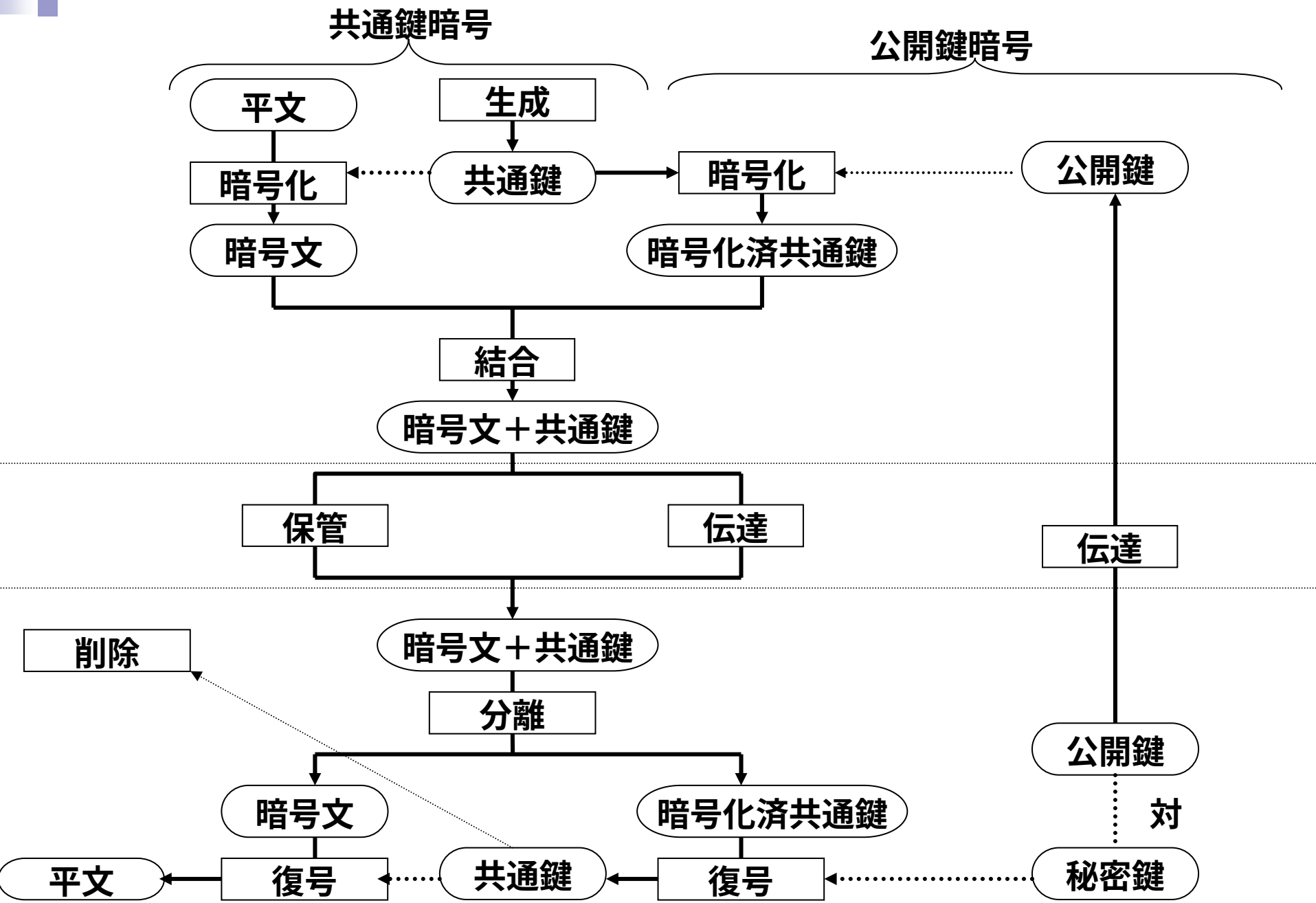
共通鍵暗号方式

- 暗号化と復号で同じ鍵を用いる暗号
- 暗号化処理および復号処理の処理コストが小さい
- 鍵を第三者には秘密にして、送信者と受信者の間で共有しなければならない
- N人の間の、任意の2人の間のみの通信を可能にするためには、N*(N-1)/2個の組み合わせがあるため同じ数の鍵が必要になるため、鍵の管理が大変になる

公開鍵暗号方式

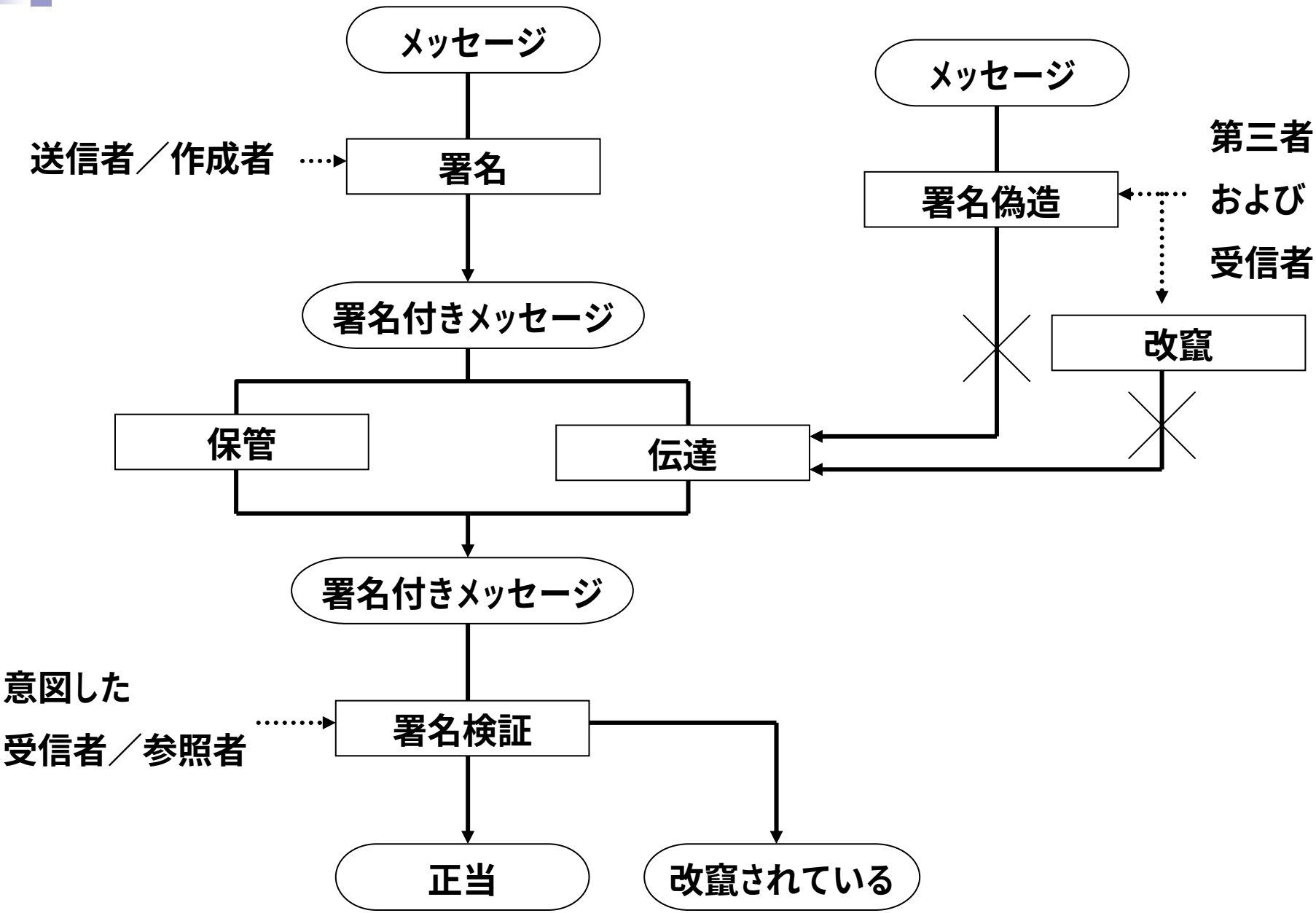
- 暗号化と復号において対になった異なる２つの鍵を用いる
- 一方の鍵から他方の鍵を導出することが困難
- 公開鍵は秘匿して共有する必要はない
- 鍵の管理が共通鍵と比べ容易
- 受信者の者と見なしている公開鍵が、本当に受信者の公開鍵であることの確認が必要
- 処理コストが大きい


共通鍵暗号
公開鍵暗号
平文
共通鍵
暗号化
送信者との
対応確認
公開鍵
送信者／作成者
暗号文
ネットワーク
密送
伝達
伝達
意図した
受信者／参照者
暗号文
共通鍵
復号
秘密鍵
公開鍵
対
平文


共通鍵暗号
公開鍵暗号
平文
生成
暗号化
共通鍵
暗号化
公開鍵
暗号文
暗号化済共通鍵
結合
暗号文＋共通鍵
保管
伝達
伝達
削除
暗号文＋共通鍵
分離
公開鍵
暗号文
暗号化済共通鍵
対
平文
復号
共通鍵
復号
秘密鍵

署名

- 変換後のデータが署名者によって署名されたことを検証する検証処理
- 署名により提供するセキュリティー能力
  A) 一貫性
  B) データ認証
  C) 否認拒否


メッセージ
送信者／作成者
署名
署名付きメッセージ
保管
伝達
メッセージ
署名偽造
第三者
および
受信者
改竄
署名付きメッセージ
意図した
受信者／参照者
署名検証
正当
改竄されている

- **署名に必要な機能**
  - A) **メッセージと署名の一体化**
  - B) **改竄検出**
  - C) **署名と署名者の対応**

電子署名

- 公開鍵暗号方式による変換をメッセージ全体に行うと、暗号と同じく変換処理コストが高くなる。
  そのため、メッセージに一方向性関数を適用し、小さいサイズの電子情報に変換する。
  この処理をメッセージダイジェスト(MD：Message Digest) 処理と呼び、得られた電子情報をMD値と呼ぶ。
- 一方向性関数とは、簡単に計算できるが逆関数の計算は非常に困難である関数

- メッセージダイジェスト処理を行う関数をf_Dとすると次の条件を満足するものである。

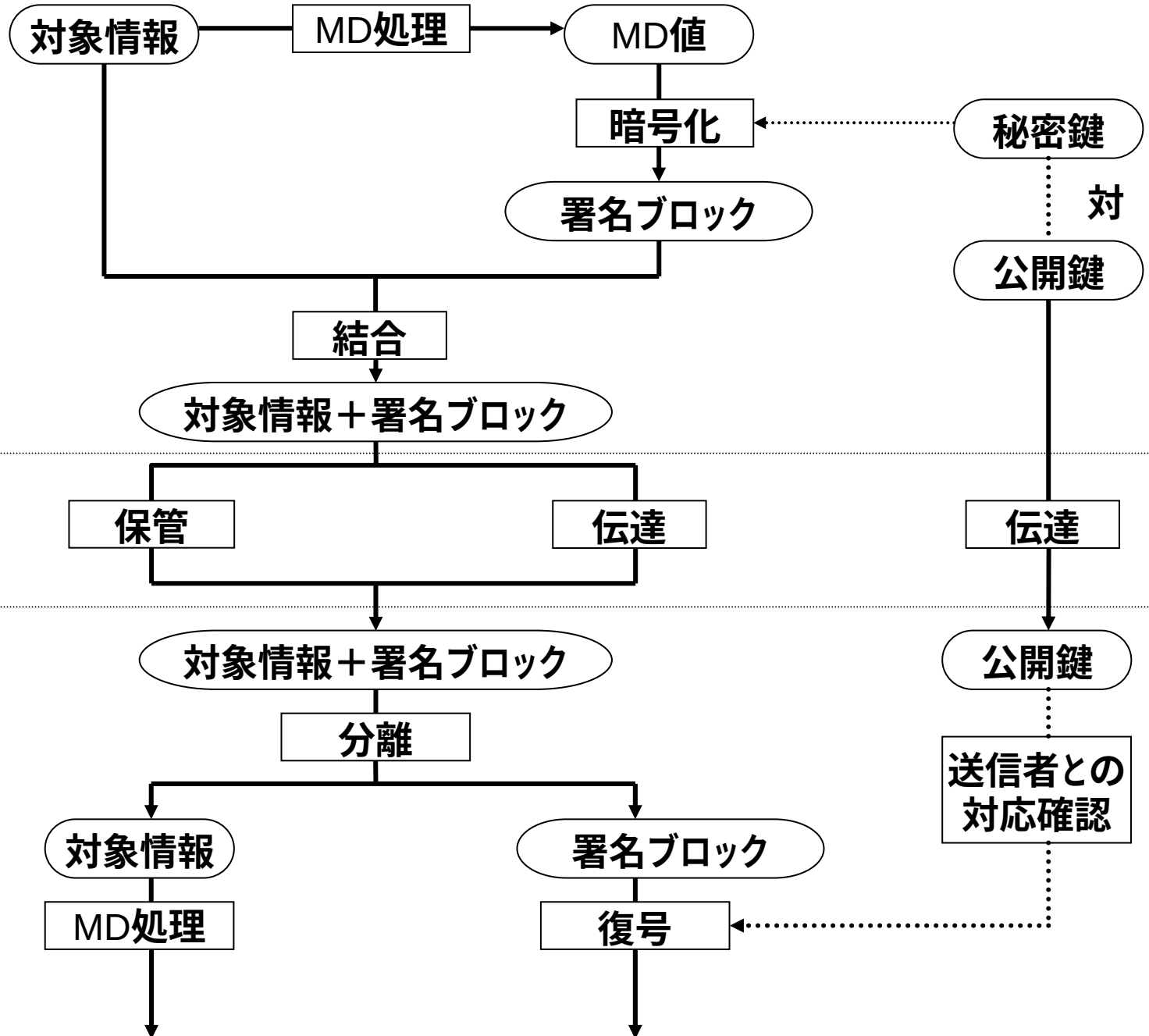
  （mが対象情報、m_DがMD値、$m_D = f_D(m)$ ）

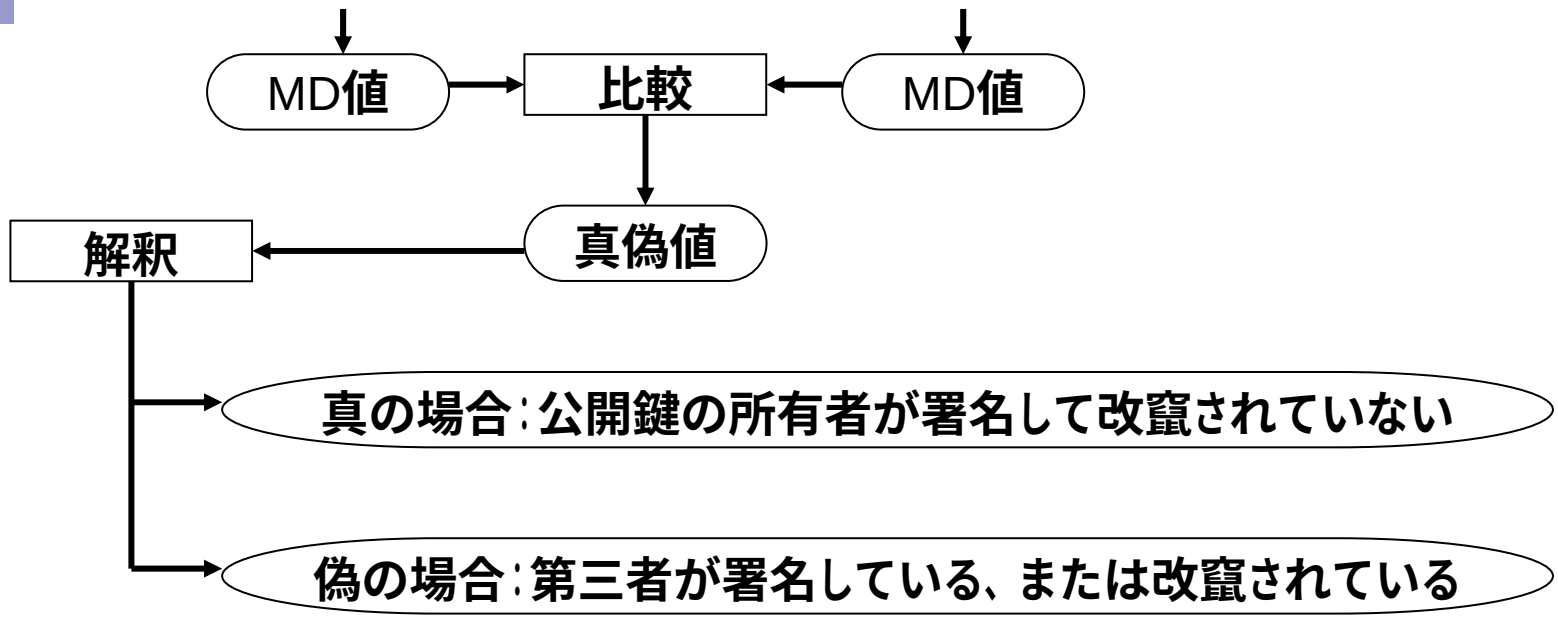
  A) 入力mは任意の長さの電子情報である

  B) $m_D = f_D(m)$ において、mからm_Dを計算することは容易である

  C) $m_D = f_D(m)$ において、特定のm_Dを得るmを見つけ出すことは困難である

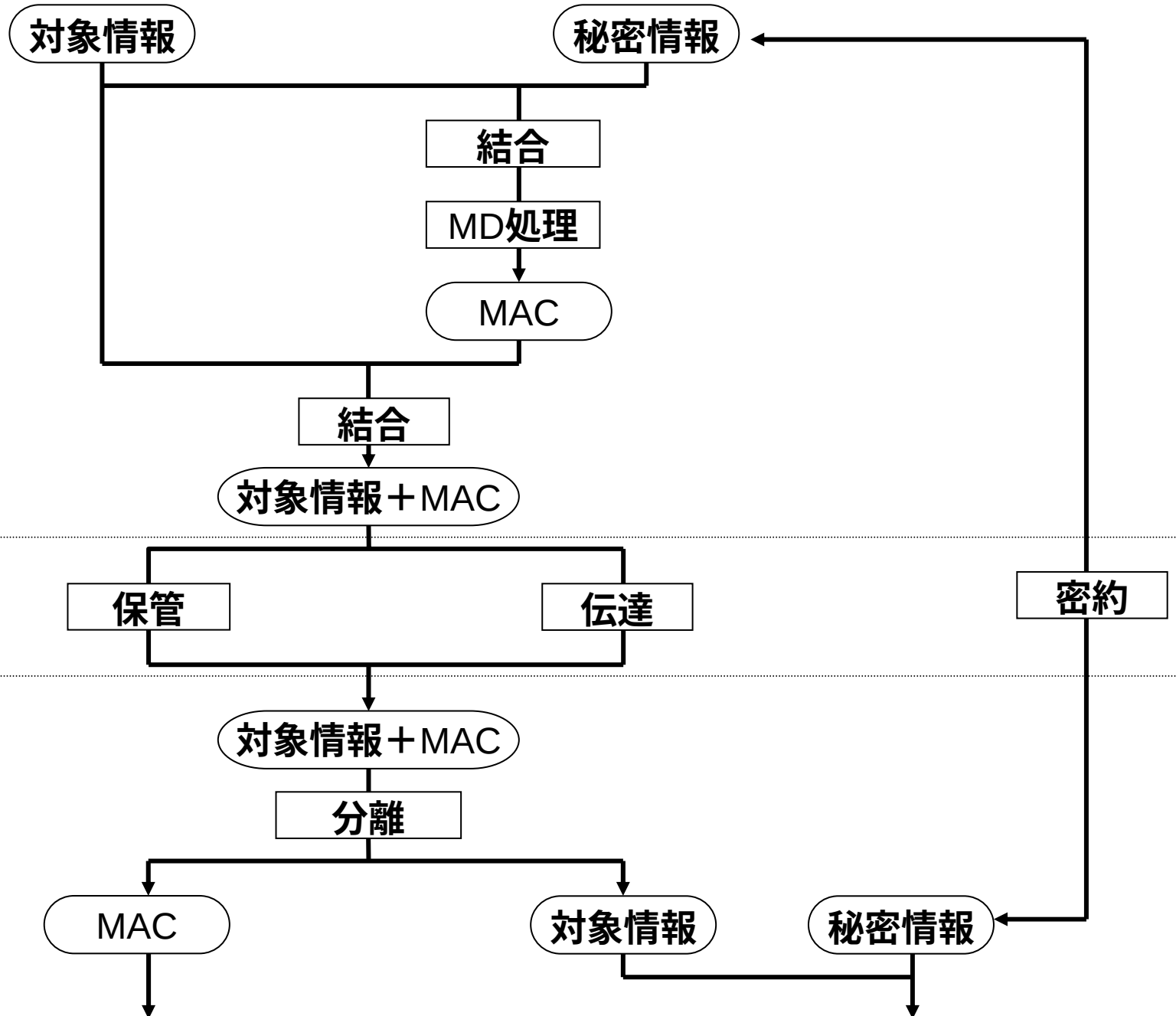
  D) mと任意の1ビットが異なるm'に対して$f_D(m) \neq f_D(m')$ である

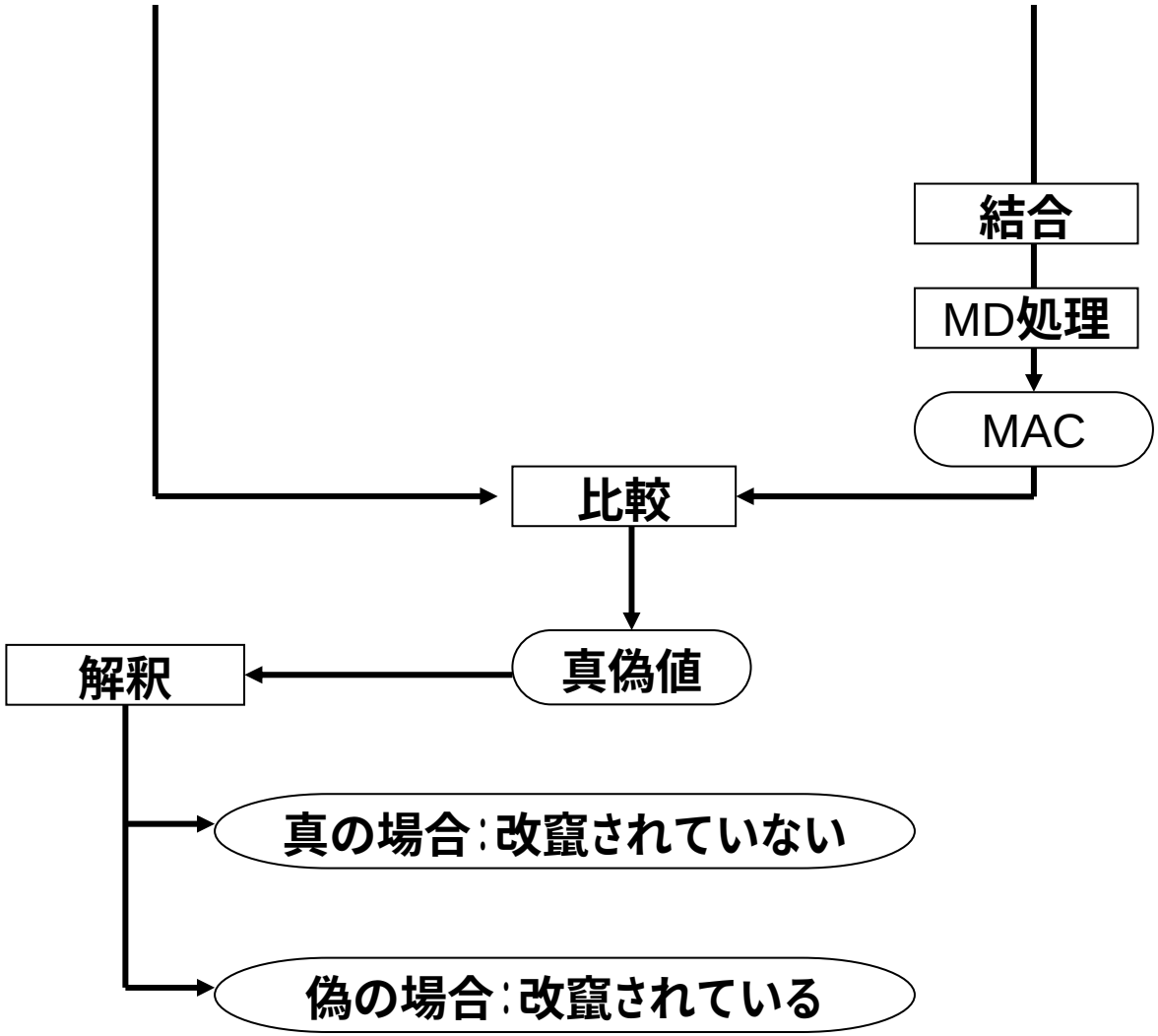

対象情報
MD処理
MD値
暗号化
秘密鍵
署名ブロック
対
公開鍵
結合
対象情報＋署名ブロック
保管
伝達
伝達
対象情報＋署名ブロック
公開鍵
分離
送信者との
対応確認
対象情報
署名ブロック
MD処理
復号


MD値
比較
MD値
真偽値
解釈
真の場合：公開鍵の所有者が署名して改竄されていない
偽の場合：第三者が署名している、または改竄されている

メッセージ認証コード
(MAC：Message　Authentication　Code)

- **送信者と受信者で共有する秘密情報を利用し、知っているもののみが付与できるコードをメッセージに付加することにより一貫性のみを提供する方法**
- **秘密情報の共有方式が任意であるため、公開鍵暗号を用いてない場合でも利用でき、原理的に処理コストが低くなる**


対象情報
秘密情報
結合
MD処理
MAC
結合
対象情報＋MAC
保管
伝達
密約
対象情報＋MAC
分離
MAC
対象情報
秘密情報


結合
MD処理
MAC
比較
真偽値
解釈
真の場合：改竄されていない
偽の場合：改竄されている

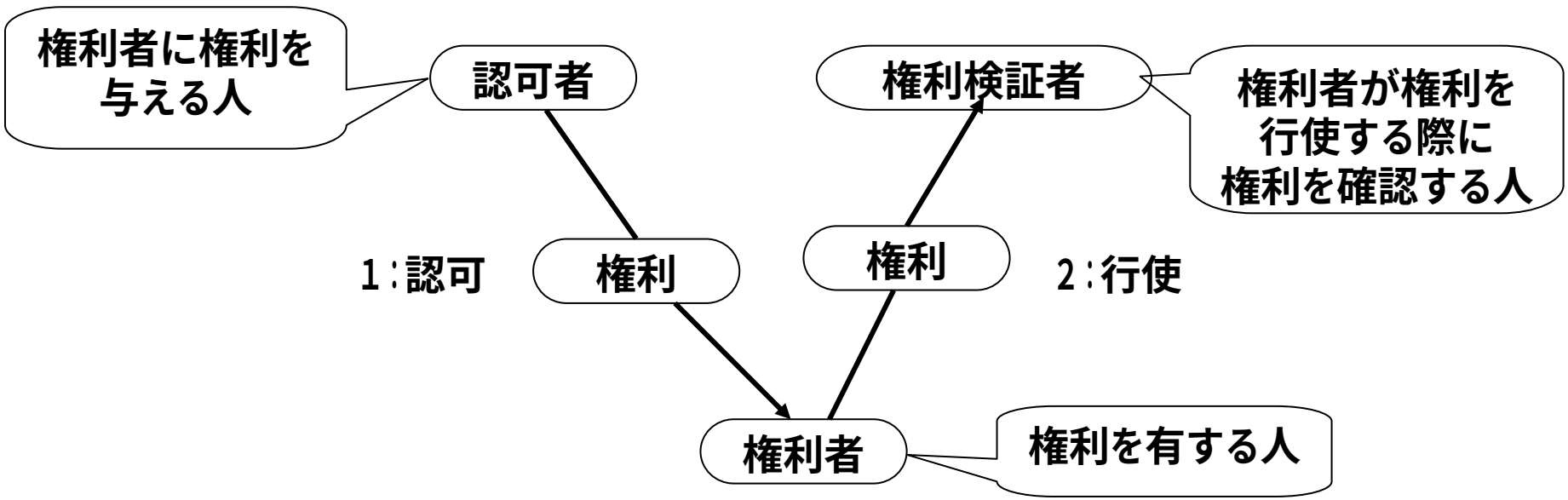
3.セキュリティの基礎モデル

- PKIの目的は、「受信者との対応確認」また「送信者との対応確認」を可能にすること
  - エンティティを特定する情報と公開鍵をペアにして利用者がすでに信用しているエンティティが電子署名することにより、エンティティと公開鍵の対応を保証する

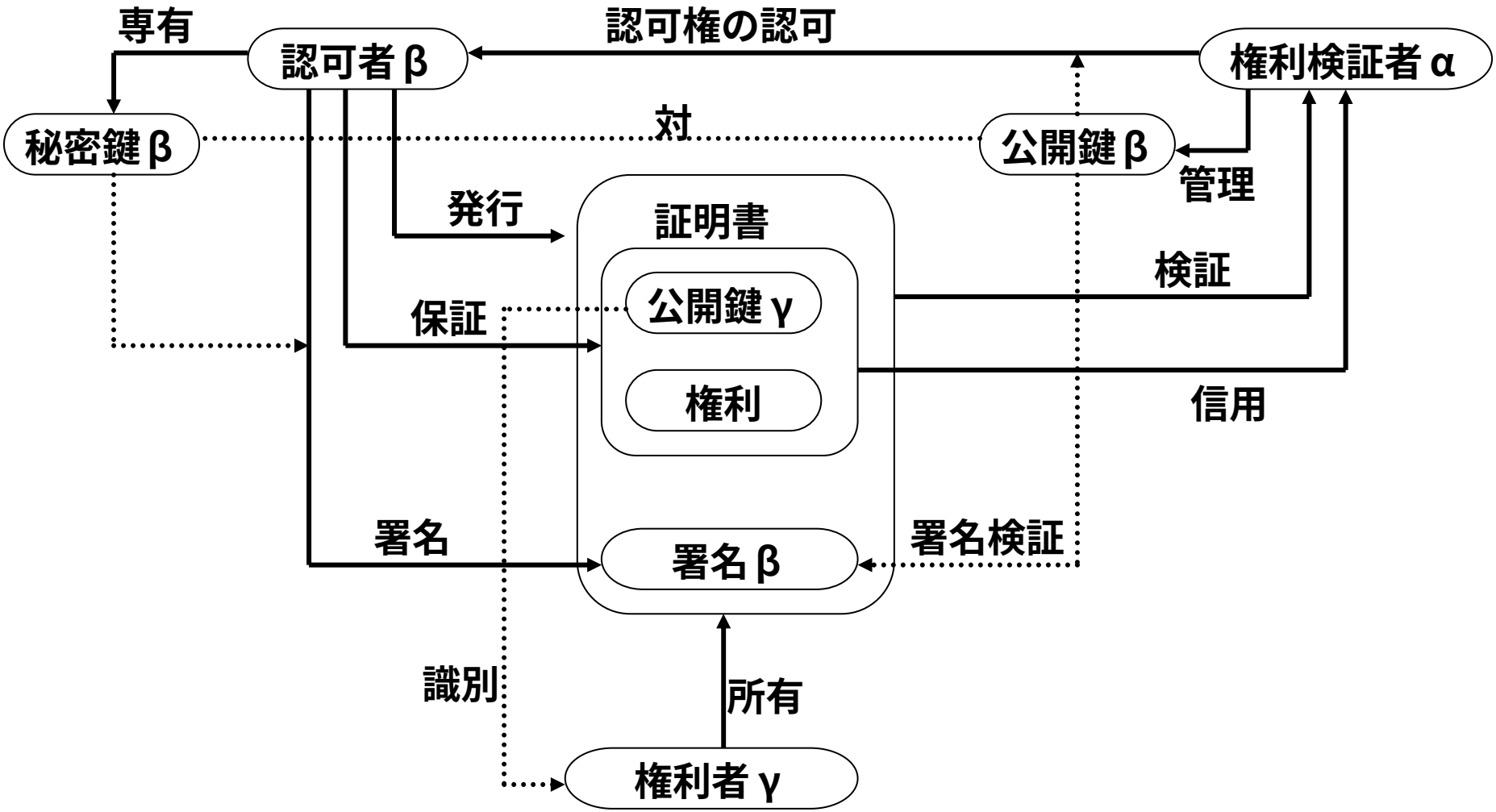
属性と権利

- 属性
  - エンティティや人に関連付けられた特定の意味を持った容器
    - 例：血液型、生年月日、住所、名前、免許、役職など
- 権利
  - 属性内で、それを有するエンティティに、何らかの行為の実施許可や実施能力を認めること

- 権利を与えることを認可、権利を用いることを行使と呼ぶ
- 権利の認可および行使に関係する役割とプロセス

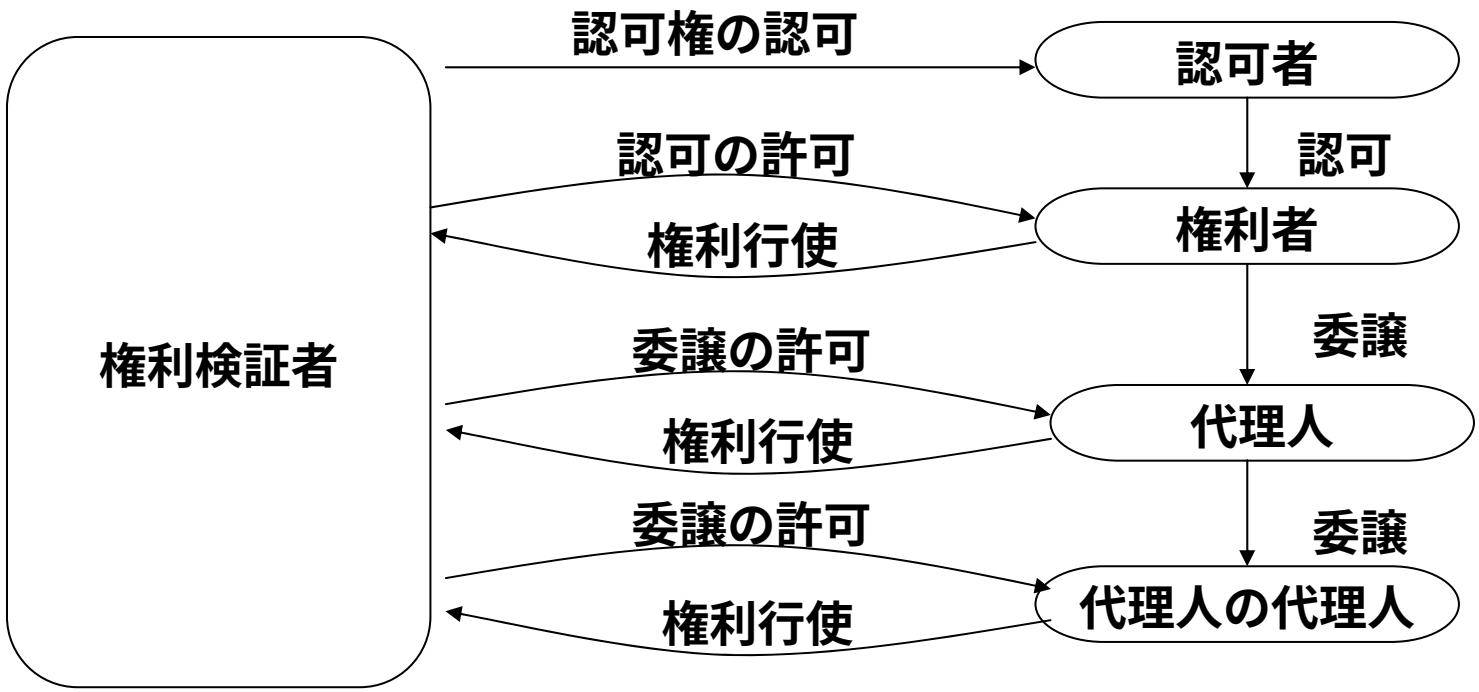


権利の保証


専有
認可者 β
認可権の認可
権利検証者 α
秘密鍵 β
対
公開鍵 β
管理
発行
証明書
検証
保証
公開鍵 γ
権利
信用
署名
署名 β
署名検証
識別
所有
権利者 γ

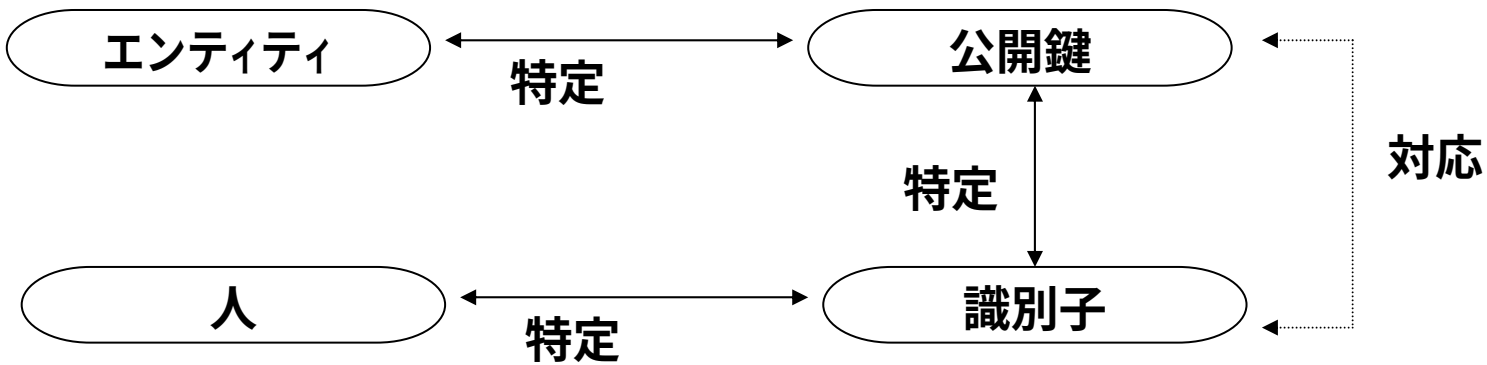
権利委譲

- 権利者が他者に対して自身が持つ権利を委譲すること
- 公開鍵認証者が他の公開鍵認証者に公開鍵認証権を委譲するという、PKIの本質的な枠組みを実現するために用いられる



本人特定

- 電子社会が現代社会の代理社会として機能するために、現代社会の人とエンティティとの対応がとられていなければならない
  - 公開鍵と対応させる



•人を識別子で特定する理由

人は電子情報として扱えないため、任意の型式のデータを人の識別子として扱う

例：氏名、住所、社員番号

おわりに

- これらのことは一般的な機能や原理と考えられ、PKIの基盤となっているものです。

終わり