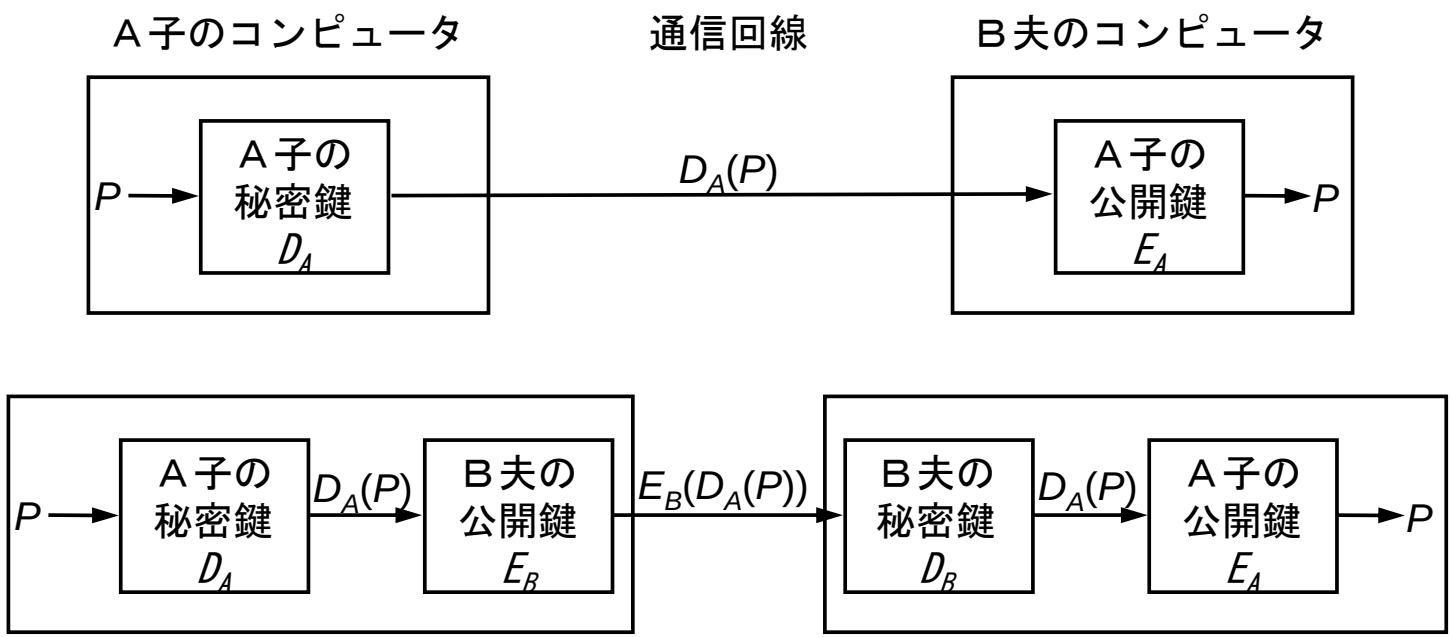
デジタル署名

- 受信者が送信者の身元を確認できる
- 送信者は、送ったメッセージの内容を否認できない
- 受信者がメッセージをでっち上げることはできない

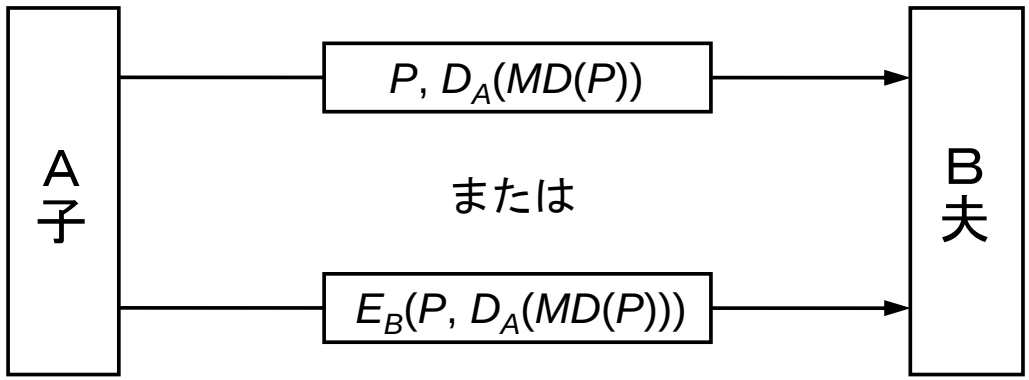
公開鍵暗号によるデジタル署名

- $E_k(D_{k'}(P)) = D_{k'}(E_k(P)) = P$ であるなら



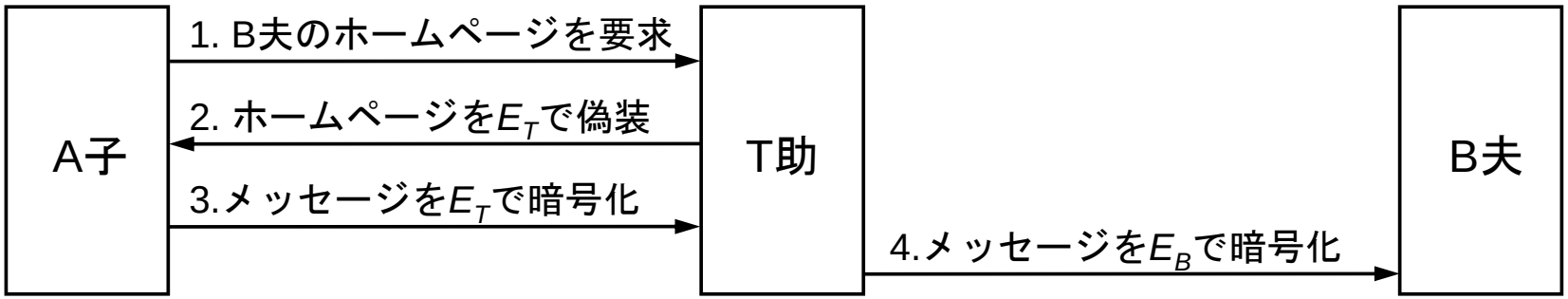
メッセージダイジェスト

- Pから$MD(P)$を計算するのは容易
- $MD(P)$からPを見つけるのは極めて困難
- $MD(P)$＝$MD(P')$となるP, P'の組を作成することはできない

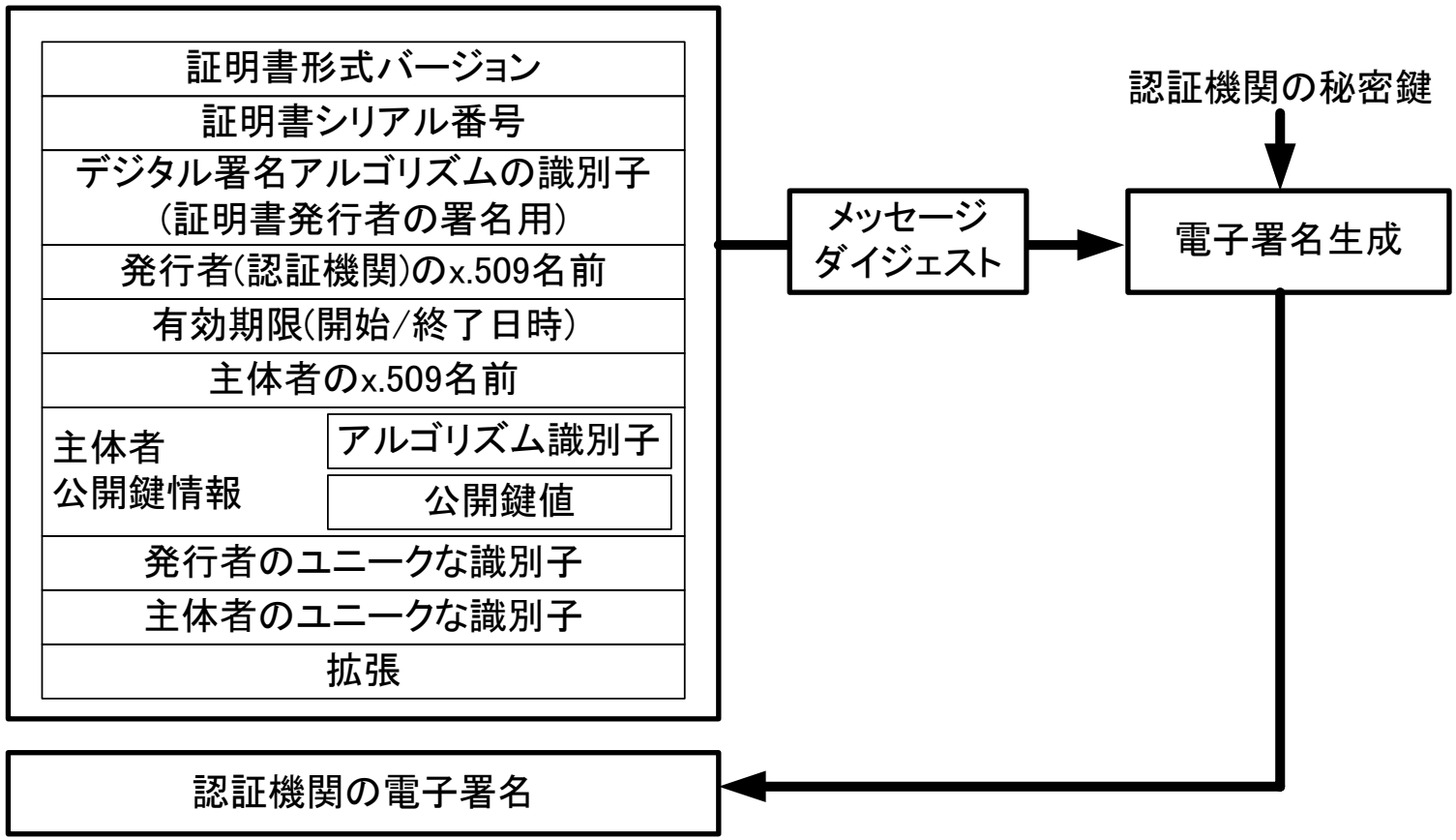


公開鍵の安全な取得

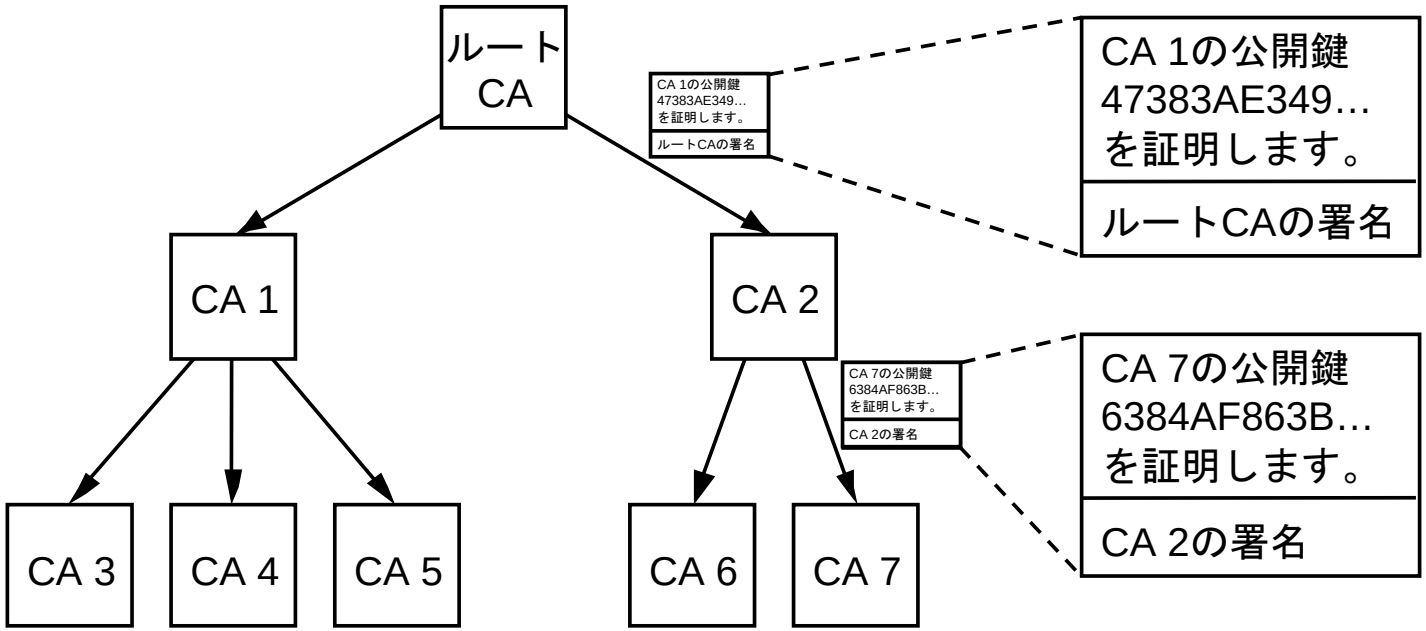
- 公開鍵をホームページで公開したら…



公開鍵証明書


証明書形式バージョン
証明書シリアル番号
デジタル署名アルゴリズムの識別子
(証明書発行者の署名用)
発行者(認証機関)のx.509名前
有効期限(開始/終了日時)
主体者のx.509名前
主体者
公開鍵情報
アルゴリズム識別子
公開鍵値
発行者のユニークな識別子
主体者のユニークな識別子
拡張
メッセージ
ダイジェスト
認証機関の秘密鍵
電子署名生成
認証機関の電子署名

Certification Authorities



PGP, S/MIME

- PGP (Pretty Good Privacy)
  - 1991にPhil Zimmermannが開発
  - フリーのPC向けパッケージソフト
  - 「友達の友達は友達」信頼モデル
- S/MIME (Secure/MIME)
  - RSA Security社が開発→RFC2311〜2315
  - 何らかの公開鍵証明書が必要

4.3 著作権保護

デジタルコンテンツと著作権

- デジタルコンテンツ：複製が容易かつ複製による劣化が生じない
- プログラムの不正コピー
- 海賊版CD
- Napster, WinMX, Winny等のピアツーピアファイル交換ソフトウェア

電子透かし

- コンテンツのヘッダ等ではなくコンテンツ本体に情報を埋め込む
- コンテンツの品質をできるだけ劣化させず、コンテンツを編集・加工しても埋め込んだ情報が消えないことが望ましい

情報の埋め込み・検出方法

- 人の知覚特性を利用し、人が知覚困難な範囲でディジタルデータを改変
  - オリジナルデータと比較することで検出な方式
  - 鍵を知るものだけが検出可能な方式
  - 誰でも検出可能な方式

電子透かしの用法

- 権利保有者の情報を埋め込む
  - 不正使用を見つけた際に権利を主張
- 一次取得者の情報を埋め込む
  - 不正使用を見つけた際に誰が「横流し」したのか確認できる