企業システムのためのPKI

発表者
00J120　保母雅敏

PKI(Public Key Infrastructure)とは

- 公開鍵暗号に基づいた証明書を作成、管理、保管、配布、破棄するために必要なハードウェア、ソフトウェア、人、手続きのこと

PKIが必要になった背景

- インターネットの急速な普及
- 電子データの大量漏洩
- 電子データの改ざん
- インターネット取引での不正
- インターネット上での盗聴や改ざん

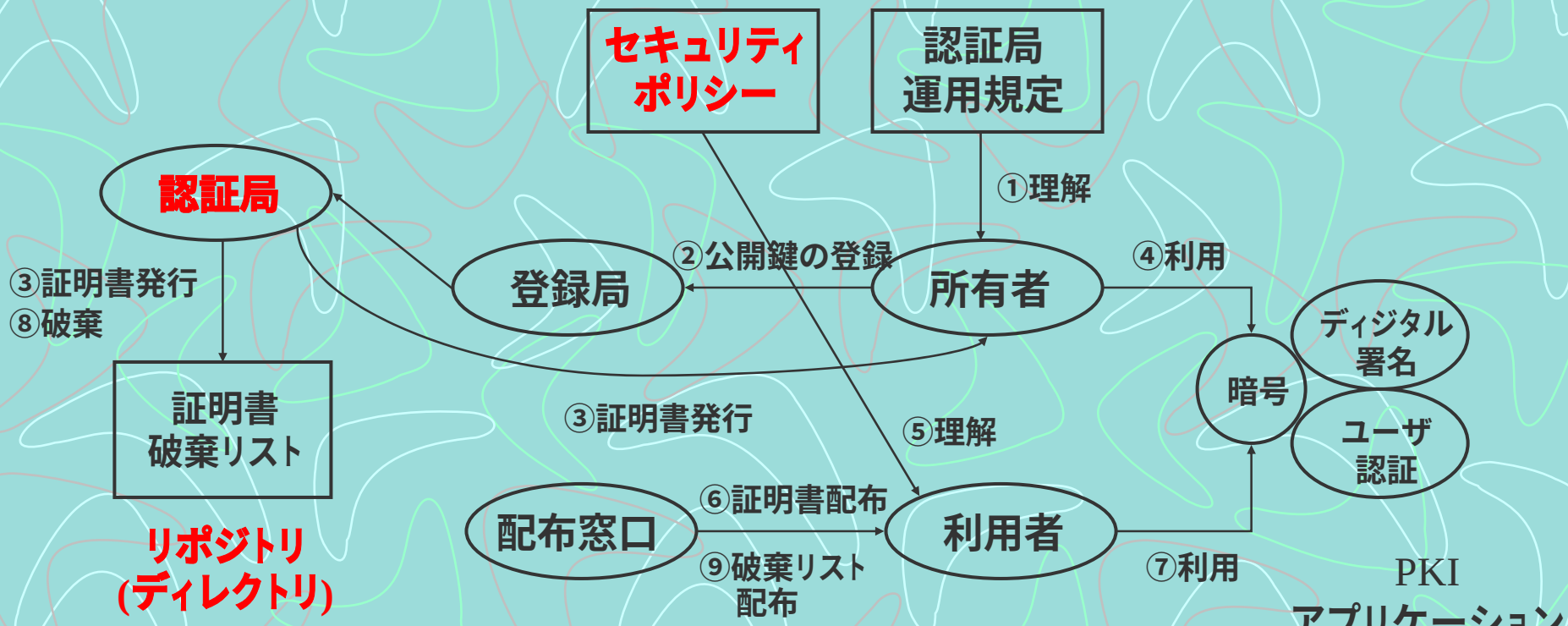
PKIの主な機能

- 暗号
- ディジタル署名
- 公証
- ブラインド署名
- タイムスタンプ
- ユーザ認証

PKIがカバーするセキュリティ機能

- 情報漏洩防止(機密性確保)
- 取引者の特定防止(匿名性確保)
- 改ざん防止(完全性確保)
- 否認防止(責任追及性確保)
- なりすまし防止(本人正確保)

PKIを構成する主な要素



認証局

- 公開鍵の持ち主を証明する機関
- 公開鍵を登録することにより、公開鍵証明書を発行する

- 認証局が信用できることを示すために、認証局運用規定を作成する

ブリッジ認証局

- 複数の認証局で発行する証明書を相互に利用可能にするための認証局

- 府省認証局
- 民間認証局
- 電子認証登記所

がブリッジ認証局と相互認証を行っている

リポジトリ(ディレクトリ)

- 証明書配布機能を持つサーバ。
- 公開鍵証明書、証明書破棄リスト(CRL)の配布を行う。

- 公開鍵証明書、証明書破棄リストは誰でも入手できる。

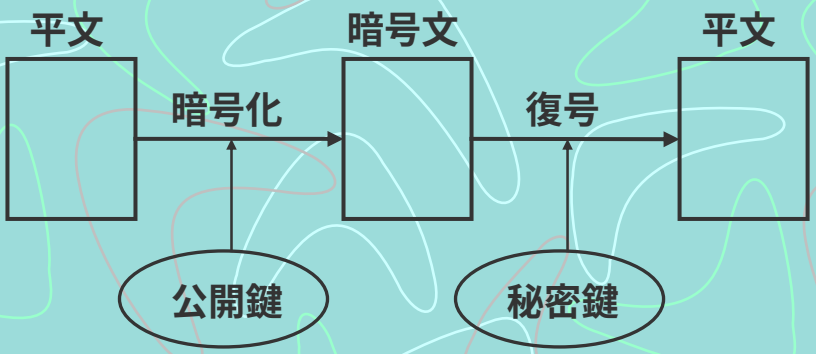
セキュリティポリシー

- 証明書利用者が証明書所有者をどのように認証するか、どのような規則でシステム利用の権限を与えているか、などを規定する文書

- 認証局運用規定はセキュリティポリシーの一部

公開鍵暗号

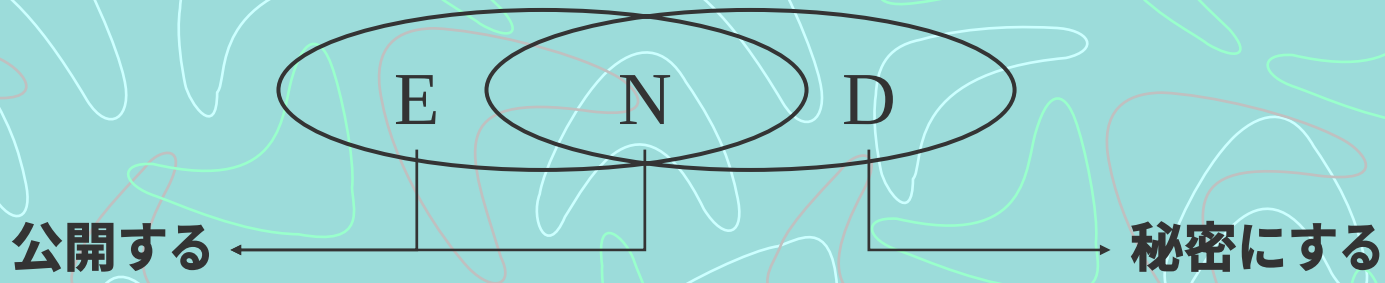
- 1976年にDiffieとHellmanによって提案された
- 公開鍵、秘密鍵のペアを使い、暗号化･復号を行う
- RSAアルゴリズムが有名



文書の暗号化

RSAアルゴリズム

- 鍵長は512,768,1024,2048ビットが使われる
- 鍵ペアはn,e,dから成り、e,nの組を公開鍵として公開する



RSAアルゴリズム
RSA鍵ペアの生成法(2048ビット)

- 1024ビットの素数p,qを乱数によって見つける
  (乱数のチェックに鍵生成の大半を消費する)
- n=pqを計算する。nは2048ビットになるものにする
- Φ(n)=(p-1)(q-1)と互いに素である小さな奇数eを選ぶ
  eは通常 $2^{16}+1=65537$ が選ばれる
- (d･e)mod Φ(n)=1となるようなdを計算する
- eとnの組PをRSA公開鍵とする
- dとnの組SをRSA秘密鍵とする

RSAアルゴリズム
–暗号化アルゴリズム-

平文をM、暗号文をCとする

$$C = P(M) = M^e \bmod n$$

$$M = S(C) = C^d \bmod n$$

データが鍵よりも短い場合は、先頭にデータを付加して鍵長を合わせる(パディング)

一般には鍵長より短いデータに使われる

RSAアルゴリズム
-公開鍵暗号の安全性-

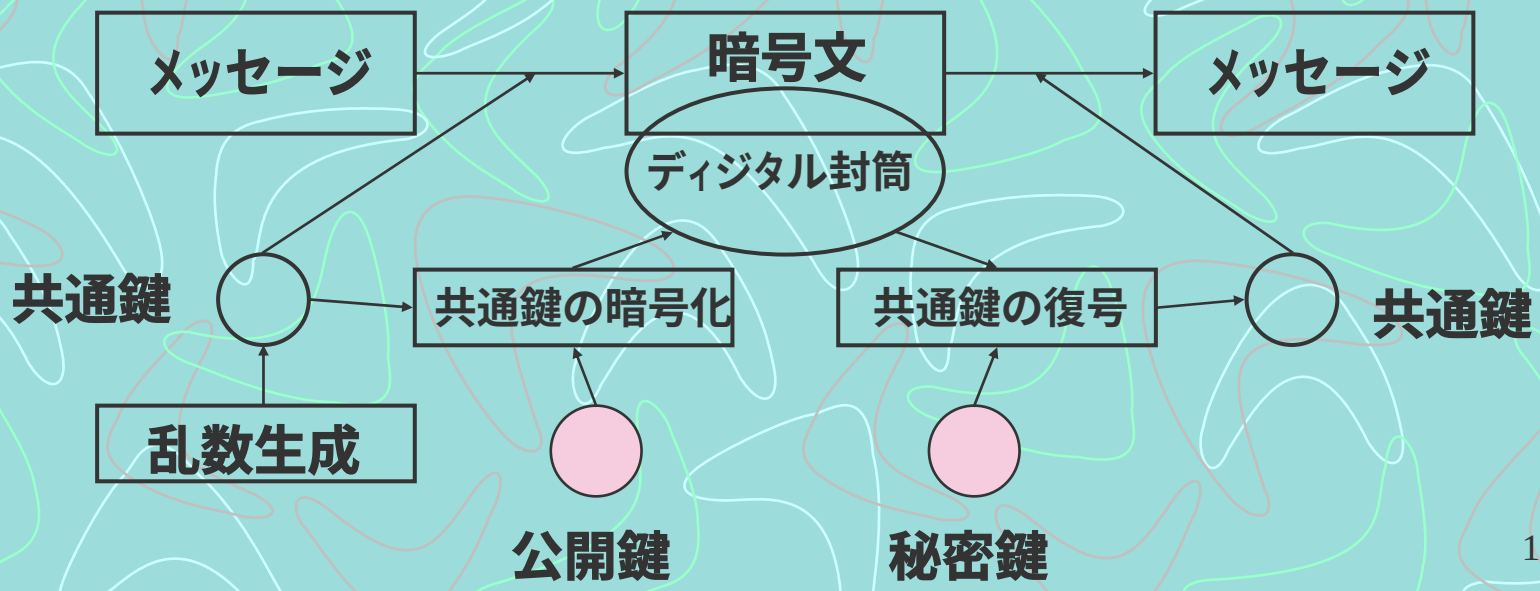
- 総当たり法でないと解読できない
- コンピュータの性能が高くなるに従い、より長い鍵が利用できるようになる
- アルゴリズムが公表されているので、安全性が広く検証されている

- RSAの安全な期間

512ビット　　・・・3ヶ月
1024ビット　　・・・3年
2048ビット　　・・・20年

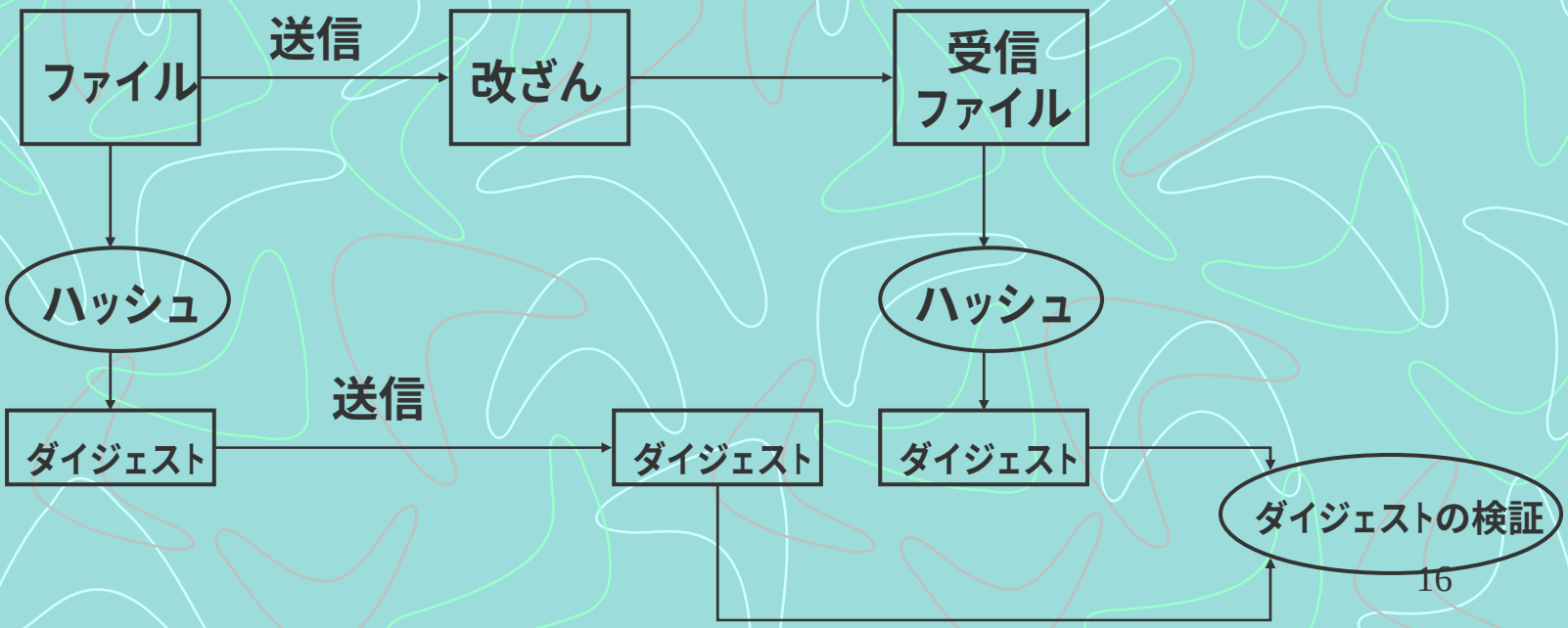
ディジタル封筒

- 公開鍵暗号は共通鍵暗号に比べて10倍～100倍の時間がかかる
- メッセージを共通鍵で暗号化し、共通鍵を公開鍵で暗号化する方法



メッセージダイジェスト

- メッセージの改ざんや転送エラーを検知する仕組み
- ハッシュ関数を利用して固定長のビット列に変換
- SHA-1、MD5といったアルゴリズムがある

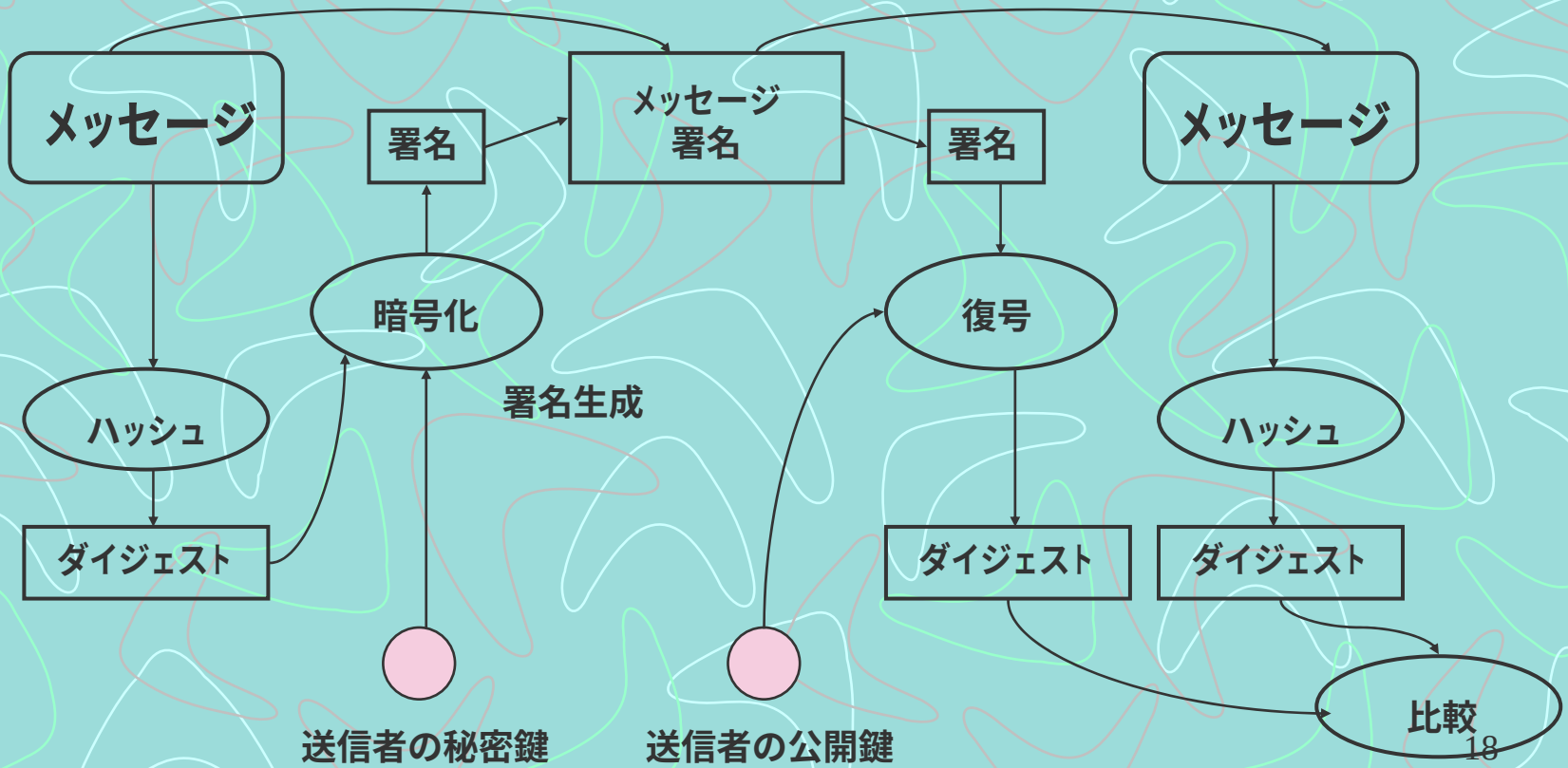


メッセージダイジェストの応用例

- ファイル転送での改ざんや転送エラー検知
- サーバ上のファイルの改ざん検知
- ディジタル証明書の偽造検知
- パスワードのチェック
- メッセージの改ざんチェック
- ワンタイムパスワード
- 電子公証
- 共通鍵生成
- 乱数の種生成

ディジタル署名

- メッセージの改ざんをチェックする仕組み



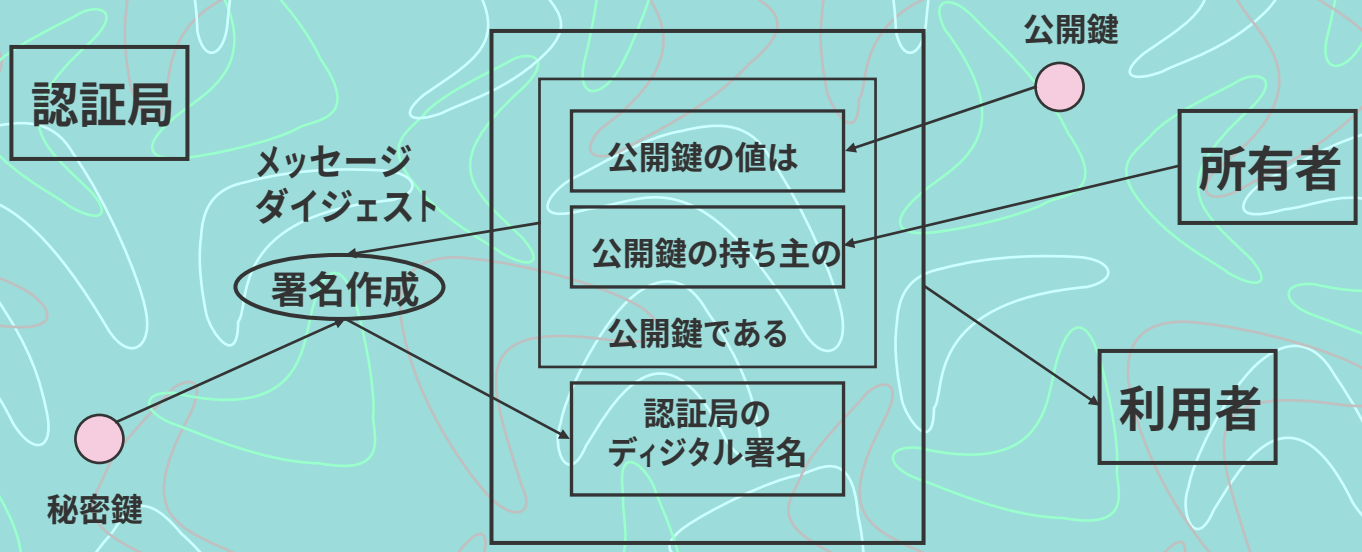
ディジタル署名の法的な有効性

- UNISITRAL(国連国際商取引委員会)により国際的取り決めに関する案が出されている。

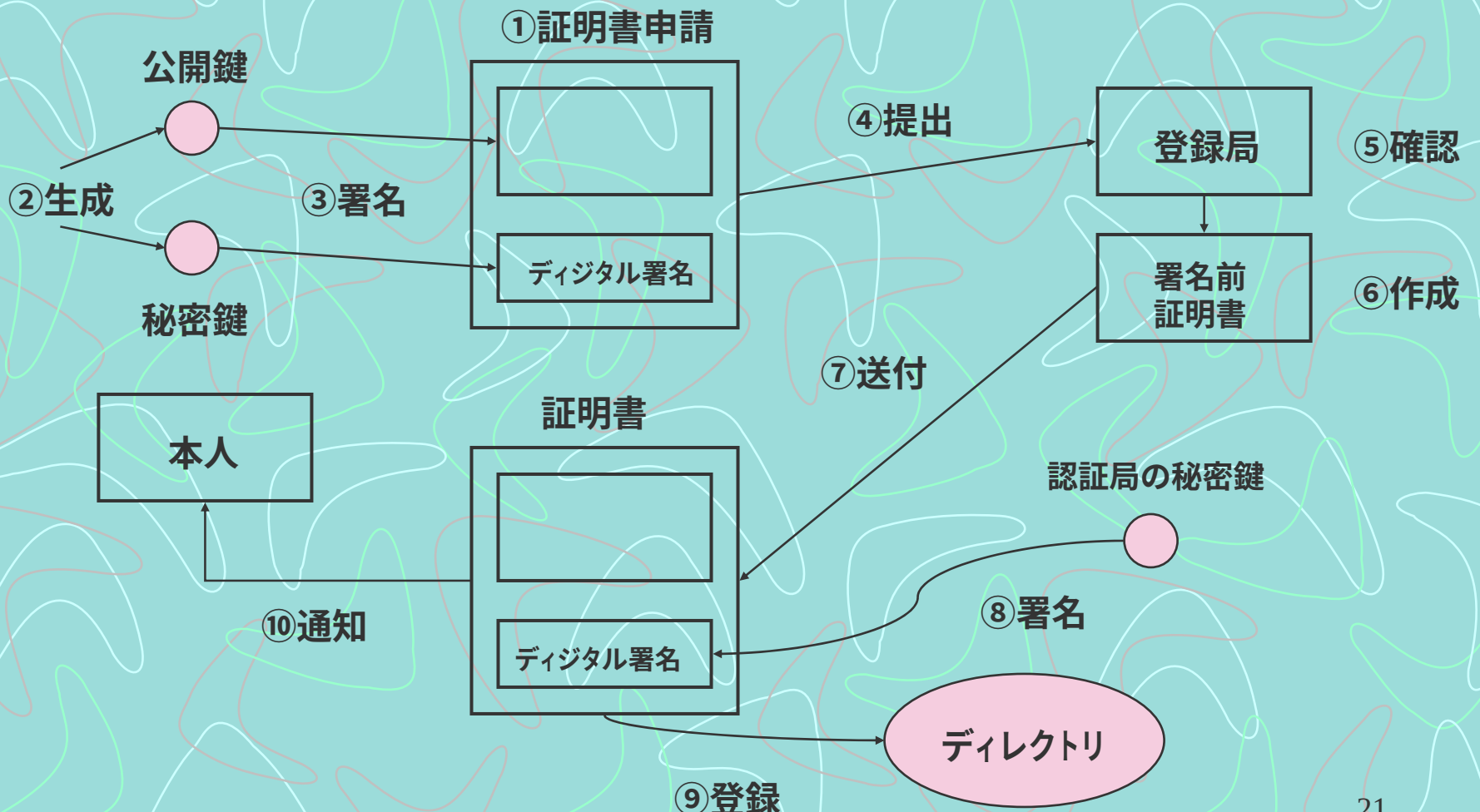
- 日本では、電子署名法が施行されている。

ディジタル証明書

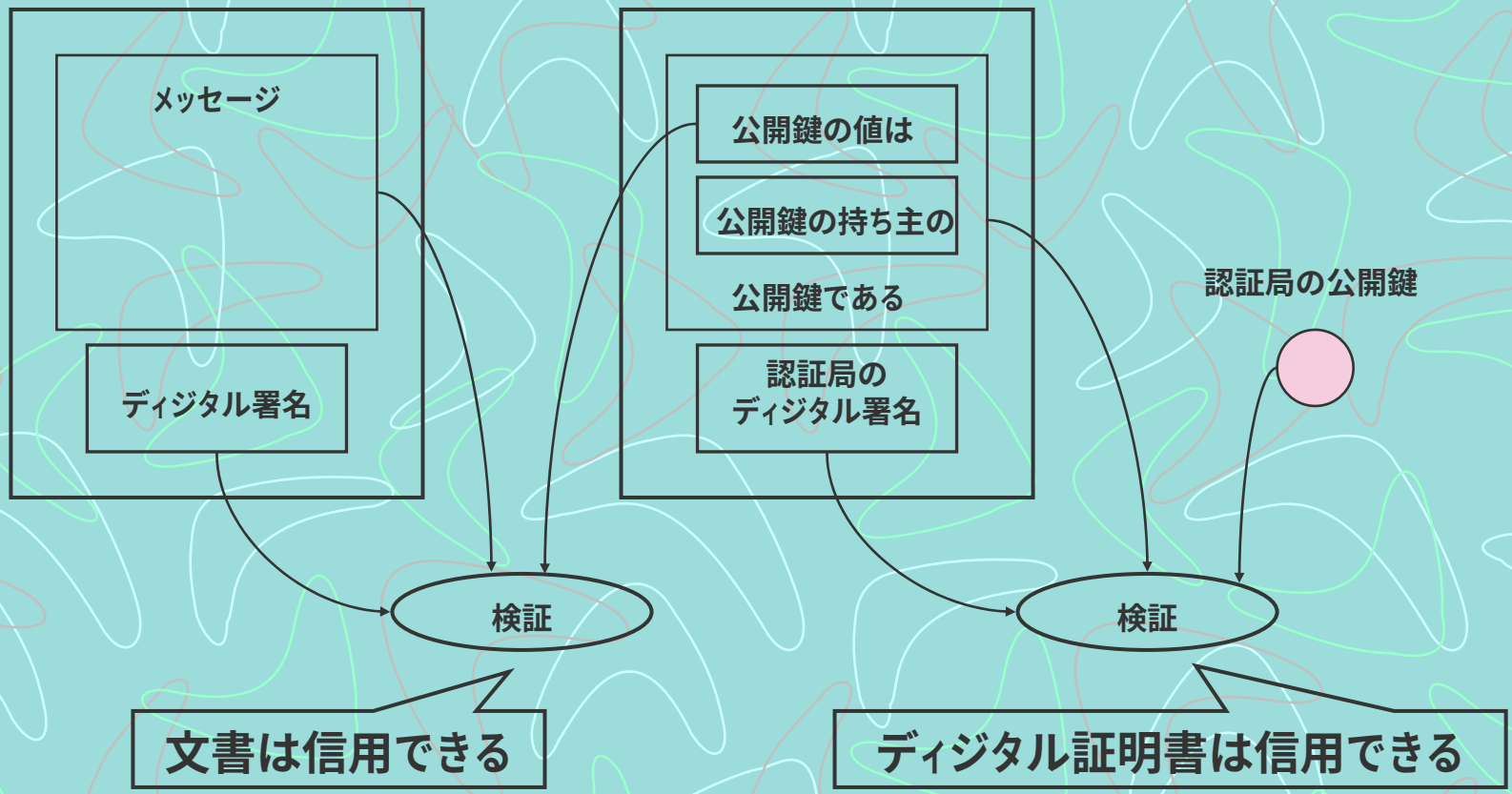
- 公開鍵の所有者を証明する文書
- オンラインでディレクトリや認証サーバに公開鍵の検索をする回数が減らす事(トラフィックの低減)が本来の目的



ディジタル証明書の発行



ディジタル証明書の検証



認証局証明書

- 認証局自身に対するディジタル署名

- 上位の認証局に証明して貰う
- 自分で証明する

方法がある

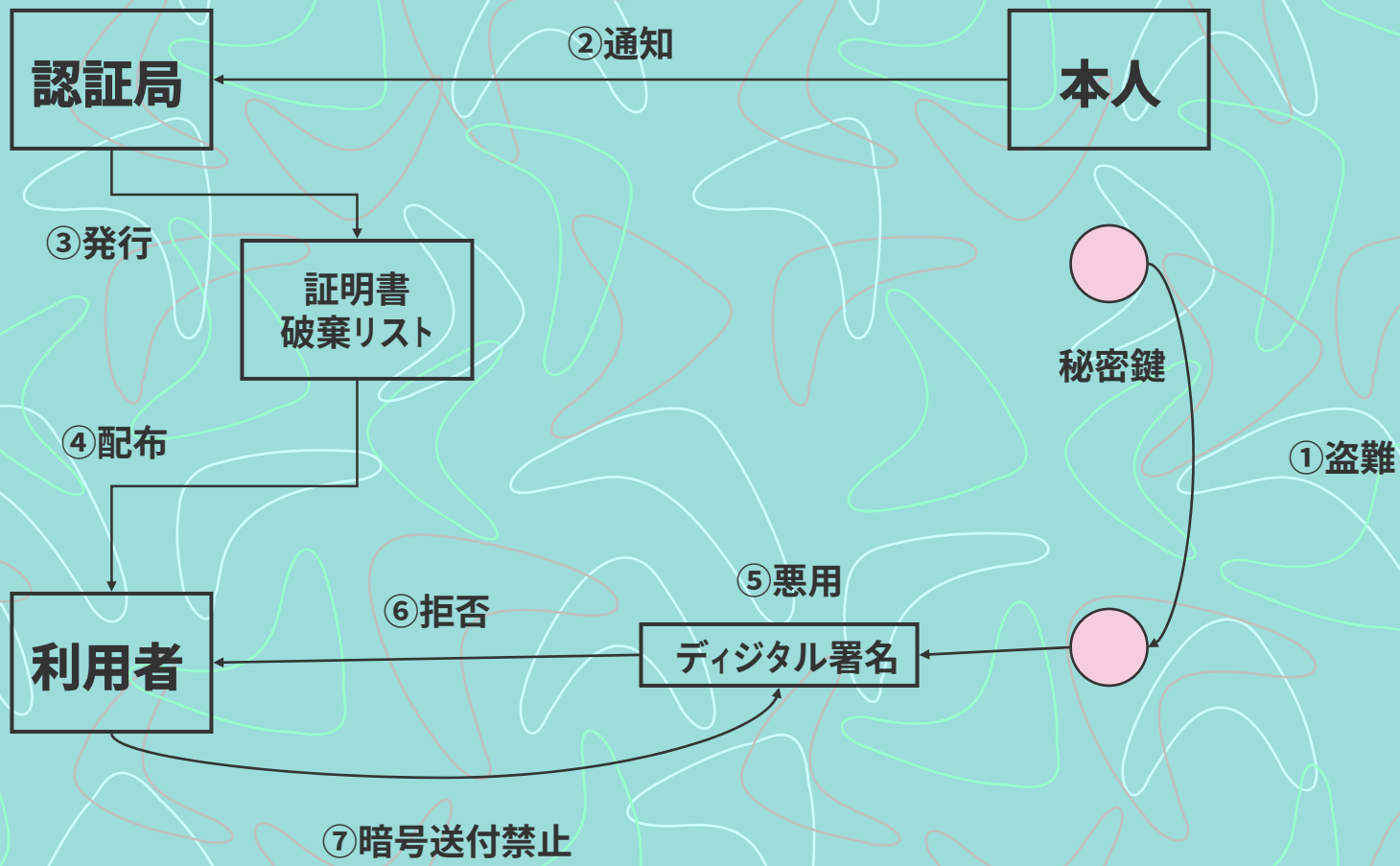
デジタル証明書の破棄

- 秘密鍵の紛失、漏洩
- 名前の変更

- 認証局を利用している組織からの脱退
- PKIシステムを利用する資格を失った
- 組織から不適格と見なされた

これらの場合、証明書を破棄しなければならない

証明書破棄リストの動き



PKIの利用方法

分野	PKIの機能
暗号通信	SSL (Secure Sockets Layer) TLS (Transport Layer Security) SET (Secure Electronic Transaction) SECE (Secure Electronic Commerce Environment) IPsec (IP security) WAP SSH
暗号メールと ディジタル署名	S/MIME (Secure Multiple Internet Mail Extensions)
データの暗号化と ディジタル署名	Code Signing XML Signature PKCS #7とCMS
暗号インタフェース	PKCS #11 Microsoft Crypto API GSS, GSS-IDUP
タイムスタンプ	Time Stamp Protocol (TSP)

PKIの利点

- 認証の際に秘密情報を送る必要がない
- サーバで秘密情報を管理する必要がない
- ユーザが秘密情報を忘れる心配がない
- 秘密情報が解読しにくい
- 相手に秘密を教えずにデータを暗号化して送ってもらえる
- ディジタル署名の検証やユーザの認証が行える
- 不特定多数から暗号データを送ってもらえる

PKIの誤解されやすい点

- ディジタル署名を秘密にする必要がある訳ではない
- 認証局はオンラインで認証する訳ではない
- コンピュータが高速になると暗号は解読されやすくなる訳ではない
- ユーザの識別と認証は違う