# 公開鍵認証基盤（ＰＫＩ）の仕組み

## PKI （Public Key Infrastructure：公開鍵認証基盤）

－PKIとは、公開鍵暗号方式に基づく電子認証の技術基盤
－具体的には、秘密鍵による暗号化（電子署名）、公開鍵による復号化、公開鍵の電子証明書を組み合わせ本人性の確認や文書の改ざんの有無の検知を行うもの
－公開鍵の電子証明書の有効性を証明する第三者機関が認証局（CA）

### 公開鍵暗号方式

公開鍵暗号方式とは、公開鍵・秘密鍵を用いた暗号技術。

公開鍵・秘密鍵とは、暗号化・復号化のアルゴリズム（処理手順）のこと。

二つの鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号化できない。

片方の鍵からもう一方の鍵を割り出すことは事実上不可能（公開鍵を公開しても秘密鍵を複製されるおそれがない。）