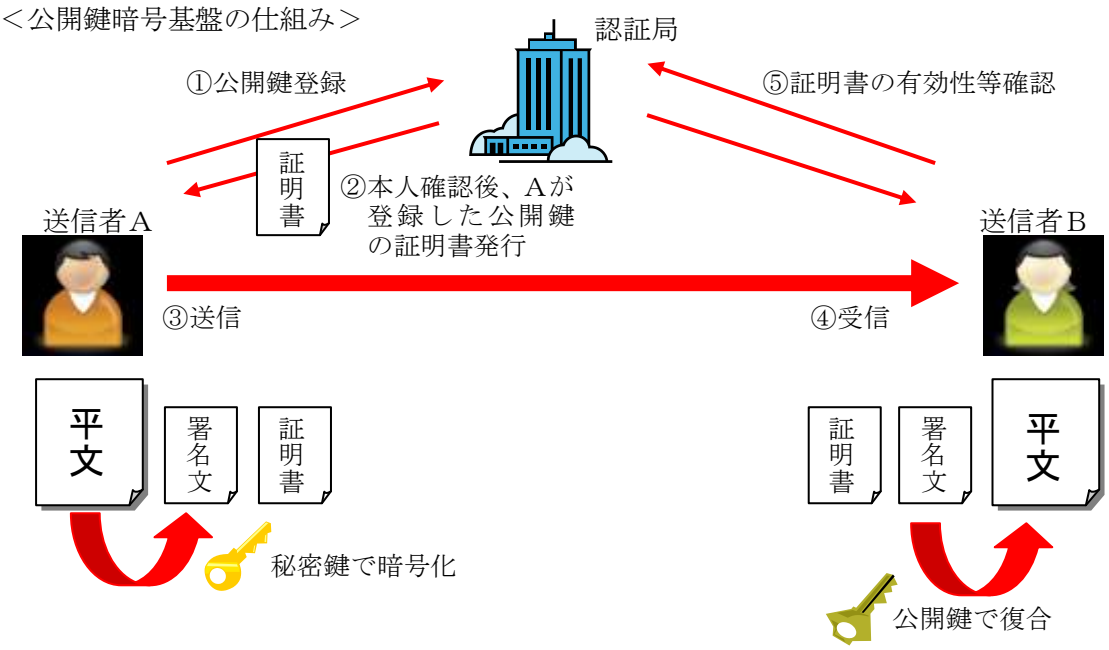
ＷＥＢ－ＦＢ電子証明書方式の認証の仕組みについて

電子認証とは、「電子署名」と「公開鍵証明書（電子証明書）」を用いて、インターネット上で本人認証を実現する技術です。

この電子認証の中核となるのは「秘密鍵」と「公開鍵」と呼ばれる一対の電子的な鍵を用いる暗号化技術です。これは、一方の鍵で暗号化したデータはもう一方の鍵でしか解読できないというものです。（公開鍵暗号基盤（ＰＫＩ））

＜公開鍵暗号基盤の仕組み＞



＊　公開鍵暗号基盤

公開鍵と秘密鍵の対になる２つの鍵を使ってデータの暗号化／復号化を行う暗号方式です。

公開鍵暗号方式では、“暗号文を作り出す鍵”と“暗号文を元に戻す鍵”が異なります。暗号通信をしたい人は、まず独自に２つの鍵のペアを作成します。１つは暗号文を作り出す鍵で公開鍵と呼ばれ、通信相手に知らせる鍵としてインターネット上でもやりとりできます。だれでもこの公開鍵で暗号文を作成でき、鍵を公開している人に送ることができます。暗号文の受け手は、公開鍵とペアになっている、本人だけが分かるように厳重に管理された秘密鍵で復号します。

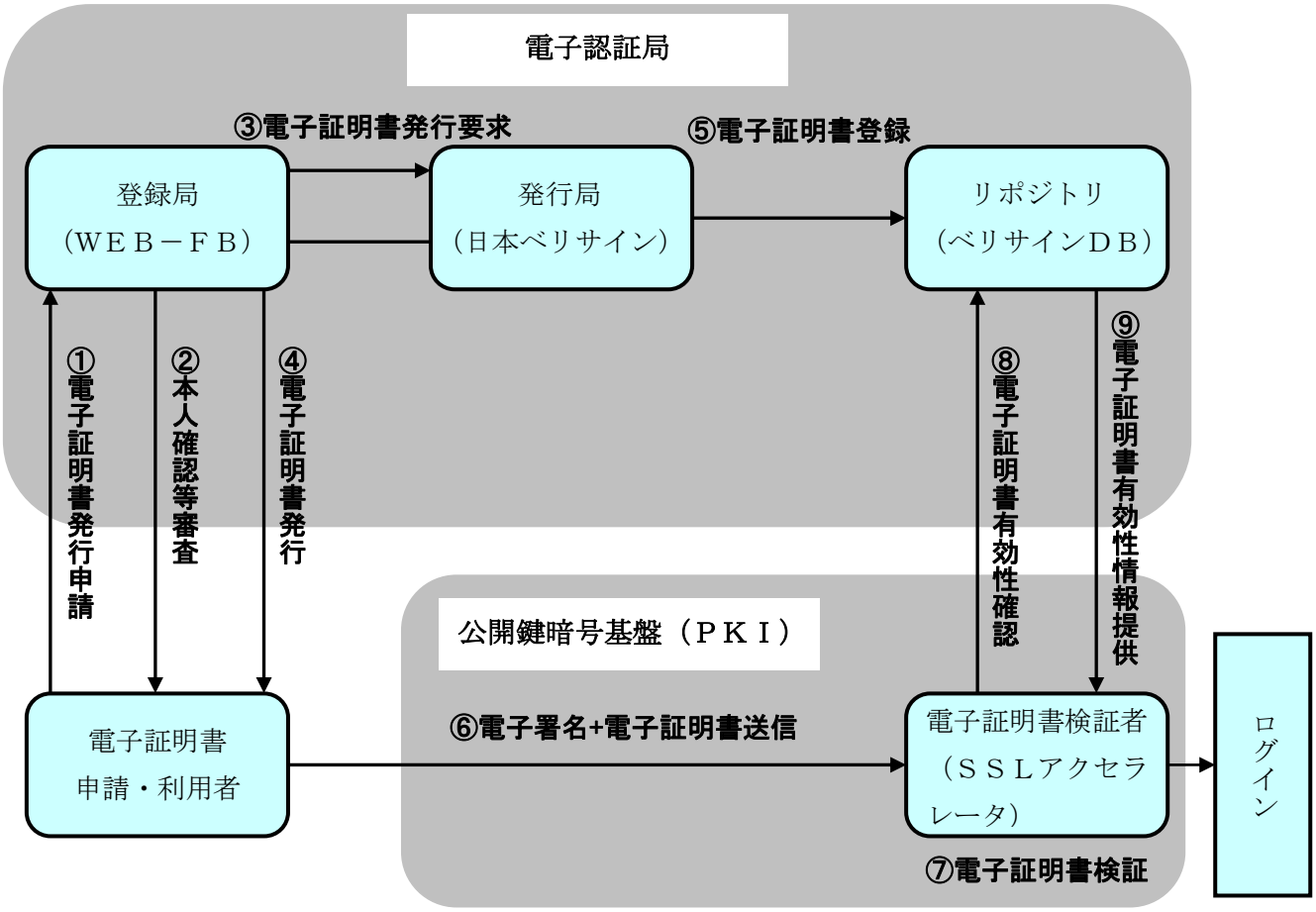
暗号化と復号化を同じ鍵で行う共通鍵暗号方式に比べ、公開鍵の共有が容易なことや、相手の数に関係なく公開鍵は１つでよいなど、鍵の管理が容易で安全性が高くなります。

公開鍵暗号方式を用いれば、デジタル署名を容易に実現でき、送信者が通信の事実を後で否認したり、他人が偽造することを不可能にするデータ転送が可能になります。

電子認証に使用する電子証明書は、電子認証局（Certification Authority）と呼ばれる認証機関が発行します。電子認証局は、電子証明書の発行申請者の本人確認と登録管理を行う登録局（Registration Authority）、登録局の指示にもとづき電子証明書の発行や失効などの処理を行う発行局（Issuing Authority）、ならびに電子認証局に関する情報や電子証明書の有効性に関する情報を提供するリポジトリ（Repository）から構成されています。

利用者は、申請を行う際、申請書を「秘密鍵」で暗号化し、「電子証明書」を添付してＷＥＢ－ＦＢシステム側に送信します。この「秘密鍵で暗号化すること」を「電子署名」と呼んでいます。これを受信したＷＥＢ－ＦＢシステムでは、まず、認証局に照会して、その「電子証明書」が有効であるかどうかを確認します。そしてそれが有効であることが確認されれば「電子証明書」に添付されている利用者の「公開鍵」で、暗号化された申請書を解読して受け付け、ＷＥＢ－ＦＢへのログインを許可します。

＜電子認証の仕組みイメージ＞



以　上

興産信用金庫