

# 公開鍵セキュリティ設定による PDFの配布について

2007/9/20



## 公開鍵セキュリティ設定

- PDFの標準仕様で公開鍵によるセキュリティ設定ができます。
  - Aさんの公開鍵でセキュリティ設定したPDFは、Aさんの秘密鍵でのみ開けます。
  - これを利用することで、特定の秘密鍵ペアを所有している人しか開けないPDFを配布することができます。
- Adobe Readerで標準サポートの仕組みです。

## メリット

- 公開鍵暗号方式は標準技術です。
- 秘密鍵ペアの証明書(個人用証明書)がWindows証明書ストアにあればAdobe Readerはそれを認識します。パスワードを入力するような手間が不要です。
- 秘密鍵をWindows証明書ストアにインポートする際に、Export不可とし、秘密鍵を複製不可にできます。

## システム

- 次の機能をもつ製品(ソリューション)を作る必要があります。
  - 公開鍵・秘密鍵ペアを作成し、受け渡す仕組み
  - 各鍵のユーザを管理する仕組み
  - 指定したユーザ向けにセキュリティを設定したPDFを作成する仕組み
- システムのコンポーネントとして
  - 「PDF電子署名モジュールV1.0」を使います。
  - PDFの受領者は「Adobe Reader」のみでOK。