

# AIR アプリケーションの 安全性と配布について

taiga & arkw

# AIR ファイルの書き出し方



# AIR ファイルの書き出し方

AIR アプリケーションとインストーラの設定

アプリケーション設定

\*ファイル名: AIR\_SAMPLE

名前: HTML AIR2 API Sample

\* ID: AIRSAMPLE \*バージョン: 1

\*イニシャルコンテンツ: sample.html

説明:

著作権: taiga.jp

ウィンドウスタイル: システムクローム

ウィンドウサイズ: 幅: 800 高さ: 600

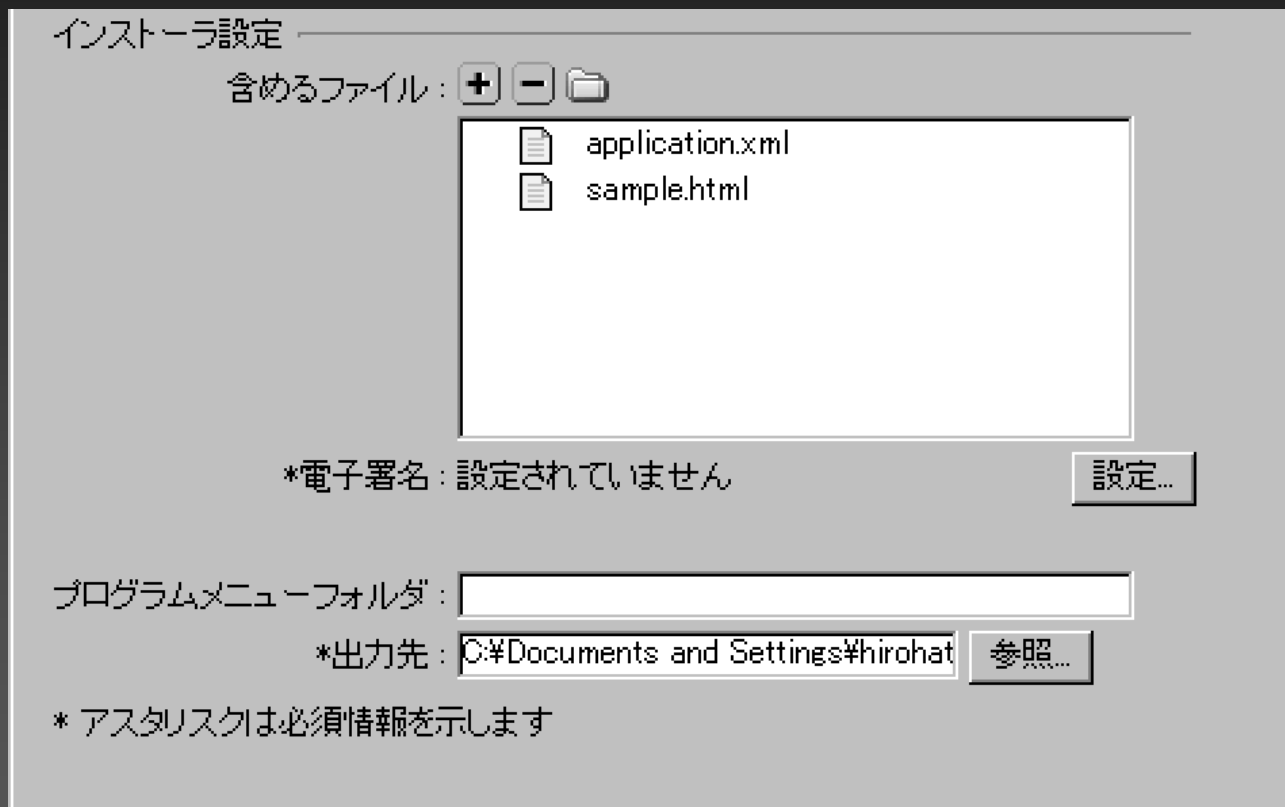
アイコン:

関連付けるファイルタイプ:

アプリケーションの更新:  AIR アプリケーションのインストーラが処理する



# AIR ファイルの書き出し方





# AIR ファイルの書き出し方

アプリケーションとインストーラーの設定

一般 | 署名 | アイコン | 詳細

出力ファイル:

Windows インストーラー (exe)

ファイル名:

アプリケーション名:  バージョン:

アプリケーション ID:   
例: com.yourdomain.appname

説明:

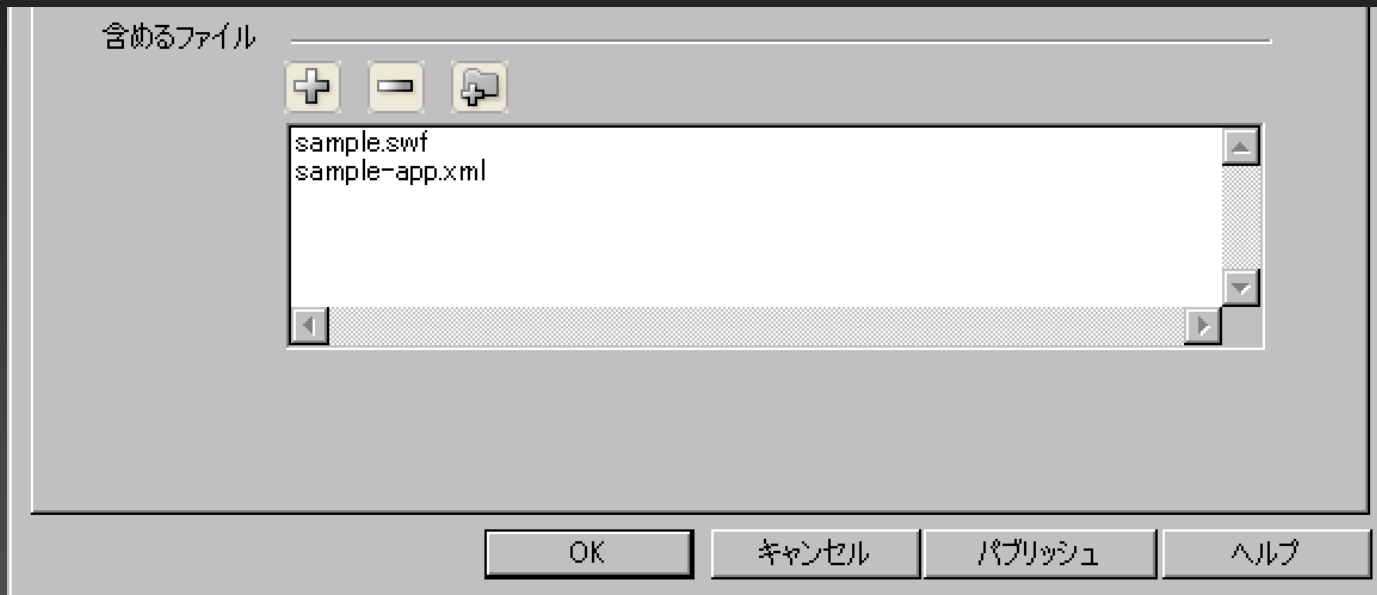
著作権:

ウィンドウスタイル:

プロフィール:  デスクトップ  モバイルデバイス  
 拡張デスクトップ  拡張モバイルデバイス

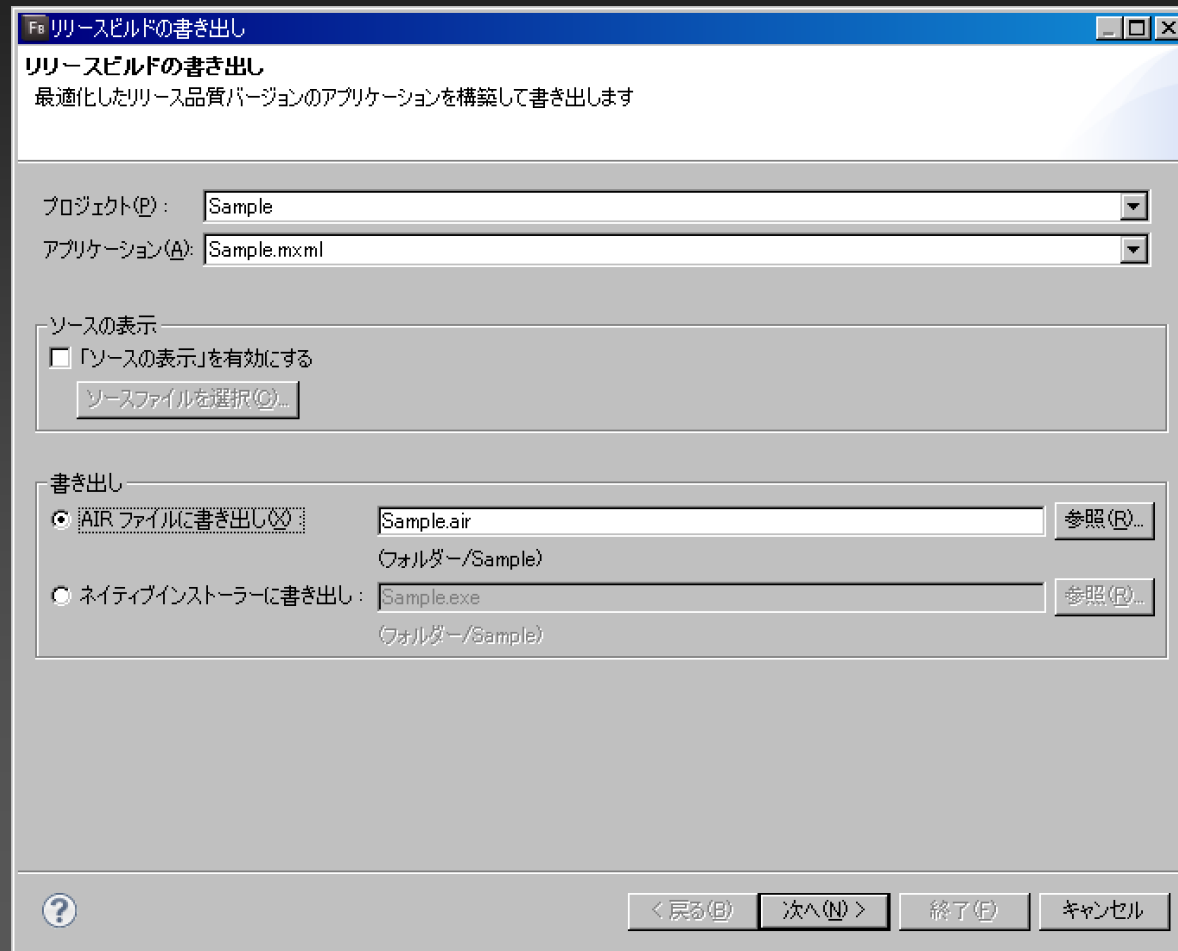


# AIR ファイルの書き出し方





# AIR ファイルの書き出し方



# 電子署名

- 認定されている証明機関 (CA) が発行した証明書を使用する
- 国内の場合、グローバルサイン株式会社にて取得可能



# 証明書の重要性

- パッケージ後に内容が改竄 / 改変されていないことの確認
- パッケージ作成者 / 組織を確認する

# AIRI (AIR Intermediate)

- 署名を行わない中間ファイル

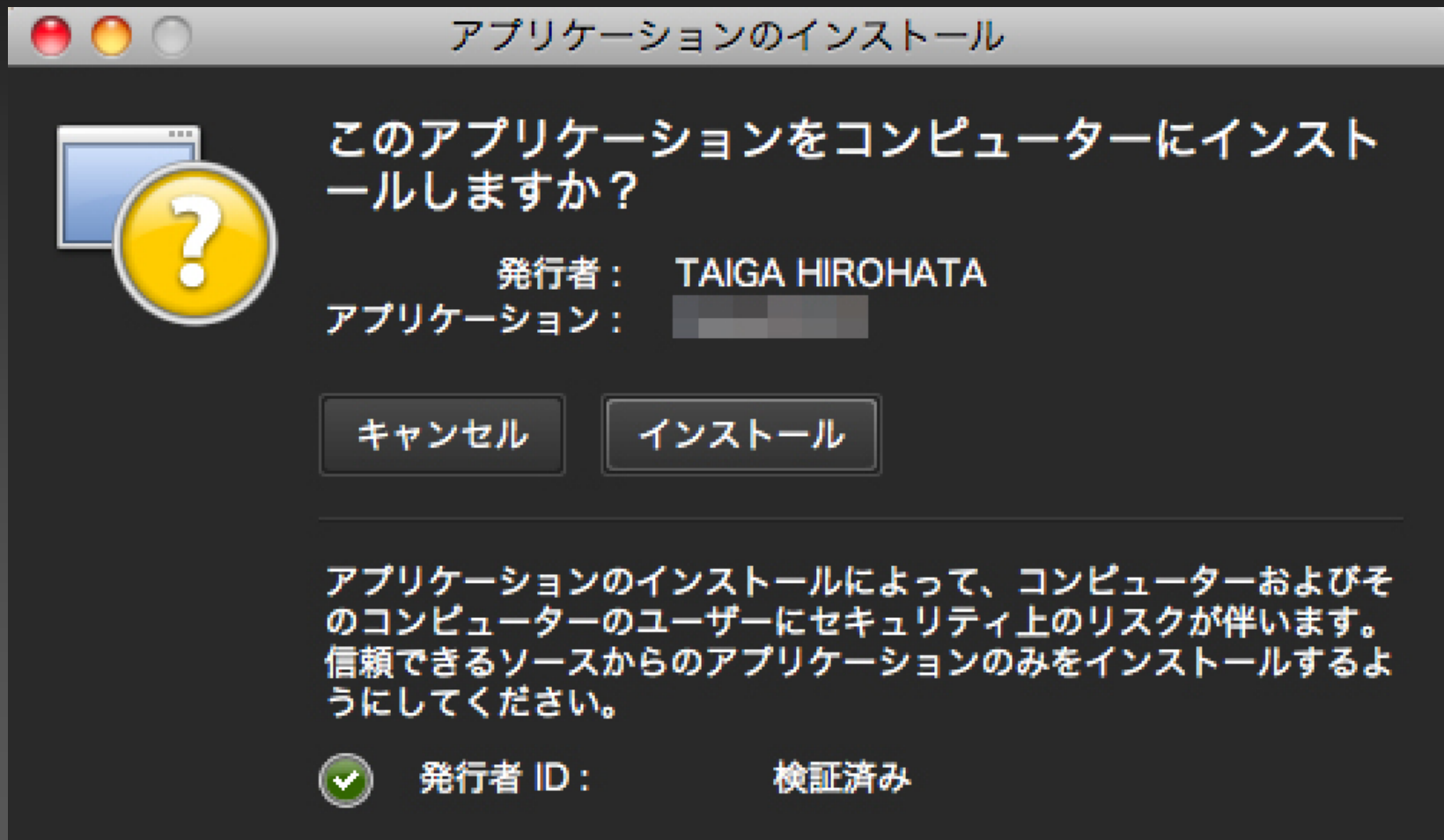
- ADT で後から署名できる

```
adt -package -storetype pkcs12 -keystore  
*****.p12 -storepass *****) app_name  
airi_name
```

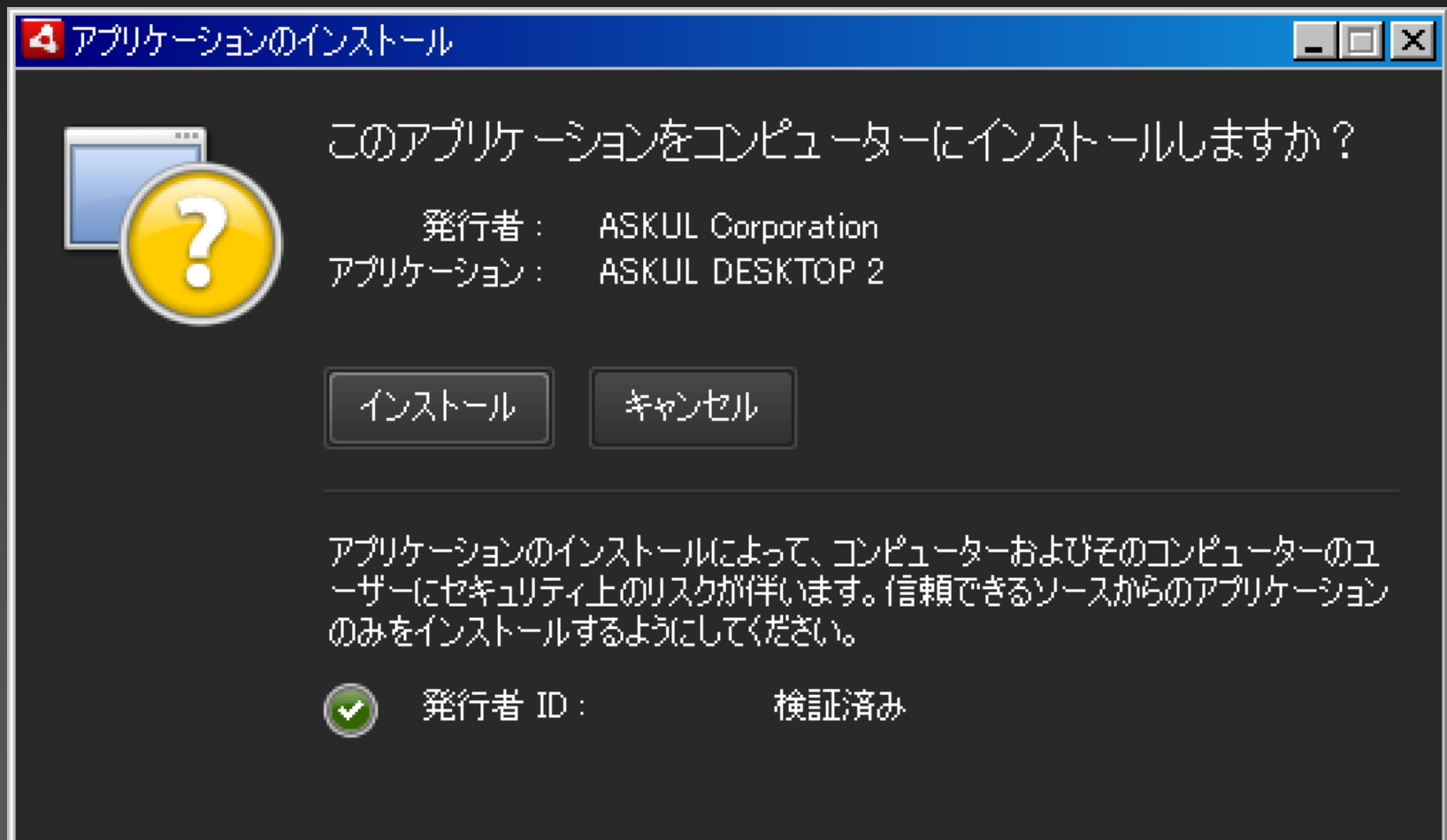
# 証明書（オレオレ）



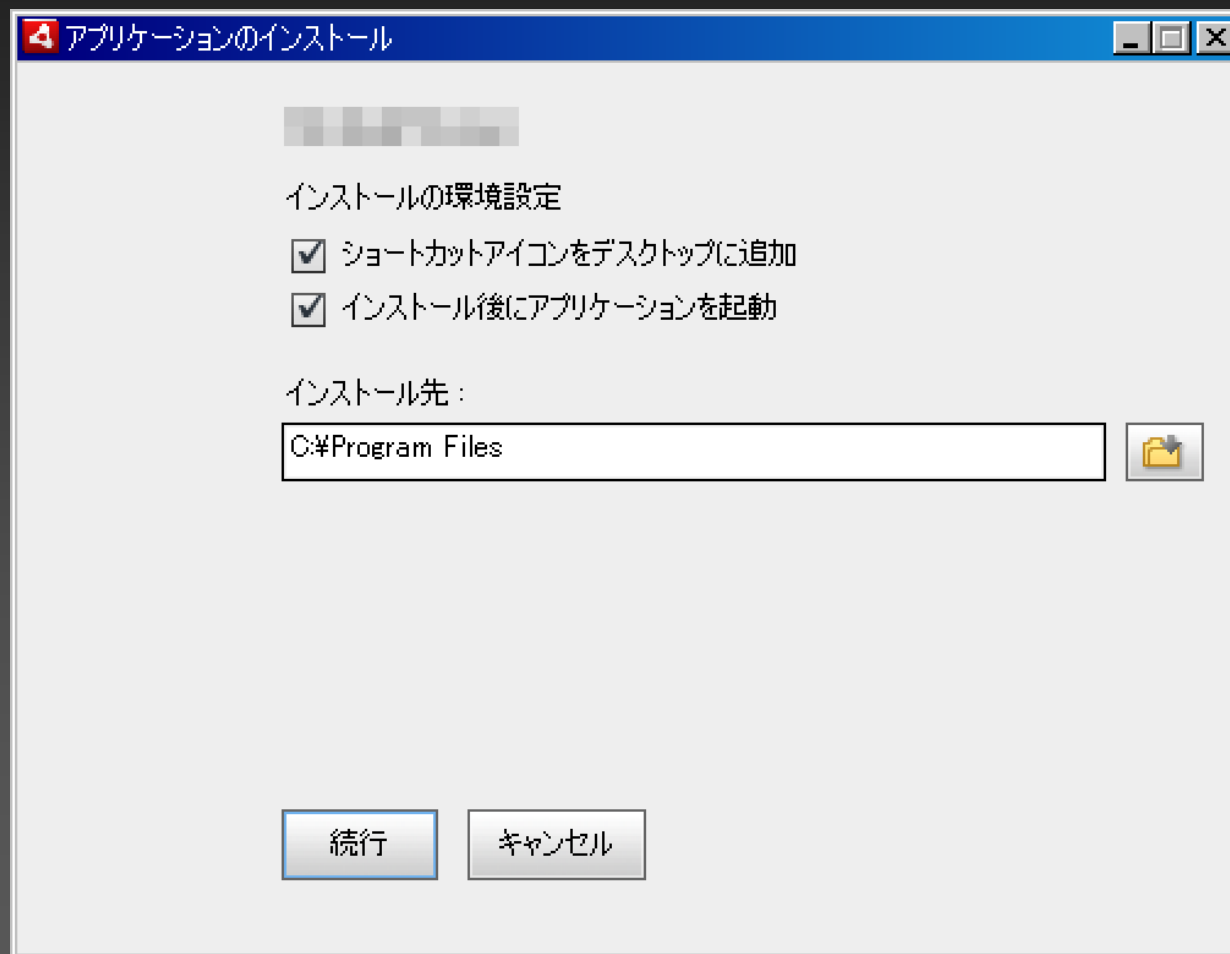
# 証明書（個人）



# 証明書（法人）



# ネイティブインストーラ



# 悪意ある AIR アプリ

- 悪意ある攻撃者が作りそうなアプリデモ



# 起こりうるリスク

- ミラーサイトの的なところから配布されている悪意ある AIR アプリ
- AIR ファイルを偽造
  - なんらかの方法で署名されているキーストアファイルを取得
  - 秘密キーを見つけ出し、署名者の ID で偽装



# 証明書のアップデート

- 組織名、個人名が変更されない限り、更新された証明書を適用

# 証明書の変更

- オレオレ証明書を CA から発行された証明書にアップグレード
- 有効期限が近いオレオレから新しいオレオレ
- ある商用証明書を別の商用証明書に変  
( 企業の ID が変更された場合など )

# 証明書の変更（方法）

- ADT の `-migrate` コマンドを使用
- 例  

```
adt -migrate -storetype pkcs12  
-keystore cert.p12 myApp.air myApp.air
```

# まとめ

- 作成者はアプリケーション配布後も責任を持ちましょう
- 使用者は配布元をしっかりと確認したうえでアプリケーションをインストールしましょう