

もっと知ろうよ。  
コード アクセス セキュリティ(CAS)

尾崎 義尚  
om(takanao)

# Who am I ?

- 尾崎 義尚 - om(takanao)
- わんくま同盟のメンバーではありません。
- Visual Studio User Group モバイル・スマートクライアント フォーラム リーダー (<http://vsug.jp/>)
- MVP for C# Oct, 2005 - Spt, 2007
- こみゅぷらす (<http://comuplus.net/>) メンバー

**COMU+**  
こみゅぷらす

## はじめに

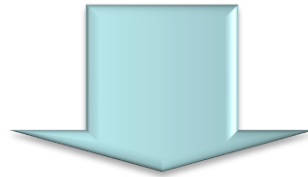
- 時間も短いですし、環境の作成が難しかったので、デモなしで突っ走りたいと思います。
- 概要ではなく、もうちょっと中の話をしていきます。

# コード アクセス セキュリティとは

- .NET Framework で採用されているセキュリティ機構

## CAS 理解度チェック！

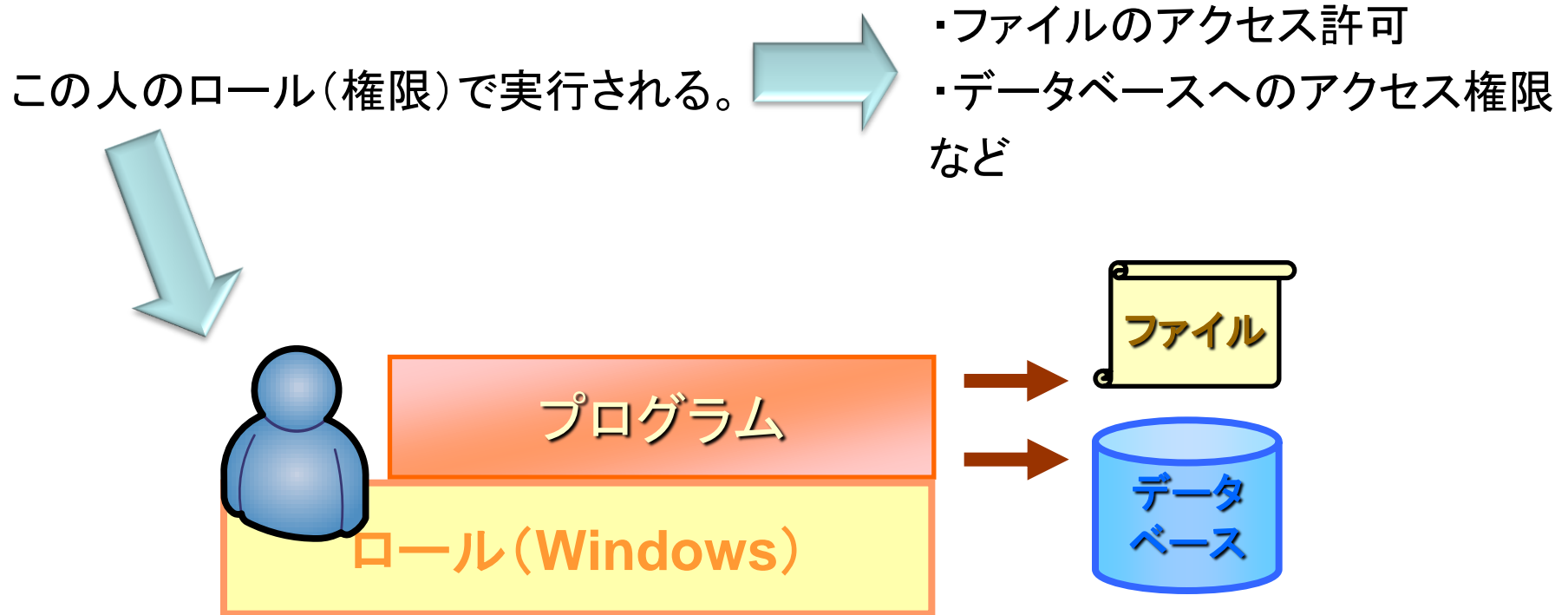
- 【Q】 Visual Studio 2005 で作成したアプリケーションをファイルサーバーにコピーして実行しました。うまく動きますか？



- 【A】 う、う～ん・・・

# .NET 以前のセキュリティ機構

- ロールベース セキュリティ



# .NETのセキュリティ機構

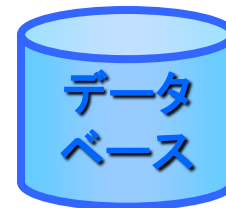
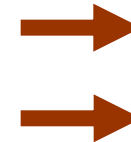
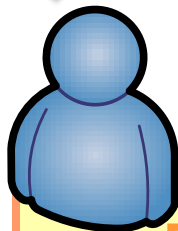
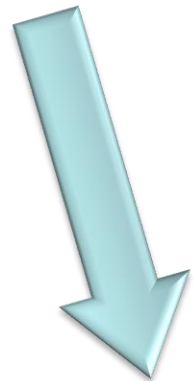
- コード アクセス セキュリティ (CAS)

この人のロール(権限)と(AND)

このアクセス許可(Permission)  
で実行される。



つまり、ロールと  
CAS のアクセス許可  
がないと処理が実行  
できない。



## アクセス許可セットが付与されるまで

- 証拠を評価して、対応するコードグループを判断、コードグループに関連づけられたアクセス許可セットが付与されます。



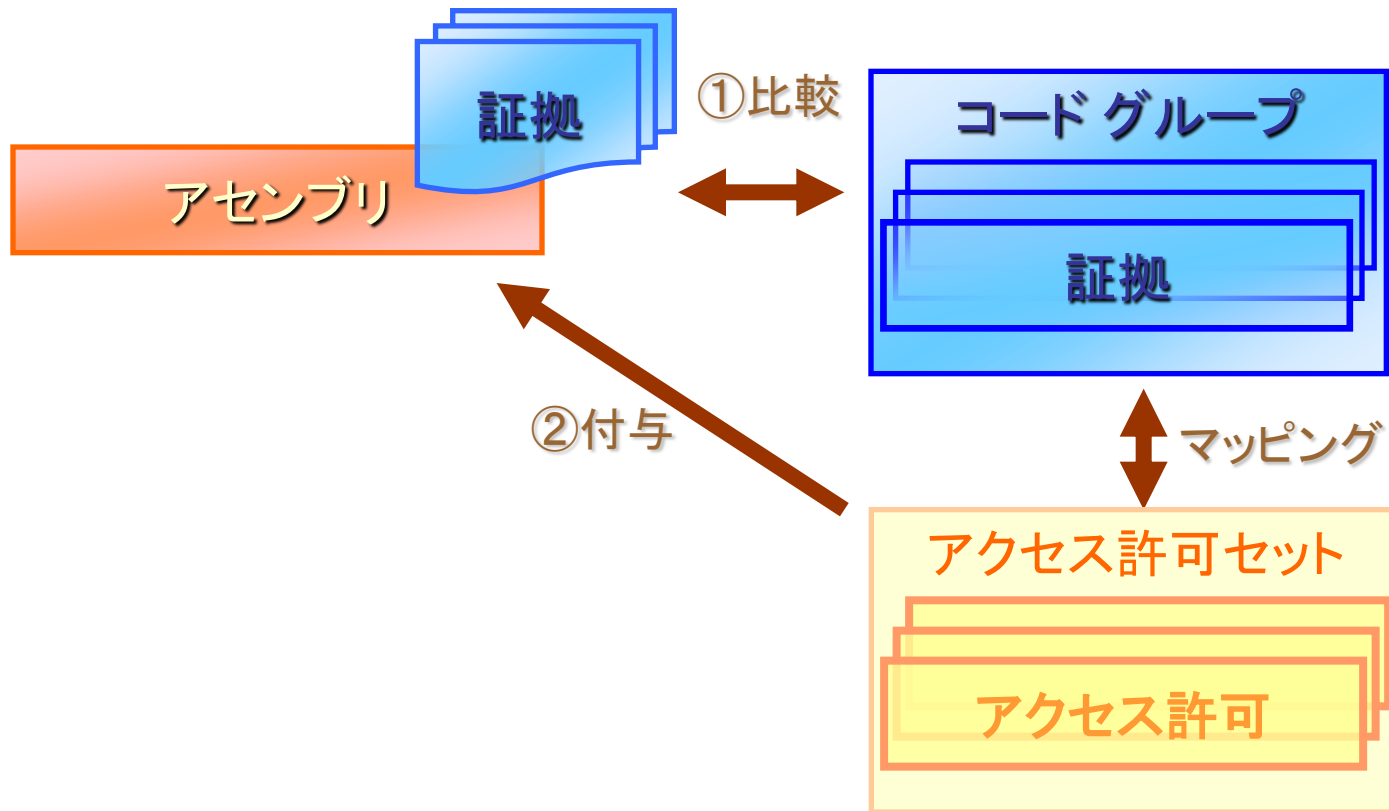
# アクセス許可セットが付与されるまで

- 証拠

コードグループ  
アクセス

アクセス許可セット

# アクセス許可セットが付与されるまで

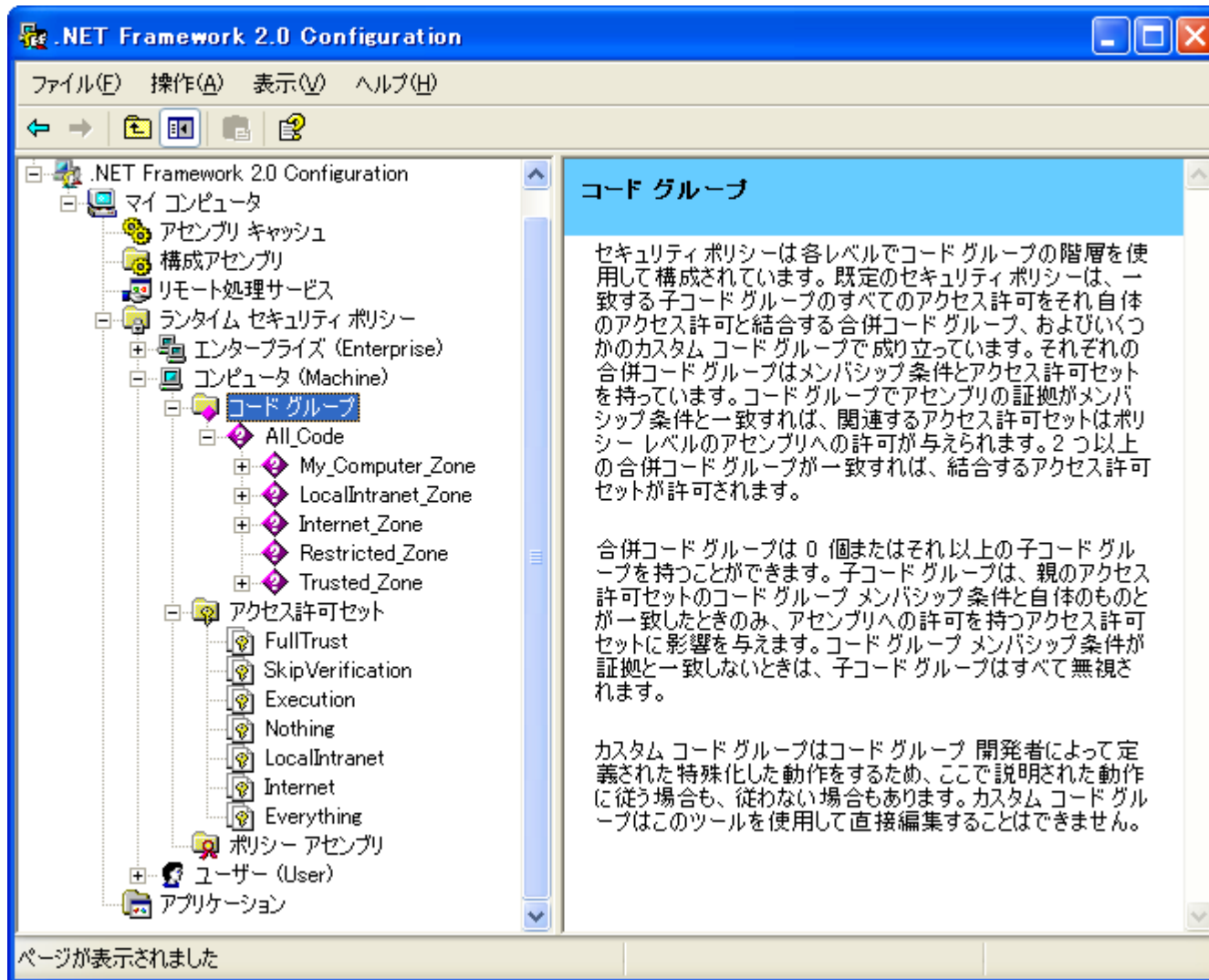


# 証拠って？

- アセンブリの身元調査資料
  - GAC
  - ハッシュ
  - 発行者
  - サイト
  - 厳密名
  - URL
  - ゾーン



# 既定で用意されているセキュリティ構成



# 既定で用意されているセキュリティ構成

コードグループ	アクセス許可セット
MyComputer_Zone	FullTrust
LocalIntranet_Zone	LocalIntranet
Internet_Zone	Internet
Restricted_Zone	Nothing
Trusted_Zone	Internet

# アクセス許可って？

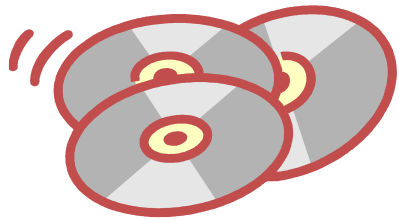


- 環境変数
- ファイルダイアログ
- ファイルIO
- 分離された記憶領域
- リフレクション
- レジストリ
- セキュリティ
- ユーザー インターフェイス
- DNS
- 印刷
- イベント ログ
- ソケット アクセス
- Web アクセス
- パフォーマンス カウンタ
- ディレクトリ サービス
- メッセージ キュー
- サービス コントローラ
- OLE DB
- SQL クライアント  
など

# アクセス許可って？

- アクセス許可は、処理実行時にチェックされる
- たとえば、
  - 「ファイルを開く」ダイアログを表示
  - 「ファイルダイアログ」アクセス許可の存在をチェック
    - 存在している場合 → 処理続行
    - 存在していない場合 → Exception が発生

# つまり



アセンブリの  
読み込み



身元調査

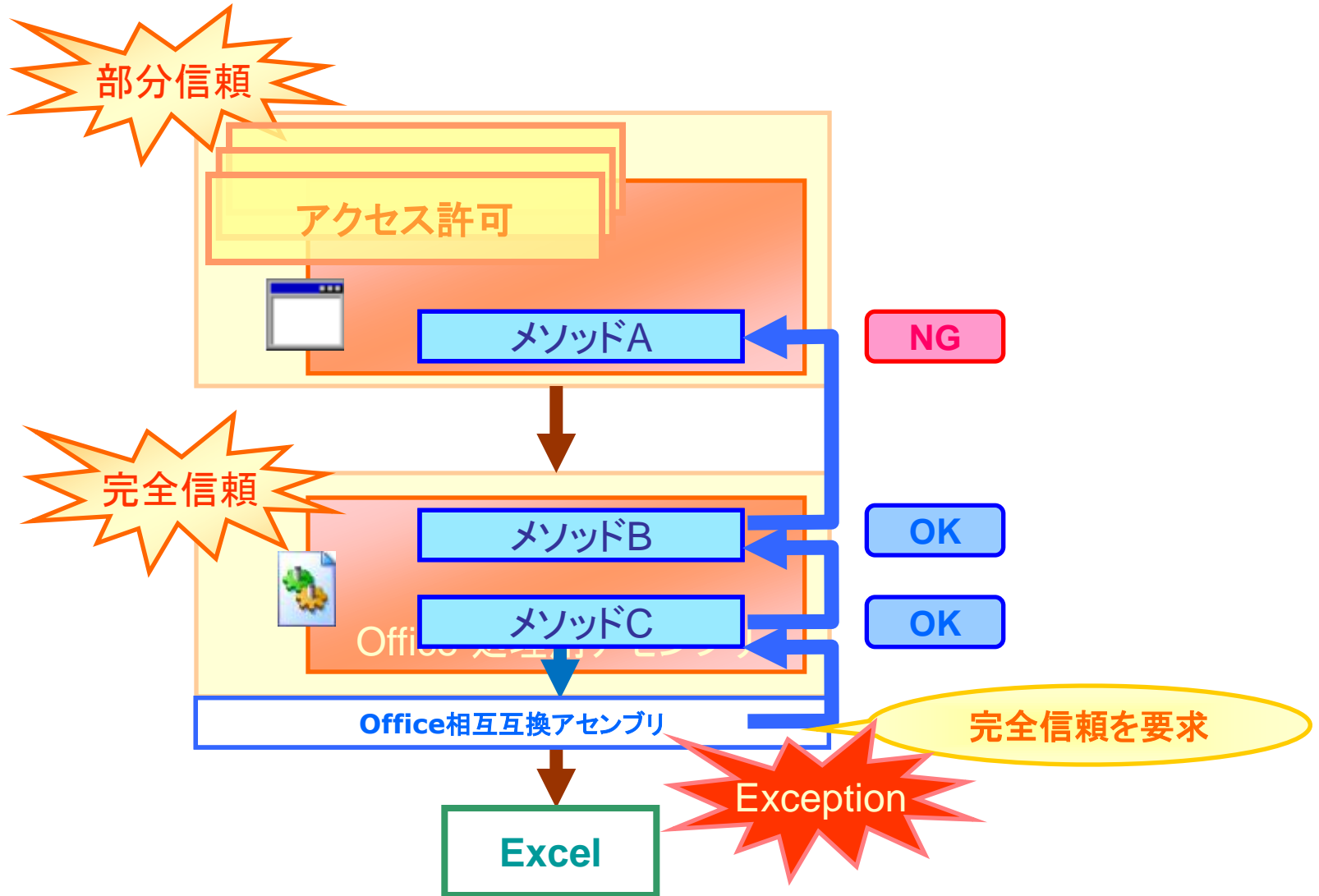


アクセス許可(権限)の  
付与

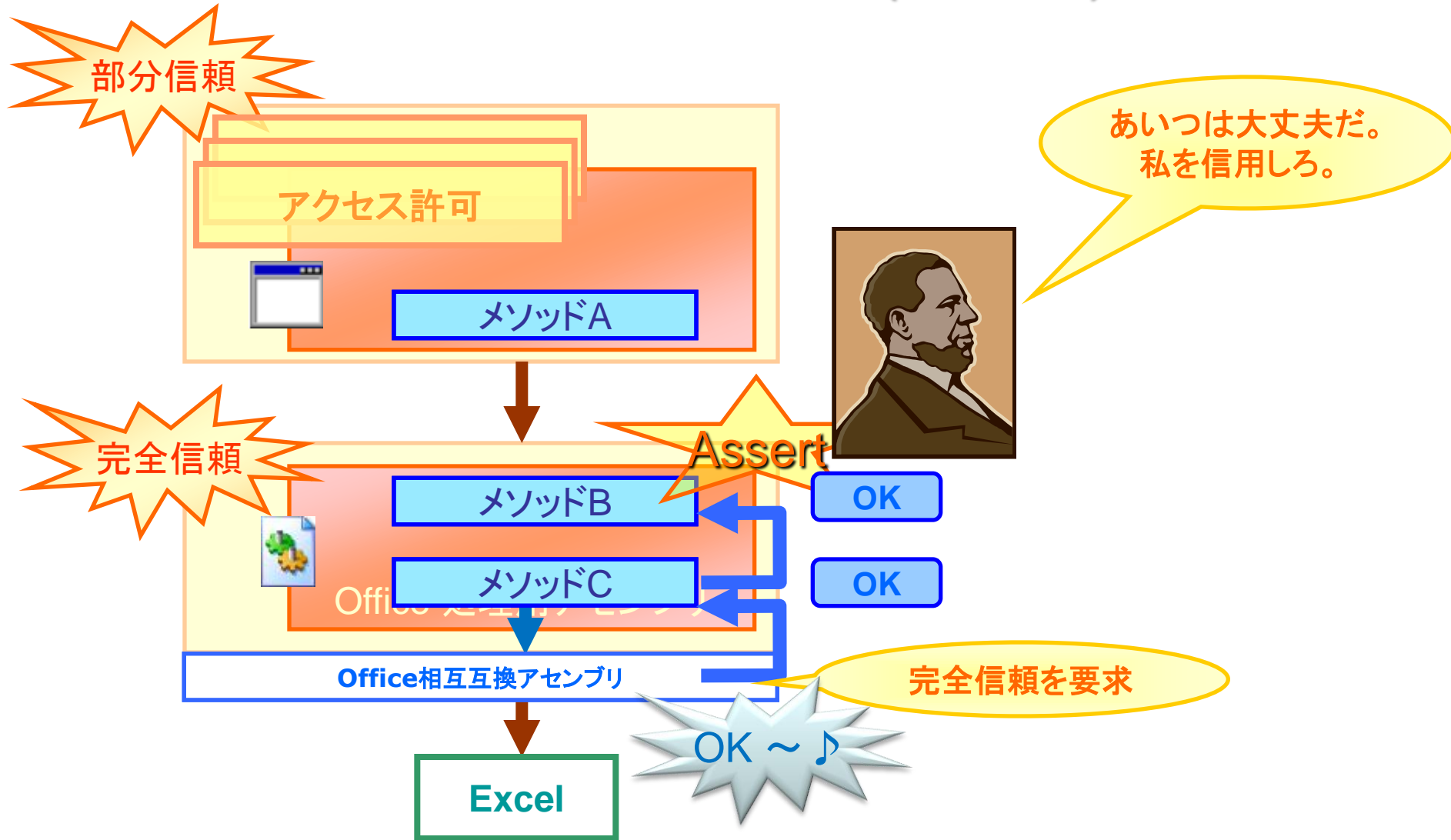
ファイル サーバーに配置したアセンブリで、LocalIntranet アクセス許可セットを超える処理をさせたい場合には、あらかじめコンピュータにセキュリティ構成を配布しておく必要がある。



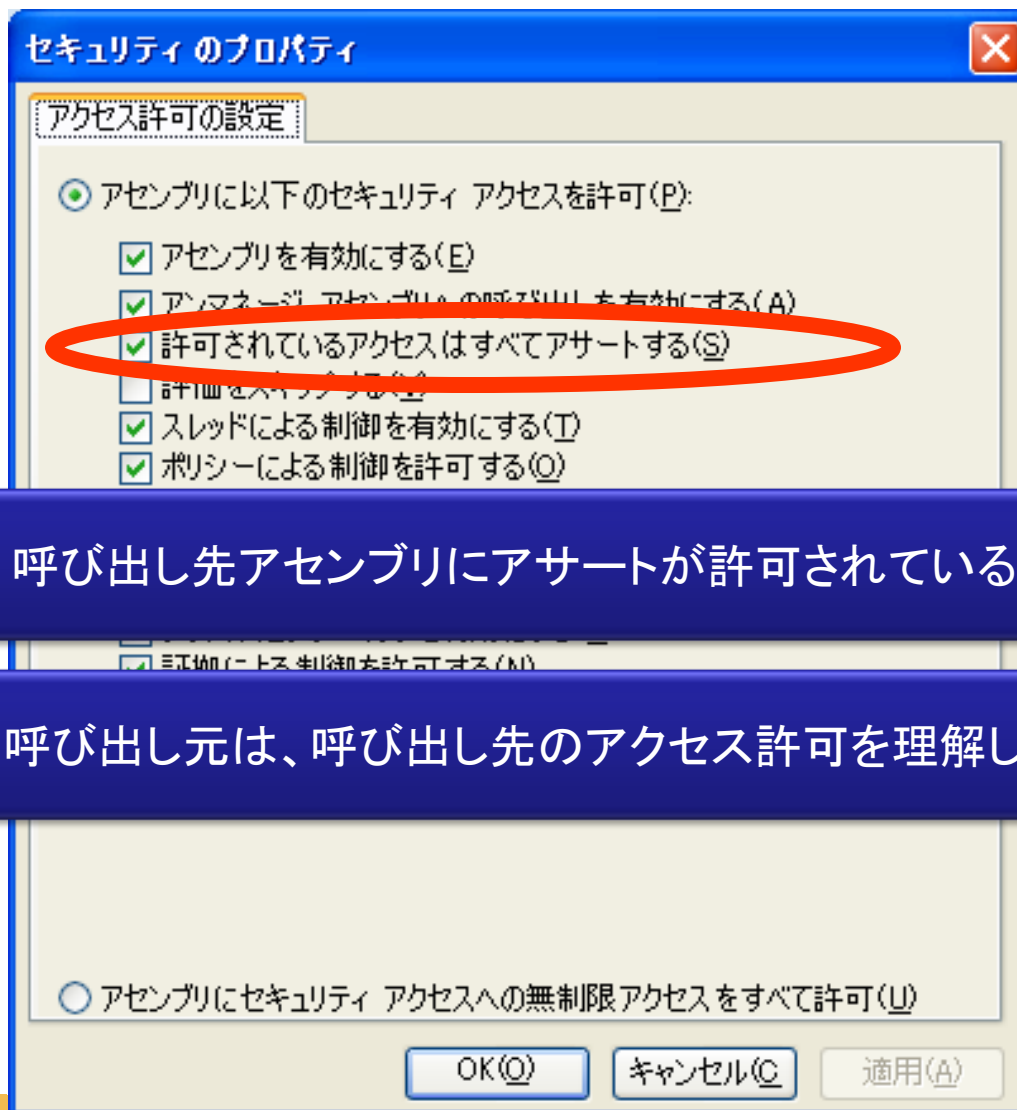
# じゃあ、こんな場合は？



# どうにかならない？ (Assert)



# どうにかならない？ (Assert)



呼び出し先アセンブリにアサートが許可されている必要がある。

呼び出し元は、呼び出し先のアクセス許可を理解して呼び出す。

# どうにかならない? (Assert)

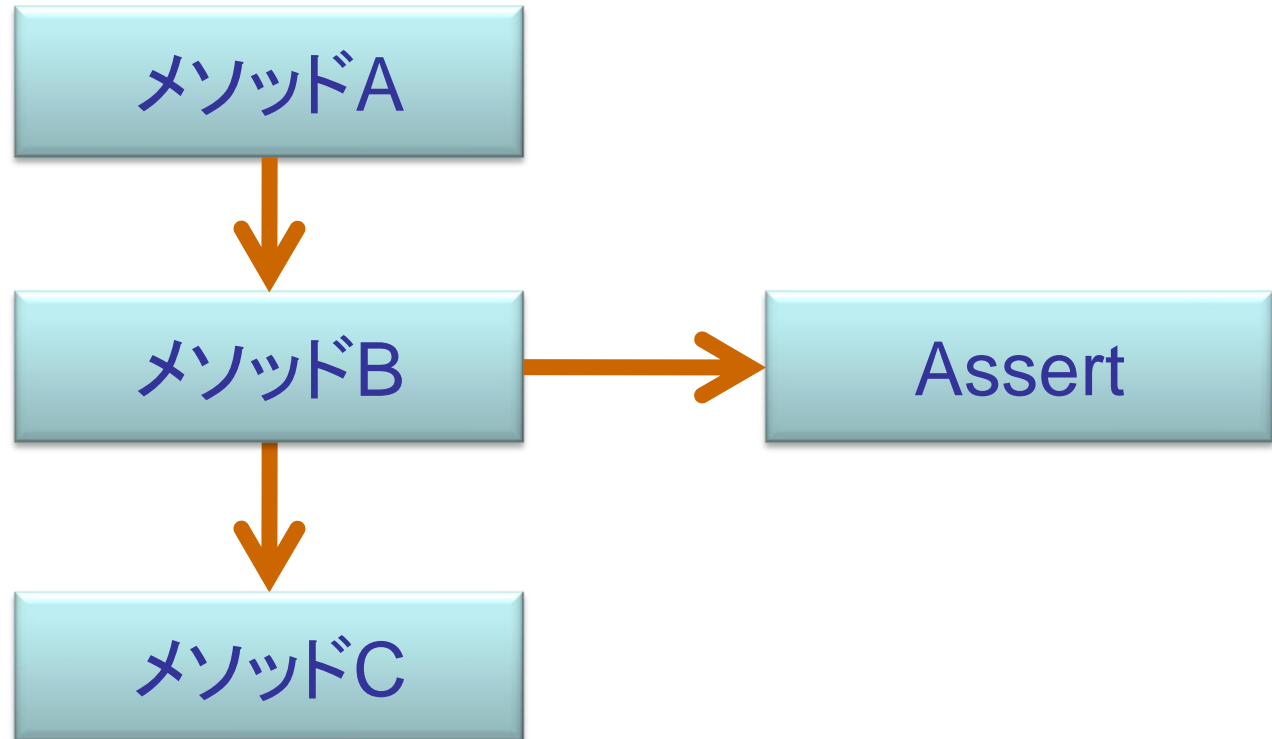
C#

```
NamedPermissionSet fullTrust;  
fullTrust = new NamedPermissionSet(_  
    "FullTrust", PermissionState.Unrestricted);  
fullTrust.Assert();  
// Excel 呼び出し
```

VB

```
Dim fullTrust As NamedPermissionSet  
fullTrust = New NamedPermissionSet(_  
    "FullTrust", PermissionState.Unrestricted)  
fullTrust.Assert()  
' Excel 呼び出し
```

Assert 処理は切り出してはいけません。



# アプリケーションをファイル サーバーで 配布するには

- あらかじめクライアントで、適切なアクセス許可が設定されている必要がある。

セキュリティ構成の配布

# ファイルサーバーの場合

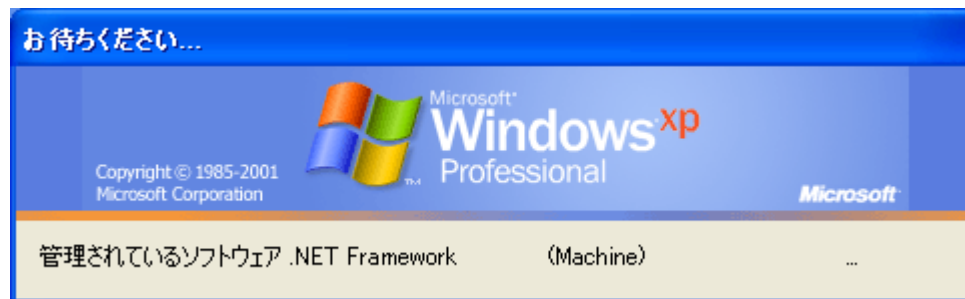
# セキュリティ構成を配布するには

- 1. Active Directory による配布
  - ソフトウェアの配布を使用して配布
- 2. SMS による配布
  - System Management Server による配布
- 3. カスタム配布
  - .msi ファイルをどうにかして配布、クライアントで実行する。



# セキュリティ構成を配布するには

- 1. Active Directory による配布



# CLICKONCE の場合

# ClickOnce の場合

## • ClickOnce のセキュリティ設定

The screenshot shows the Visual Studio 'Security' settings for a ClickOnce application. The left sidebar has 'セキュリティ\*' selected. The main area shows the 'ClickOnce セキュリティ設定を有効にする(N)' checkbox checked. Below it, the radio button for 'これは部分的に信頼するアプリケーションです' is selected. The 'ClickOnce セキュリティのアクセス許可' section shows the application zone set to 'ローカル イン트라ネット'. A table lists the permissions and their settings for this zone.

ClickOnce アプリケーションの実行に必要なコード アクセス セキュリティのアクセス許可を指定してください。 [コード アクセス セキュリティに関する詳細の表示...](#)

ClickOnce セキュリティ設定を有効にする(N)

これは完全に信頼するアプリケーションです

これは部分的に信頼するアプリケーションです

ClickOnce セキュリティのアクセス許可

アプリケーションがインストールされるゾーン(Z):

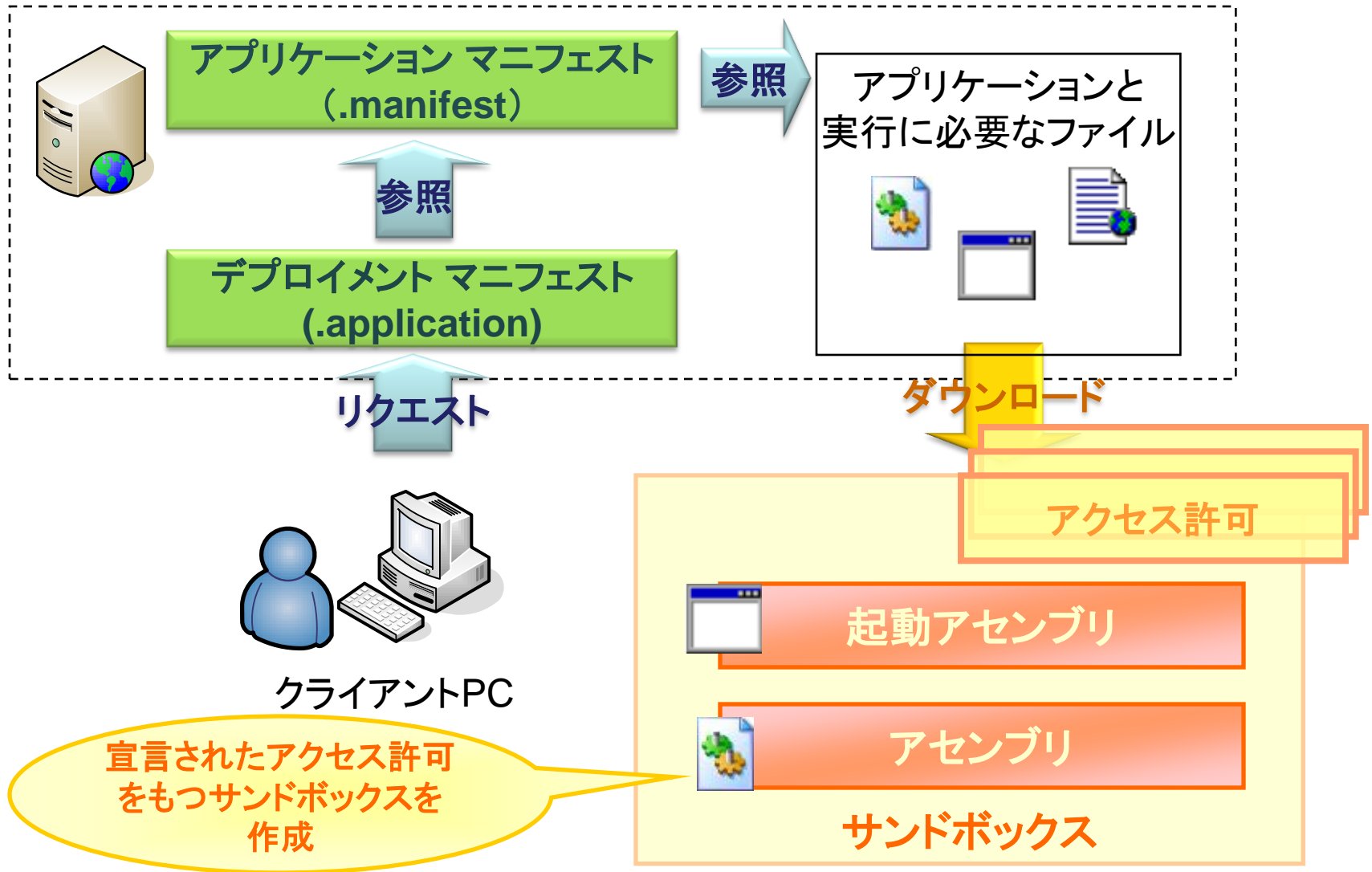
ローカル イン트라ネット

アプリケーションに必要なアクセス許可:

アクセス許可	設定	含まれるアクセス許可
EnvironmentPermission	ゾーン既定値	<input checked="" type="checkbox"/>
FileDialogPermission	ゾーン既定値	<input checked="" type="checkbox"/>
FileIOPermission	ゾーン既定値	<input type="checkbox"/>
IsolatedStorageFilePermission	ゾーン既定値	<input checked="" type="checkbox"/>
ReflectionPermission	ゾーン既定値	<input checked="" type="checkbox"/>

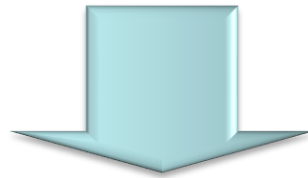
アクセス許可の検出(O)      プロパティ(O)...      リセット(R)

# ClickOnce の場合



## CAS 理解度チェック！

- 【Q】 Visual Studio 2005 で作成したアプリケーションをファイルサーバーにコピーして実行しました。うまく動きますか？



- 【A】 ファイル サーバーなどに配置しているときには実行できない処理もあります。
- その場合には、クライアントに適切なアクセス許可を設定するか、ClickOnce での配布を検討する必要があります。