# アドホックインスペクション
## ハンズオンでのインスペクション観点

本資料は、特に技法を利用せず、これまでの経験や普段のインスペクション／レビューで欠陥をみつけるときと同じようにインスペクションを実施いただくグループのための説明です。インスペクションは以下の観点で実施してください。

## 準備

本ハンズオンでは、以下のドキュメントが配布されます。

- インスペクション対象物（要件定義書、ソースコード）
- 参考資料（設計書）
- 空の欠陥リスト
- アンケート

**インスペクション観点：**　3つのセキュリティ要件が満たされているかの評価

以下にセキュリティ要件1、要件2、要件3を示します。セキュリティ要件1から順に評価してください。成果物（要件定義書、ソースコード）に含まれる、セキュリティ要件を満たさない欠陥を見つけたら、欠陥リストに記録してください。欠陥リストには、欠陥が含まれる文書名／欠陥の具体的な箇所／欠陥の簡単な説明／欠陥がどのセキュリティ要件を満たさないものであるかを記録してください。なお、欠陥リストの「指標番号／質問番号」への回答は不要です。

## セキュリティ要件

### 要件1：　シングルアクセスポイント

アクセスポイントとは、ユーザの要求がシステムのサービスを得るために経由しなければならないクラスやコンポーネントです。一般的に、認証／認定の一貫性を保つために、全ての認証／認定を一箇所で行うシングルアクセスポイントが望ましいとされています。しかし何らかの理由により、複数のアクセスポイントが必要になる場合もあります。そのような場合、各アクセスポイントで一貫した（同じ登録ユーザ名、パスワードでの）認証／認定を行うことが重要です。

### 要件2：　安全なユーザ登録

ユーザの新規登録を安全に行うためには、SSL(Secure Socket Layer)等の安全な（盗聴されない）通信路が必要です。システムには、ユーザを一意に識別できるIDを割り当てることにより、複数の登録者が誤って1つのIDでログインすることを防ぐ必要があります。また、登録しようとしているユーザが本当に本人なのかを確認する必要があります。たとえば、チャレンジレスポンス方式（例：メール内の確認リンク、折り返しの電話）による登録者の信憑性や個人情報の確認があります。個人情報は、文字列の妥当性検査（例：特殊文字の確認（メールアドレスに@が含まれる）、名前に含まれる母音数）、もしくは外部のシステム（例：クレジットカードの有効性をクレジットカード会社に、住所の詳細を住所録データベースに）の助けを受けることにより確認することができます。

### 要件3：　パスワード再発行の安全性

ユーザ名とパスワードの認証を使用するシステムは、パスワードが忘れられた場合に再発行する仕組みを用意しておくべきです。一般的に、ユーザがパスワードを設定済みの状態で、ユーザにパスワードを送り返すことは好ましくないとされていますが、ユーザがパスワードを思い出す可能性が低いことと、ユーザは安全でない通信路ではパスワードを送信しないだろうということか

© Fraunhofer IESE, 2009

ら、システムが自動生成した一時的な仮パスワードをユーザに送信します。この方法を使用するシステムには注意点があります。仮パスワードを発行した時点でユーザが元々設定したパスワードが無効になると、悪意ある攻撃者がパスワードの再発行を要求し、ユーザの元のパスワードを使用不可にさせることができ、正当なユーザが締め出される可能性があります。また、仮パスワードを同時に複数発行でき、それらが全てでログインが可能になる場合、悪意ある攻撃者が有効なパスワードを推測しやすくなります。また、仮パスワードは安全でない通信路で渡される場合には、仮パスワードではパスワード変更以外の機能を利用できないように制限することが望まれます。

© Fraunhofer IESE, 2009