アプリケーション開発への効果的なセキュリティ導入
Effective security implementation for application development

奥山 順子・マネジメント分科会・情報セキュリティ大学院大学

Abstract: As for information security measures, various guidelines, measures, and corresponding products have been announced. In application (software) development, many security design methods have been proposed, but there aren't enough man-hours and/or there aren't enough security skillful engineers in many development sites. In small-scale application development, "agile" has become the mainstream, emphasis on function and early release, so the designing security measures tends to be a lower priority. Drawing a data flow diagram (DFD) as the first step in security threat analysis to identify the key areas, then consider how to maximize the effectiveness of the security measures.

① 研究の背景とフォーカス

現在主流の開発手法:アジャイル

＜特徴・メリット＞
- 開発スピードを重視
- 開発の単位が小さい
- 顧客視点で機能の確認をしながら開発が進む
- ユーザーの隠れたニーズを掘り起こせる

＜弱点・デメリット＞
- 開発計画を立てて進めにくい
- 手法に熟練した開発者が少ない

プロトタイプ型、スパイラル型、DevOpsの特徴も便宜上こちらに分類する

セキュリティ実装のためのよく聞く手法

- DevSecOps
- OWASPシリーズ
- セキュリティ・バイ・デザイン

しかし

開発現場で聞いた課題

- セキュリティを考慮する対象が広すぎる
- セキュリティ設計のための標準が難しい
- セキュリティ設計のための期間・人材を配置できない
- セキュリティ対策より、早期に機能をリリースする優先度が高い
- 機能中心の考え方がデータ中心の考え方より開発には実用的と考えている

本研究のフォーカス

- 元々、アジャイルはウォーターフォール型開発の弱点を克服する開発手法として発展
- ウォーターフォール型開発の時代に利用されたデータに着目した方法論に、セキュリティ実装のヒントがないかを考えてみた

データに着目した方法論
- DOA(データ中心アプローチ)
- DFD(データフロー図)

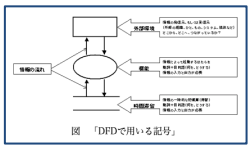
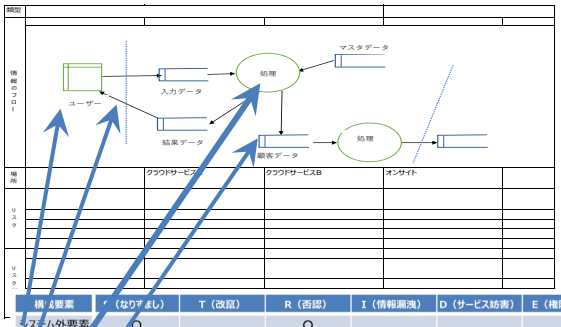


図 「DFDで用いる記号」

② データに着目した方法論をベースにした対策

脅威の分析 x DFDの作成



構成要素	S（なりすまし）	T（改竄）	R（否認）	I（情報漏洩）	D（サービス妨害）	E（権限昇格）
システム外要素	○		○			
プロセス	○	○	○	○	○	○
データフロー		○		○	○	
データストア		○	△	○	○	

脅威分析の対象を、重要情報(データ)に限定する

脅威分析:STRIDE分析とDFDは親和性が高い

対象システムの脅威分析を実施

＜分析スキル、分析期間、要員が十分ある場合＞
- ✓ システム構成、守るべき情報を網羅
- ✓ それぞれのコンポーネントに対して、脅威分析を行い、対策が決定するまで繰り返し検討

＜分析スキル、分析期間、要員が十分ない場合＞
- ✓ 機能の設計がスタートになりがち

提案する手順

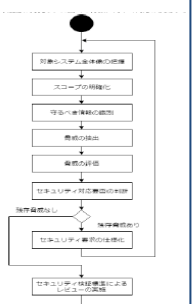
1. 脅威分析の最初のステップで、漏えい、改ざんされてはいけない情報が見えるデータフロー図を作成する
2. 情報の優先度を決める
3. 優先度の高い情報の周辺の脅威分析を、分析を許容できる期間内で重点的に実施する

③ 有効性の検証

＜検証の方針＞
- ✓ 現行方法での脅威分析と、提案する手法での脅威分析で効果を比較する(自社のアプリケーション開発)
- ✓ もし新手法の十分な実践での適用ができなかった場合は、既存の開発例に対して机上のシミュレーションで検証

＜検証の方法＞
- ✓ 優先度の高い情報(データ)を、個人情報に限定して分析を実施

※優先度の判断基準などを適用する工数が現時点では取りづらいため、情報漏洩のインパクトが大きい個人情報に限定して適用を試みる



↑ 全ての脅威にこのステップを適用しようとしている現状の手法

＜有効性の判断＞
- ✓ 作業工数、品質の比較
- ✓ 開発エンジニアが、手法を有用と認めるかの感覚
- ✓ 優先度を下げた対策箇所の残存したリスクの度合い

④ 今後の研究方針

- □ アプリケーション開発の実践への適用
  - ✓ 適用する難易度が高くないこと
  - ✓ 現行の開発工数を増やさないでできるか
- □ 先行研究を参照して検証の妥当性を確認する
  - ✓ 検証の方法は妥当か
  - ✓ 有効性の判断基準は妥当か

実際の開発現場に適用するには、エンジニアの協力が欠かせない。ただし実務への支障は最小限に抑える必要があり、現時点では論文の作成に必要な十分なデータが集まらない可能性もある。
これを補完する検証方法についても並行して検討していく必要があると考えている。