トップエスイー修了制作

コンポーネントベース開発における セキュリティ要件記法の提案

株式会社 日立製作所　山﨑　裕紀　hiroki.yamazaki.nt@hitachi.com

開発における問題点

コンポーネントベース開発によりソフトウェアコンポーネントの再利用・開発効率向上が期待されるが、コンポーネントが備えるべきセキュリティ機能は実際の配置(デプロイメント)の状況によって左右されるため、インテグレーションの度にコンポーネントのセキュリティ分析が必要となり、インテグレータにとって負担となっていた。

手法・ツールの提案による解決

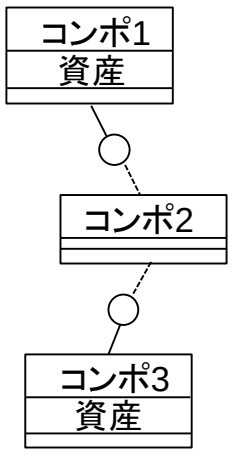
コンポーネント再利用に柔軟に対応可能なセキュリティ要件の記法を目指し、ソフトウェアプロダクトライン(SPL)化技法における意思決定モデルの拡張記法を提案する。セキュリティ脅威のリスク値とセキュリティ機能とを対応付け、パラメータ選択によりリスク値を自動再評価することで必要なセキュリティ機能を選択可能とする。

プロダクトライン化と意思決定モデルの拡張記法の提案

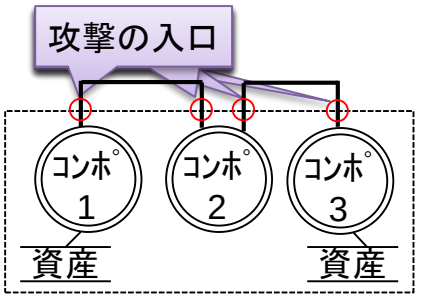
ドメインエンジニアリング【セキュリティ分析専門家がサポート】

・ソフトウェアコンポーネントの様々な配置に備え予め網羅的に脅威を分析
・拡張意思決定モデルで 脅威のリスク値 ⇔ 対策要件 ⇔ 機能 を対応付け

STEP1 コンポーネント分析



STEP2 コンポーネントの繋がりから攻撃の入り口を仮定し網羅的に脅威を洗い出し



コンポ1の脅威一覧	
T.漏洩	○○の資産が××により漏洩
T.改竄	○○の資産が△△により改竄
…	

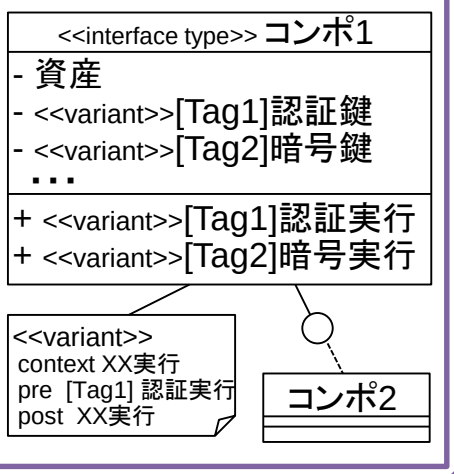
STEP3 STEP2の脅威事象を基に拡張意思決定モデル作成（STEP2を基に解析的に算出）

脅威事象	リスク値	対策要件
T.漏洩	6.6	O.認証
		O.暗号化
T.改竄	9.4	O.認証
		O.データ検証
…	…	

（セキュリティ機能単位でタグを付す）

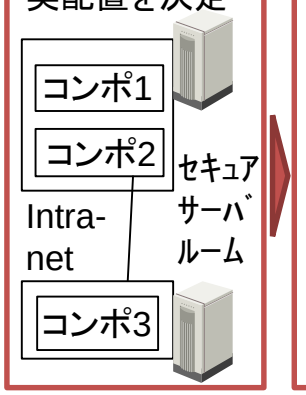
	対策要件	機能
コンポ1	O.認証	[Tag1] 認証機能
	O.暗号化	[Tag2] 暗号機能
	…	…

STEP4 STEP3でタグを付した機能を可変要素としてコンポーネント仕様に反映しアセット化



アプリケーションエンジニアリング【セキュリティ分析が専門ではないインテグレータが実施】

STEP1 実配置を決定



STEP2 配置環境から得られるパラメータ選択のみで自動でリスク値を再計算し機能選択

脅威事象	リスク値	対策要件
T.漏洩	3.7	O.認証
		O.暗号化
T.改竄	5.9	O.認証

・外部との繋がり(NW/近接/ローカル、直接接続 or not)
・事前認証の有無

	対策要件	機能
コンポ1	O.認証	[Tag1] 認証機能
	O.暗号化	[Tag2] 暗号機能

タグ参照しアセットの必要機能を選択

評価

・一定の情報資産を持つ架空のシステム（生体認証で本人確認を行うポイントシステム）に例題適用し、工数を評価

工程	工数
ﾄﾞﾒｲﾝｴﾝｼﾞﾆｱﾘﾝｸﾞ	約2週間
ｱﾌﾟﾘｹｰｼｮﾝｴﾝｼﾞﾆｱﾘﾝｸﾞ	約1−2日

・ｱﾌﾟﾘｹｰｼｮﾝｴﾝｼﾞﾆｱﾘﾝｸﾞの工程自動化により、インテグレータの負荷軽減を確認
・実案件への適用等を通した従来プロセスとの総工数比較は今後の課題