

ソフトウェア設計におけるセキュリティ脆弱性の検索方式

塚本 良太[†] 小林 大樹[†] 山田 亮[†] 田村 孝之[†]

三菱電機株式会社 情報技術総合研究所[†]

1. はじめに

1.1. セキュリティ脆弱性対策の主な手法

近年、ソフトウェアの活用は IT システムに留まらず、様々な機器やシステムの制御に広がっており、ソフトウェアのセキュリティ脆弱性対策の重要性が一層高まっている。一般的にソフトウェアのセキュリティ脆弱性の対策費用はシステムライフサイクルの後工程になるに従い増大する。従って、製品出荷前にできるだけ脆弱性を低減する必要がある。

セキュリティ脆弱性を検査する方法はセキュリティベンダ等が検査ツールを提供する形態や、検査工程そのものを業務サービスとして提供する形態がある。具体的な手法は表 1 に示すように、ソースコードを検査する手法、脆弱性を発現させやすいデータを入力する手法（ファジング）、システムのバージョン等を検査する手法、Web アプリケーションに特化した検査手法やペネトレーションテストなどがある。

表 1：主なセキュリティ検査手法[1]

セキュリティ検査	実施フェーズ
ソースコードセキュリティ検査	実装・テスト
ファジングによる検査	実装・テスト
システムセキュリティ検査	テスト・運用
Web アプリケーションセキュリティ検査	テスト・運用
ペネトレーションテスト	運用

1.2. 本研究の目的

上記のように脆弱性検査には様々な手法があるが、実装やテスト以降のフェーズを対象とした手法が主であり、設計フェーズにおける検査は依然として綿密なレビューを必要とする。セキュリティ脆弱性に関するガイドラインは整備されつつあるが、実際の活用には専門的な知識が必要であり、属人性が高く対策に要する期間も長くなるという課題がある。

よって、本稿ではセキュリティの専門知識を A method for searching security vulnerabilities in software design

[†] Ryota TSUKAMOTO, Taiki KOBAYASHI, Ryo YAMADA and Takayuki TAMURA
Information Technology R&D Center, Mitsubishi Electric Corporation

持たない設計者であってもガイドラインを用いて漏れのない脆弱性検査を可能とする検索方式を提案する。本方式によって設計フェーズにおけるセキュリティ脆弱性の検出の支援が可能になり、属人性の排除と対策期間の短縮が期待できる。

2. 情報資産の操作特性に基づく検索方式

2.1. 検索方式の概要

本方式はソフトウェア設計者が検査対象ソフトウェアの設計書から読み取れる特性を入力し、脆弱性一覧を取得するシステムである。本方式のシステム構成図を図 1 に示す。

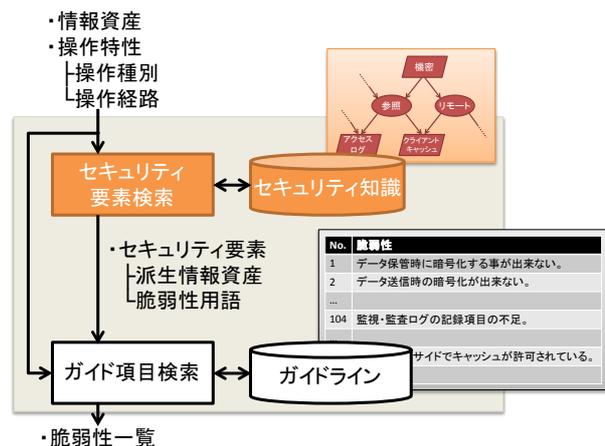


図 1：セキュリティ脆弱性検索システム構成図

検査対象ソフトウェアを構成する個々の機能の特性を、扱う情報資産、操作種別（CRUD 等）、操作経路（ネットワーク等）で表現することとし、この 3 要素を検索のインタフェースとする。以下、操作種別と操作経路をまとめて操作特性と呼ぶ。

セキュリティ要素は情報資産とその操作特性に関する派生情報資産と脆弱性用語であり、それらの関係をグラフ構造のセキュリティ知識として格納しておく。セキュリティ要素検索がこのグラフを辿ることで、セキュリティ専門家と同様の視点で脆弱性項目を指摘することが狙いである。また、グラフ構造とすることで、情報資産、操作特性、セキュリティ要素の組み合わせを柔軟に表現でき、単純なキーワード検索では漏れる関係を管理できる。

このように得られたセキュリティ要素を加えてガイドラインを検索することで、機能の特性に直接関わる脆弱性だけでなく、セキュリティ専門家の知見が反映された脆弱性一覧が得られ、設計者がセキュリティ専門知識を必要としない。

2.2. セキュリティ要素の検索方法

ここではリモートから機密を参照する機能について検査を行う場合を例に検索方法を説明する。セキュリティ知識は図2に示すように、情報資産、操作特性、セキュリティ要素の3段のグラフで構成する。

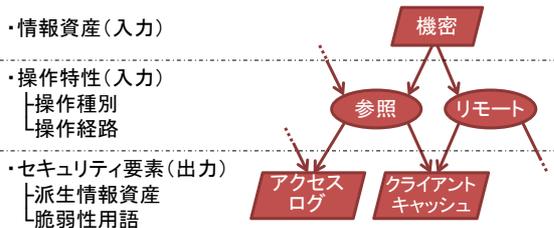


図2: セキュリティ知識の構成

セキュリティの専門家は、例えば「機密」を「参照」するときには「アクセスログ」が必要といった知識を3段のグラフで紐付けし蓄積する。3段目の派生情報資産は1段目の情報資産に紐付けされても良い。

検索時には、入力された情報資産を示すノードを起点に、入力された操作特性を示すノードを辿り、セキュリティ要素を示すノードを取得することで、検査対象ソフトウェアの機能の特性に応じたセキュリティ要素を得る。

3. 脆弱性の検査手順評価

3.1. 評価環境

ここでは表2に示す環境において本方式を用いる場合と手動の場合の脆弱性検査の手順を示し比較評価する。

表2: 評価環境

検査対象	機能数: 4 機能 設計書: 19 ページ
ガイド	分類(セキュリティ要素): 123 項目
ライン	脆弱性: 493 項目

3.2. 手動による検査手順 (従来方式)

従来の手動による脆弱性抽出の手順を示す。

- (0) 検査対象の設計内容とガイドラインの内容の両方を十分に理解した者が実施する。
- (1) 検査対象の機能毎に以降の手順を実施する。
- (2) ガイドラインから検査対象機能に関すると考えられる脆弱性を含む分類を選定する。
- (3) 選定した分類に含まれる全ての脆弱性を抽出する。
- (4) 抽出結果の各脆弱性について、検査対象機能に該当するか判断する。

3.3. 本方式による検査手順

本方式を用いた脆弱性抽出の手順を示す。

- (1) 検査対象の機能毎に以降の手順を実施する。
- (2) 検査対象機能が扱う情報資産とその操作種別・経路を設計書から特定する。
- (3) 特定した情報を基に脆弱性を検索する。
- (4) 検索結果の各脆弱性について、検査対象の機能に該当するか判断する。

3.4. 比較評価

従来方式と本方式による手順との比較結果を表3に示す。属人性の課題に対しては検査に必要な知識を比較し、対策期間の課題に対しては分担作業の可能性を比較し、本方式の効果を確認した。

表3: 手順の比較評価

評価項目	従来方式	本方式
必要知識	検査対象 セキュリティ	検査対象
分担作業	困難	容易

必要知識について、従来方式では検査対象の設計知識とセキュリティ知識が必要であったが、本方式の手順では検査対象の特徴で検索するためセキュリティ知識が不要となる。

分担作業について、従来方式では作業員全員がセキュリティ知識を有すれば可能であるが、継続的な学習が必要なため実際は困難である。一方で、本方式では分担作業は容易である。

精度や工数の定量評価のうち、従来方式については、598 項目の脆弱性を抽出しており、綿密に手動抽出した結果を正として、適合率 77.8%、再現率 100%であった。また工数は 3 人日/100 項目であった。本方式の定量評価は精度に関わる関連研究[2]も含めて今後実施する。

4. まとめ

本稿では、ソフトウェアの設計時において、機能が扱う情報資産とその操作種別・経路を検索軸としてセキュリティ脆弱性対策を検索する方式を提案した。これにより従来に比べて属人性の排除と対策期間の短縮に効果が見込めることを示した。

今後は定量評価を行い、課題抽出とさらなる自動化を図っていく。

参考文献

- [1] IPA: 脆弱性検査と脆弱性対策に関するレポート, <http://www.ipa.go.jp/files/000032929.pdf> (2013)
- [2] 小林 大樹: ソフトウェア設計に適用する複数ガイドライン間の用語揺れとその対策, 情報処理学会全国大会 (2014)