5ZC-07

BEYOND:セキュリティ対策システムの運用手法と脆弱性検知率向上のための WebUI の開発

中村 友昭† 竹原 一駿† 山下 俊明† 宗雪 勝也† 小野 滋己† 後藤田 中† 喜田 弘司† 最所 圭三†
香川大学†

1. はじめに

近年，大学に対する脆弱性を利用した攻撃が増加している．こうした攻撃に対して企業等では脆弱性診断ツールを用いて対策を行うが，大学では機器を一元管理していないため難しい．そのため，我々は公開されている脆弱性情報と組織内の機器にインストールされているソフトウェア名やバージョン番号などの機器情報を元に脆弱性を検知するセキュリティ対策システム BEYOND を開発した．

BEYOND の有効性を確かめるべく香川大学で運用している機器に対して BEYOND を導入し，システム管理者に対して評価実験を行った[1]．対象機器に存在する脆弱性を持つソフトウェアの件数で評価をしたが，本格運用するには再現率が不足していることがわかった．その原因として，収集した機器情報のソフトウェア名とバージョン番号に対応できないパターンがあったためである．

本稿では，機器情報を修正するためのシステム管理者に向けた WebUI の作成と自動修正機能の開発を述べる．

2. BEYOND

脆弱性情報収集部，IT 資産管理部，影響算出部，ネットワーク制御部，更新支援部，フロント部によって構成される(図 1).

A.脆弱性情報収集部にてインターネット上に公開されている脆弱性情報を収集しデータベース(以下 DB)化する．**B.**IT 資産管理部にて組織内の機器情報はエージェントソフトウェアと WebUI からの入力により取得する．機器情報にはソフトウェア情報(ソフトウェア名とバージョン番号)が含まれる．**C.**影響算出部にて，**A, B** で収集された情報を突き合わせ，脆弱性を検知する．検知した脆弱性の深刻度と機器の利用状況から対策方針を算出し，機器の利用者や情報システムの管理者に通知を行う．**D.**影響度の高い脆弱性が発見されたときなど早急に保護が必要である場合はネットワーク制御部でネットワークから遮断，隔離を行うことで対処する．**E.**更新支援部ではソフトウェアの更新を自動で行うスクリプトを配布することで脆弱性の解消を行う.**F.**フロント部においてこれらの機能を制御する．

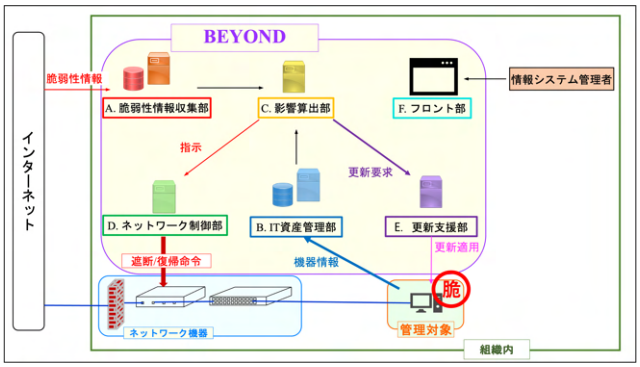

図 1 BEYOND の構成図

3. 課題・要件

影響算出部では，脆弱性の検知にソフトウェア名とバージョン番号を用いる．しかし，[1]で行った評価実験では，図 2 に示すパターンに対応できておらず，今後も未対応のパターンが収集されることになると考えた．

そこで，未対応のパターンをシステム管理者が修正し，その修正内容を自動で継続的に適用する修正機能を開発することで，本番運用に向けた脆弱性検知の再現率の向上を目指す．

当修正機能を使用した未対応のパターンに対する修正の流れを述べる(図 3)．PC1 に導入したエージェントからソフトウェア情報が IT 資産管理部に送信される．送信されたソフトウェア情報は修正機能で修正履歴と比較される．修正履歴に無い場合，未対応のパターンに対し，当修正機能を用いて WebUI からシステム管理者が修正作業を行う．未対応のパターンの判別方法として，図2の表1行

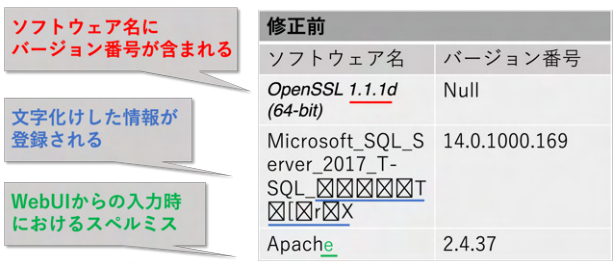

図 2 未対応パターン

BEYOND: Development of WebUI to improve security system operation method and vulnerability monitoring rate
† Tomoaki NAKAMURA, Ichitoshi TAKEHARA, Toshiaki YAMASHITA, Katsuya, MUNEYUKI Shigemi Ono, Naka GOTODA, Koji KIDA, Keizo SAISHO ・ Kagawa University

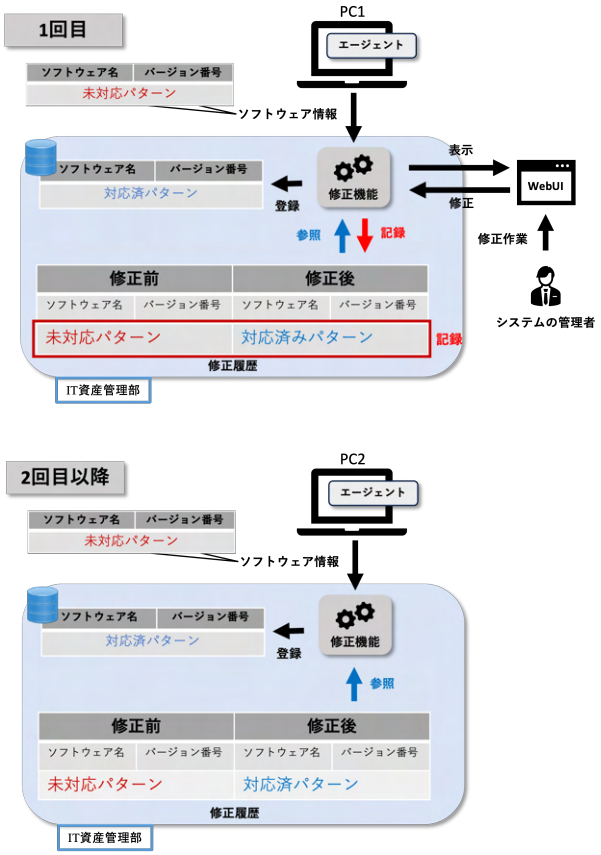

図 3 自動修正機能

目のパターンの場合，ソフトウェア譲歩のどちらかに null 値が登録されるため null で検索をかけることで判別する．それ以外のパターンについては目視で行う．修正した内容は修正履歴(表 1)に記録される．次に，PC2 に導入したエージェントから PC1 と同様のソフトウェア情報が IT 資産管理部に送信される．PC2 から送信されたソフトウェア情報は，修正機能が修正履歴を参照し，同様のパターンがあれば修正履歴に従って修正を行う．

修正作業の負担について述べる．図 2 の表 1, 2 行目のパターンは，パッケージソフトウェアやレジストリからの収集で見られる．ここで収集されるソフトウェア情報は標準でインストールされているものを含むため，登録されるソフトウェアの種類は機器の台数に正比例しないことから，修正作業は比較的容易であると考えられる．図 2 の表 3 行目のパターンは，修正を繰り返すことで発見される未対応のパターンは徐々に減少していくと考えられる．

4. 修正機能の開発

以下に示す WebUI を使用してシステム管理者は修正作業を行う(図 4)．

①ソフトウェア情報の選択

機器から収集したソフトウェア情報の一覧から

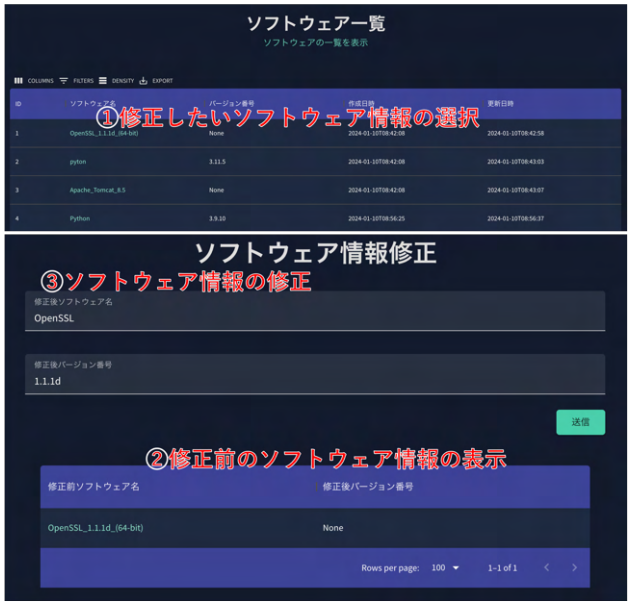

図 4 ソフトウェア情報修正インターフェース

未対応のソフトウェア情報を選択する．選択すると，ソフトウェア情報修正フォームが表示される．

②修正前のソフトウェア情報の表示

ソフトウェア情報修正フォームには選択されたソフトウェア情報の現在の状態が表示される．システム管理者はこの情報を参考にしながら，適切な修正を行う．図の場合「OpenSSL_1.1.1d_(64-bit)」というソフトウェア名が登録されている．

③ソフトウェア情報の修正

修正後のソフトウェア情報を入力フォームに入力する．この場合修正後のソフトウェア名は「OpenSSL」バージョン番号は「1.1.1d」となる．入力後、「送信」ボタンを押すと，ソフトウェア情報が更新され，修正前後の情報が修正履歴に記録される．これ以降，エージェントから送信されたソフトウェア情報は，修正履歴の修正前に記録された内容を同様であれば修正後のソフトウェア情報を IT 資産管理部の DB に記録できる．

5. おわりに

セキュリティ対策システム BEYOND の開発を行っている．本稿では，開発している BEYOND の再現率向上のための WebUI の開発と修正機能の開発について述べた．今後の課題として修正作業を補助するためのサジェスト機能の追加などを考えている．異なるソフトウェアバージョンが送信された場合への拡張を考えている．

参考文献

[1] 中村 友昭, 竹原一駿, 大野真伯, 山下俊昭, 宗雪勝也, 小野滋己, 喜田弘司, 後藤田中, 最所圭三, "脆弱性情報を用いたセキュリティ保護システム“BEYOND”の開発", 大学 ICT 推進協議会 2022 年度年次大会論文集, 13PM2B-3, 2022