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

22G359 中村 友昭 (最所研究室)

1 はじめに

当研究室では, 脆弱性を利用した攻撃から組織内 の情報資産を守るという目的で, インターネット上 に公開されている脆弱性情報と組織内の機器情報を 用いて脆弱性対策を行うセキュリティ対策システム "BEYOND" (Bring Enhancement Your Own Nonvulnerable Device) の開発を行なってきた. BEYOND はインターネット上に公開された脆弱性情報を収集す る脆弱性情報収集部、組織内の機器情報を管理するIT 資産管理部, 脆弱性情報と機器情報を突き合わせるこ とで脆弱性を検知し、対応方針を算出する影響算出部、 影響算出部で算出された制御方針に基づいてアクセス 制御を行うネットワーク制御部、ネットワーク制御さ れた機器に対して、修正パッチの適用支援を更新支援 部で構成される. BEYOND の構成を図1に示す. 本 稿では、BEYOND が脆弱性対策に効果的か示すため に本学の情報メディアセンターにて試験導入し、そこ で発見した課題を解決することで実運用を目指す.

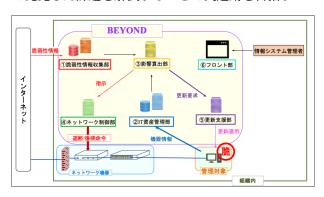


図 1: BEYOND の全体図

2 先行研究の課題

先行研究により、BEYOND の統合と情報メディアセンターへの試験導入を行った結果、以下に示す課題があった。

課題 1 BEYOND では、機器情報の収集から脆弱性の検知まで行うには各機構で得られた結果を手動で他の機構に渡す必要があった。また、利用者に対する UI がなく、機器情報の登録や閲覧、更新、削除を行うことが困難だった。

課題 2 BEYOND を試験運用した際, 脆弱性検知の 再現率が不足していた. 原因としては, ソフトウェア 名とバージョン番号に機械的にマッチングできない形 式が存在したためであった.

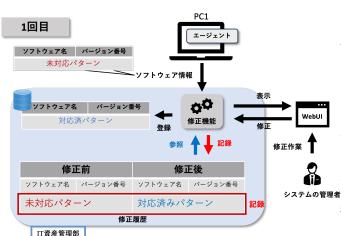
3 課題の解決方法

2章で述べた課題の解決方針を以下に示す.

課題1の解決: WebAPIと WebUIの実装課題1 の解決方法として、各機構に対して WebAPI を実装 し、それらを制御するための WebUI の開発を行った. 脆弱性収集部では、BEYOND 統合のための API と して、影響算出部が脆弱性を検知する際に必要な脆弱 性を持つソフトウェアやバージョンの範囲を提供する API を実装した。また、フロント部において、脆弱性 情報の詳細情報 (対策方法,影響等) を提供する API を実装した. IT 資産管理部では、影響算出部が脆弱性 を検知する際にサービスが使用しているソフトウェア 情報やインストールされているソフトウェア情報を必 要とするため、それらの情報を提供する API を実装 した. さらに、フロント部での機器情報の登録を補助 するための API を実装した. 影響算出部では、フロン ト部から脆弱性の検知を行うための API を実装した. さらに、BEYOND のフロント部を開発し、WebAPI から得た情報の受け渡しを行う WebUI を開発するこ とで各機構の制御を行えるようにした.

課題 2: ソフトウェア情報修正機能の実装

課題 2 の解決方法として, 脆弱性検知の再現率を 向上させるためのソフトウェア情報修正機能を開発す る. ソフトウェア情報修正機能は, IT 資産管理部で収 集された影響算出部において未対応のパターンのソフトウェア情報を修正する機能である。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修正した内容は修正履歴に記録される。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。



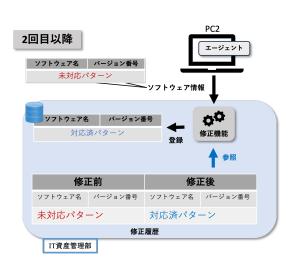


図 2: ソフトウェア情報の自動修正機能

4 評価

開発したソフトウェア情報修正機能を使用した時の BEYOND の性能評価について述べる.評価対象として評価結果を図3に示す.拡張したエージェントの性能評価について述べる.エージェント実行時の CPU 使用率は 0.2

	再現率	適合率	F値
LDAPサーバ2修正前	0.577	0.94	0.715
LDAPサーバ2修正後	0.994	0.954	0.973
SMTPサーバ3	0.994	0.954	0.973

図 3: 評価結果

5 終わりに

本稿では、BEYOND 運用のために各機構に対してWebAPIを実装し、各DBの情報を他の機構でも扱えるようにすることでBEYONDを1つのシステムとして統合した。また、ユーザがBEYONDを利用するためのWebUIを実装した。これにより、BEYONDを一つのシステムとして扱うことが出来るようになった。さらに、ソフトウェア修正機能を実装することで、脆弱性情報の再現率を向上させることができた。

参考文献

[1] 中村友昭 他, "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