# 脆弱性情報を用いたセキュリティ保護システムの運用に向けた機能改善

23G355 衣川達 (最所研究室)

## 1　はじめに

香川大学では現在，機器情報を手動で管理し，古い機器情報のまま放置されていること，脆弱性の情報が入ると資料を目視で比べて判断を行っているという現状がある．また，Check Point Software Technologies Ltd. の Check Point Research によると，教育機関に対するサイバー攻撃の割合は増加している [1]. 機器の管理が正確に行われていない状態が続いている状態は危険であるため，対応が急務である．

当研究室で開発している，組織内の機器を一元管理し，公開されている脆弱性情報を元に組織内の機器が持つ脆弱性を検知するセキュリティ対策システム“BEYOND”[2] を用いることで，情報をシステムで管理し，脆弱性を利用したサイバー攻撃を対策する．

本研究では，香川大学の情報メディアセンターで実運用に向けて残っている課題を整理し，解決，運用を視野に入れた調整を行う．

本稿では，解決する課題を整理し，解決案について述べる．

## 2　BEYOND 本格運用のための課題

BEYOND は現在，これまでの研究で開発されたシステムのうち，脆弱性情報収集部，IT 資産管理部，影響算出部，フロント部を統合し，情報収集から脆弱性の検知までを行うことが可能となっている．検知率については，情報の修正を行うことで機器が持つほぼ全ての脆弱性を検知できることが確認されている．一方，検証は Linux のサーバでのみ行われている，現在の BEYOND では作業が楽にならないといった職員からのアンケート結果が得られている．

1. 診断を行う際に不要な情報を参照する
2. 脆弱性情報から機器を検索できない
3. 通知機能がない

### 2.1　診断を行う際に不要な情報を参照する

機器に対して脆弱性診断を行う際，1 つの機器が持つ全てのソフトウェア情報と，収集した全ての脆弱性情報を突き合わせる．初回の診断であれば問題ないが，情報が更新された場合においても，更新部分とは関係ない情報まで全て参照する仕組みになっている．これにより，処理に非常に時間がかかること，登録される情報に重複が生じるといった問題が発生する．

### 2.2　脆弱性情報から機器を検索できない

現在，機器情報からその機器が持つ脆弱性一覧を閲覧することができる．しかし，実際に脆弱性が発表され，対応するまでの流れとして，発表された脆弱性を確認し，組織の中に対象となる機器が存在するかを確認するという流れとなる．この流れに従うには，機器情報ではなく脆弱性情報を起点として，対応が必要な機器を発見する必要がある．

### 2.3　通知機能がない

対応が必要だと考えられる診断結果が出た場合には，通知を行う必要がある．現状の BEYOND にはその機能がないため，追加する必要がある．

これらの課題のうち，本研究では診断を行う際に不要な情報を参照する問題を解決する．

## 3　課題の解決手法

脆弱性診断機能は，現在保有している全ての脆弱性情報 (version テーブル) と機器情報 (softwares テーブル) を入力して脆弱性診断を行い，検出した脆弱性を機器情報 DB の vulnerablities テーブルに登録する．この処理を拡張することにより，追加された新規情報と既存の情報との突き合わせを行うことが出来るようにする．新規情報が登録される場合は以下に分けられる．

1. 脆弱性情報をインターネットから 1 日 1 回収集するとき
2. 機器の登録またはソフトウェアの更新により，ソフトウェア情報を登録するとき

### 3.1　脆弱性情報をインターネットから 1 日 1 回収集するとき

脆弱性情報をインターネットから 1 日 1 回収集する場合，新規に登録された脆弱性情報と管理する機器が持つ全てのソフトウェア情報を突き合わせる．処理方法を図 1 に示す．

新規情報を保存するためのテーブルを用意する．インターネットから脆弱性情報の収集を開始する前にこ

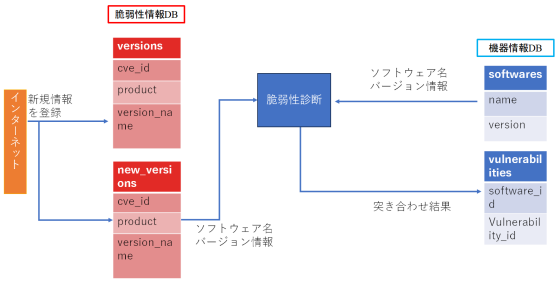


図 1　新規の脆弱性情報が登録された場合の処理

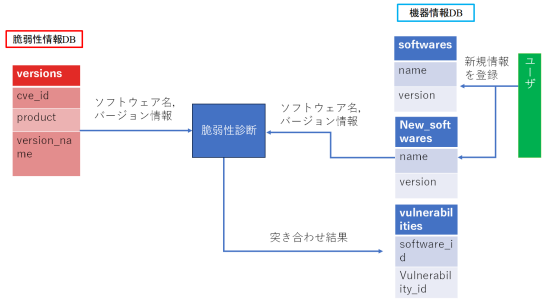


図 2　新規の機器情報が登録された場合の処理

のテーブルを空にする．収集を完了した後に新規情報と機器情報を突き合わせ，機器情報 DB に診断結果を登録する．

### 3.2　機器の登録またはソフトウェアの更新によりソフトウェア情報を登録するとき

機器の登録またはソフトウェアの更新によりソフトウェア情報を登録する場合，登録される情報のうち既に他の機器が持っているソフトウェア情報と重複しているものを除いた，新規に登録されるソフトウェア情報と収集されている脆弱性情報全てを突き合わせる．処理方法を図 2 に示す．

新規情報を保存するためのテーブルを用意する．ソフトウェア情報の登録が実行されたとき，最初の処理としてこのテーブルを空にし，既存のテーブルと同一の情報を登録する．登録完了後，新規の機器情報と脆弱性情報を突き合わせ，機器情報 DB に診断結果を登録する．

## 4　評価

### 4.1　評価手順

機器管理 DB に登録されているソフトウェア 966 件に対して，参照する脆弱性情報 DB に登録される versions テーブルの件数を変えて診断の実行時間を計測する．計測には，診断開始時に実行時間を計測するコードを埋め込む．登録する versions テーブルの件数は，全体の件数 1940076 件，1 年を想定した件数 14923 件，1 日を想定した件数 657 件とする．

### 4.2　評価結果

件数と実行時間の結果を以下の表 1 に示す．

表 1　評価結果

| 件数 | 実行時間 (s) |
|---|---|
| 1917878 | 3445.981 |
| 8461 | 48.650 |
| 657 | 25.728 |

### 4.3　考察

実験結果より，実行時間の短縮が見込めた．脆弱性を持つ可能性のあるソフトウェア名を 1 件ずつ versions テーブルから探しているため，機器情報 DB に登録されているソフトウェア 1 件当たりにかかる探索の時間が短縮されたと考えられる．

## 5　おわりに

本稿では，脆弱性情報を用いたセキュリティ保護システムの運用に向けた機能改善について述べた．脆弱性情報を新規登録時に一時的に保存するテーブルを用意し，診断に使用することで診断時間の短縮を確認することが出来た．今後の課題として，通知機能の作成や新規情報を活用したデータの閲覧，インシデント対応履歴を残すような機能の追加が必要だと考えている．

## 参考文献

[1] Check Point Software Technologies Ltd., “Check Point Research Warns Every Day is a School Day for Cyber Criminals with the Education Sector as the Top Target in 2024”, https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/, 2024/12/4.

[2] 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.