脆弱性対策のためのセキュリティ保護システム”BEYOND” における WebUI の改善

最所研究室 18T306 岩下蓮師

１．はじめに

本研究室ではセキュリティ保護システム“BEYOND”[1]を開発している．本システムは脆弱 性を持つソフトウェアの情報と組織内の機器情報を収集し，これらの情報から脆弱性を持つ機器を検知し，内部ネットワークから隔離するなどのアクセス制御を行う．隔離された機器を復帰させるためには脆弱性を解消する必要があり，機器のユーザや管理者はソフトウェアを更新する必要がある．ソフトウェアを更新するために更新に必要なファイル(パッチ)を提供している外部のサーバにアクセスする必要が出てくるが，このために隔離された機器(対象機器)が外部ネットワークにアクセスできるようにすることは危険である．

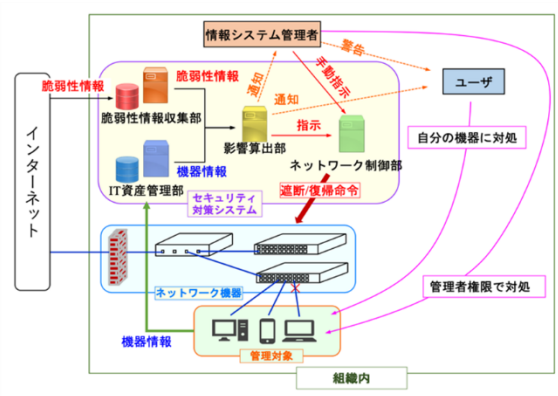

図 1 BEYOND の概要

現在 BEYOND では，システム利用者が直接操作する WebUI に様々な問題がある．本研究では組織で本システムを利用する際に使用する WebUI の改善をすることにした．

２．課題

現在，先行研究[2]で開発されている WebUI にはいくつかの問題がある．

①ユーザの属性によるアクセスレベルの管理

現在，ユーザがシステムを利用する際に，組織の管理者と一般利用者でアクセス可能なページが同一である．そのためユーザの属性(管理者，一般利用者等)によるアクセス可能な範囲の変更が必要である．

②検索パラメータの不足

収集した脆弱性情報を WebUI で確認する際に，現在の WebUI では CVE-ID とソフトウェア名での検索しか行うことが出来ない．実際に利用する際には，CVSS スコアやキーワード等の複数のパラメータでの検索に対応しなければ， 目的とする脆弱性情報にアクセスすることができない．

③情報のソート

各情報(機器一覧，ソフトウェア一覧等)を閲覧する WebUI が現在は，データベースから取得したテーブルを直接表示されるだけの状態になっている．そのため，人 2 の情報にアクセスするまでにかなりの時間を要する．

以上の課題を解決できる WebUI の改善を行う．

３．WebUI の概要

現在の WebUI の遷移図を図 2 に，本研究で提案する WebUI の遷移図を図 2 に示す．

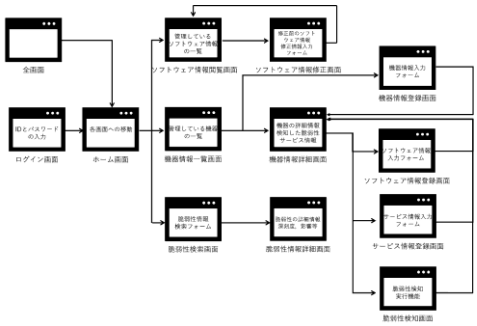

図 2 現在の WebUI の遷移図

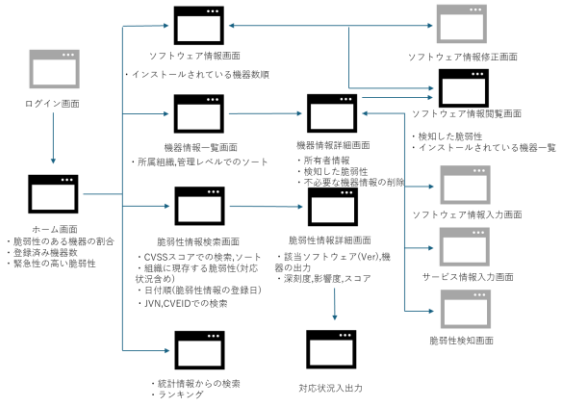

図 3 本研究での WebUI の遷移図

図 3 においてグレーアウトしている部分につ

いては現在既に実装済みの部分で，実線での表示部が本研究での提案部分である．

3．1 ユーザの属性によるアクセスレベルの管理

本システムを利用する各部局ごとで最初にユーザ登録を行ったものに管理者である権限である admin 権限を付与する．admin 権限を持つもののみ，組織全体の機器に関する情報にアクセス可能である．その後に登録を行う一般利用者には，member 権限を付与する．member 権限では自身の機器に関する情報のみ，閲覧，編集が可能になっている．

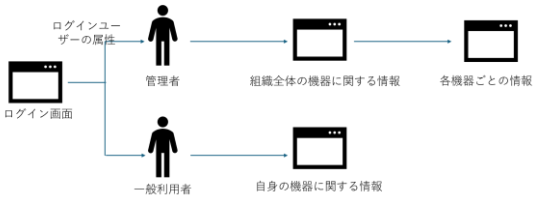

図 4 ユーザの属性によるアクセスレベルの管理

3．2 検索パラメータの設定

脆弱性情報を検索する際に現在は，CVE - ID とソフトウェア名での検索しか行うことができな いため，特定の脆弱性の検索をするために必要な情報が固定されていた．そのため，検索に用いる事ができるパラメータを増やし，様々の情報から脆弱性の検索を行うことができるように変更した．

具体的に実装した検索パラメータは CVSS スコア(0．0 - 10．0)，脆弱性情報の公開日，深刻度，キーワードである．

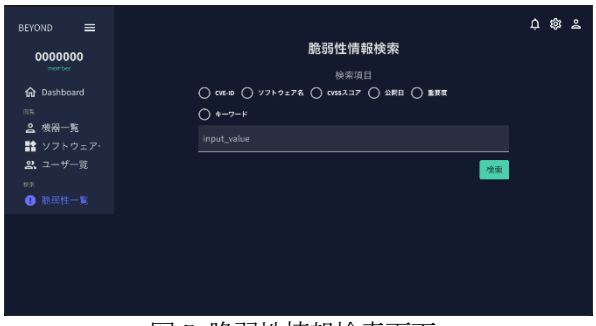

図 5 脆弱性情報検索画面

3．3 情報のソート

従来のソフトウェア情報一覧画面では IT 資産管理部で収集した情報で構築したデータベースから取得した情報を一覧として表示していたのみであったため，目的のソフトウェアを探すことが困難であった．そのため，本研究では，ソフトウェア名，ヴァージョン，重要度，該当ソフトウェアの脆弱性の有無から，絞り込み，ソートを行うことができるように WebUI の改善を行った．

図 6 ソフトウェア情報一覧画面

4．機能評価

本システムを組織で利用する想定でデータベース経データの挿入を行い，実装したものが機能するか実験を行った．

ユーザの作成順によるアクセスレベルの管理，各パラメータでの検索，ソフトウェア情報の絞り込み，ソートが実際に機能することを確認できた．

図 7 ユーザ一覧での権限レベルの確認

5．おわりに

本稿では，セキュリティ保護システム“BEYOND”において本システムをユーザが利用する際に操作する WebUI の改善を行った．本改善をおこなったことにより，組織内でのアクセス管理や，特定の情報へのアクセスを可能とした．今後の課題として，各脆弱性に対する対応状況の入出力，ダッシュボード上での組織に存在する脆弱性の対応率，緊急で対応する必要のある脆弱性の表示や組織全体に存在する脆弱性の多さや使用している OS 等の統計情報からのランキング機能などの開発を考えている．

参考文献

[1] 細川洋輔，竹原一駿，西岡大助，中村友昭，岩下蓮師，喜田弘司，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における機器の利用実態に基づいたアクセス制御ポリシーの考案”，令和 3 年度電気・電子・情報関係学会四国支部連合大会，16-3，2021