脆弱性対策のためのセキュリティ保護システムにおける影響算出部の開発

17T271　細川洋輔（最所研究室）

１．はじめに

ゼロデイ攻撃などの脆弱性を突く攻撃から組織内の機器を守らなければならない．本研究では，インターネット上に公開されている脆弱性情報と，組織内のネットワークに接続される機器の機器情報・ソフトウェア情報を用いて，機器に脆弱性が存在するか検査を行い，脆弱性の深刻度と該当機器のサービス情報に基づいてネットワークのアクセス制御を行うシステム“BEYOND”を開発している．本稿では，開発した BEYOND の影響算出機構について述べる．

２．BEYOND

BEYOND の全体構成を図 1 に示す．BEYOND は，インターネット上で公開されている脆弱性情報を取得し DB 化し管理している脆弱性情報収集部，組織のインターネットに接続される機器の機器情報・ソフトウェア情・サービス情報を取得し DB 化し管理している IT 資産管理部，脆弱性情報とソフトウェア情報を突き合わせてアクセス制御ポリシーを決定する影響算出部，必要に応じて該当機器のネットワークのアクセス制限を行うネットワーク制御部の 4 つの部門で構成されている．

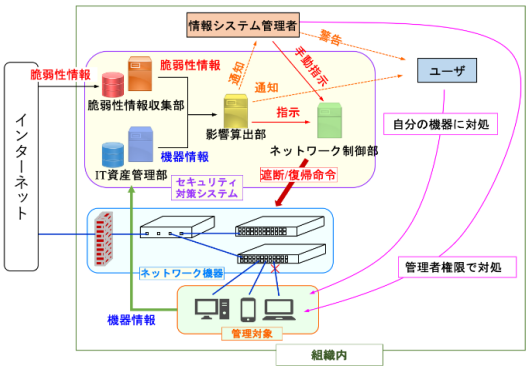

図 1　BEYOND 全体構成図

３．影響算出部の要件

影響算出機構に求められる要件を以下に示す．

① 脆弱性を持つソフトウェアの検出

脆弱性情報収集部 DB と IT 資産管理部 DB に共通に含まれるソフトウェアを探す．発見した場合は，該当ソフトウェアのバージョンが脆弱性を持つバージョンの範囲内か確認する．

② アクセス制御ポリシーの決定

該当機器のサービス情報を取得し，該当脆弱性の深刻度を取得する．サービス情報と脆弱性の深刻度を用いてアクセス制御ポリシーを決定する．

③ 必要に応じた通知

機器のネットワークのアクセス制限を行う場合は，ネットワーク制御部へ，該当機器の MAC アドレス，IP アドレス，アクセス制御ポリシーを通知する．同時に，機器の所有者とシステム管理者へ，機器のアクセス制御ポリシー，脆弱性の概要，脆弱性の対策情報を通知する．アクセス操作を行わない場合は，機器の所有者とシステム管理者へ注意喚起を促す通知を行う．なお，この機能は現在要件定義の段階であり，実装できていない．

４．影響算出機構

3 節で示した影響算出部の要件について，以下の手法にて実装した．

① 脆弱性を持つソフトウェアの検出

脆弱性を持つソフトウェアを検出する手法として，IT 資産管理部 DB に登録されているソフトウェア全体を検査し，脆弱性を持つソフトウェアがインストールされている機器を特定する方式と，機器にインストールされているソフトウェア一覧を取得し機器ごとにスキャンを行う方式の 2 つがある．前者の方式は，日付を指定することで更新のあった脆弱性情報やソフトウェア情報のみを指定できるため，日常的な脆弱性対策のスキャンを行う場合に使用する．後者の方式は，組織内のネットワークに初めて接続し，初回の脆弱性のチェックを行う場合や，脆弱性を含むソフトウェアが存在していた機器が脆弱性の問題を解決しスキャンを行う場合など，任意の機器を指定しスキャンを行う必要がある場合に使用する．本研究では，組織内のインターネットに初めて接続する機器を想定し，後者のスキャン方式にて脆弱性の検査を行う手法で実装した．

脆弱性情報収集部 DB と IT 資産管理部 DB からそれぞれソフトウェア名とバージョン番号を取得する．脆弱性情報収集部 DB から CPE 情報，脆弱性を含むバージョンの範囲，CVE-ID を取得する．CPE 情報をコロンで分割し，該当部分を取得することでソフトウェア名を抽出する．IT 資産管理部より，機器 ID を取得する．機器 ID に紐付くソフトウェア情報とバージョン情報一覧を取得する．ソフトウェア情報から拡張子などを消去し，ソフトウェア名のみを抽出する．バージョン情報から，エポック番号やリリース番号を消去し，バージョン番号のみを抽出する．抽出したソフトウェア名同士を比較し，一致するものを探す．発見した場合は，そのソフトウェアのバージョンが脆弱性を含むバージョンの範囲内であるか確認する(図 2 水色，赤色，緑色の線)．

② アクセス制御ポリシーの決定

脆弱性の深刻度と，機器のサービス情報に従って，表 1 に示す 4 パターンの中から選択する．表 1 について，a は脆弱性の深刻度が閾値未満である場合に採用するパターンである．b は Web サービスなど，外部に向けたサービスを提供しており外部と継続的に通信する必要のある場合に採用するパターンである．内部の機器と通信することができないため，組織内の他の機器に対する攻撃の予防や攻撃の被害拡大を防止できる．c は DB やファイルサーバなど内部に向けたサービスを提供しており内部と継続的に通信する必要のある場合に採用するパターンである．外部からの攻撃の予防や情報資産の外部流出を予防する効果がある．d はサービス提供のないクライアントマシンや，内部と外部の両方にサービスを提供しているサーバに採用するパターンである．インターネットのアクセスを断つことにより，攻撃を受ける可能性や情報資産が流出する可能性を無くすことができる．利便性やアクセシビリティが

低下するが，脆弱性による被害を防ぐことができる．

アクセス制御ポリシーを決定するために，脆弱性の深刻度とサービス情報を取得する．①で取得した CVE-ID を JVN-ID に変換し，脆弱性の深刻度を登録しているテーブルに対して JVN-ID で検索を行い，CVSS スコアを取得する(図 2 オレンジ色，紫色の線)．サービス情報を登録しているテーブルに対して機器 ID で検索を行い，サービスの提供範囲を取得する．検索の結果，サービス情報がない場合は，その機器はクライアントマシンと判定する．機器がクライアントマシンである場合は脆弱性の深刻度のみで判定を行う．深刻度が閾値未満の場合は表 1 の a を選択し，閾値以上の場合は d を選択する．サービス情報がある場合は，サービスの提供範囲を参照する．外部に対してサービスを提供している場合は b を選択する．内部に対してサービスを提供している場合は c を選択する．内部と外部の両方にサービスを提供している場合は d を選択する．

本研究では閾値を 4.0 とした．PCI-SSC[1]が策定した PCI-DSS の仕組みにて同値を採用しており，それを参考にした．さらに，組織や部署によってはセキュリティ対策を厳しく制限し，閾値を高めて運用したい場合が考えられる．そのため，閾値をシステム管理者が変更できるように，別のファイルから閾値を読み込む手法にて実装した．

表 1　アクセス制御ポリシーのパターン

パターン	アクセス制御ポリシー
a	何もしない
b	内部の通信のみを切断
c	外部の通信のみを切断
d	内部の通信と外部の通信を切断

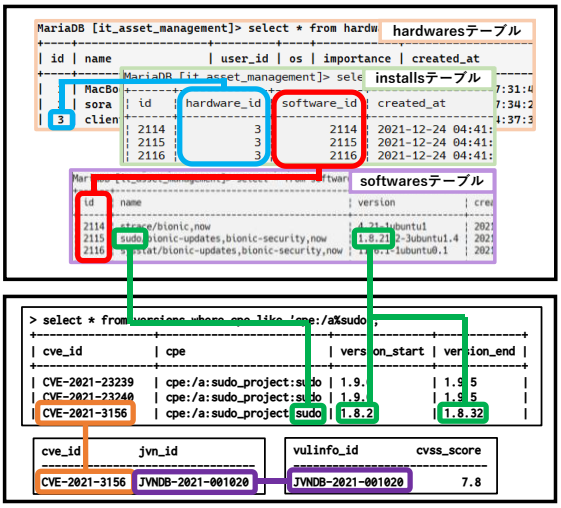

図 2 脆弱性の検出及び深刻度の取得

5．評価

開発した影響算出機構の脆弱性を持つソフトウェアの検出機能に関して機能評価を実施した．使用したデータに関して，今回は 2021 年 12 月時点で脆弱性情報収集部 DB と IT 資産管理部 DB に登録されているものを使用した．クライアントとして利用することを想定して作成された Cent OS の仮想マシンを用いた．この機器には 399 件のソフトウェアが登録されている．脆弱性情報に関して，脆弱性情報収集部が収集した 1999 年 12 月から 2021 年 12 月までの約 166 万件を使用した．作成した影響算出部のプログラムを実行した結果を図 3 に示す．表示内容は，上から，機器 ID，検出の結果，CVSS スコアの一覧，CVSS スコアの最大値，サービス情報，機器の利用目的，アクセス制御ポリシーの結果である．検出の結果について，左から，該当脆弱性の CVSS スコア，脆弱性があるソフトウェア名，そのソフトウェアのバージョン，脆弱性を含むバージョンの最小値，脆弱性を含むバージョンの最大値である．この機器からは 5 件の脆弱性を含むソフトウェアが検出された．なお，この中に python が含まれている．IT 資産管理部 DB に登録されている python は python2 系であるが，脆弱性情報収集部 DB に登録されている python は python3 系である．現在の実装では，2 系と 3 系の違いを判断することができない．

検出された 5 件に関して，IT 資産管理部 DB と脆弱性情報収集 DB にはそれぞれ図 4 に示す内容で登録されている．IT 資産管理部 DB に登録されているソフトウェア情報は，赤枠で示す通り拡張子が含まれており，バージョン情報は紫枠で示す通りエポック番号やリリース番号が含まれている．脆弱性情報収集部 DB に登録されている脆弱性情報は赤枠で示す通りソフトウェア名が CPE 情報の中に登録されている．それぞれの DB から取得したソフトウェア情報，脆弱性情報を利用して，脆弱性を含むソフトウェアを検出できていることが確認できた．

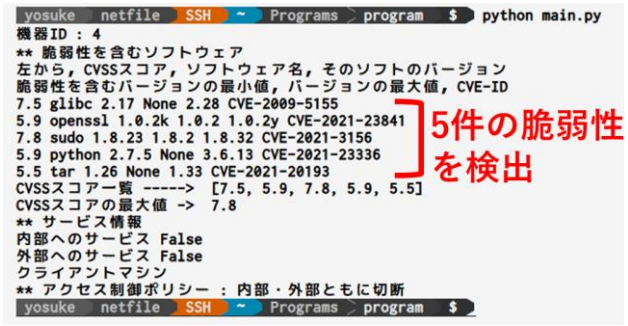

図 3　作成したプログラムの実行結果

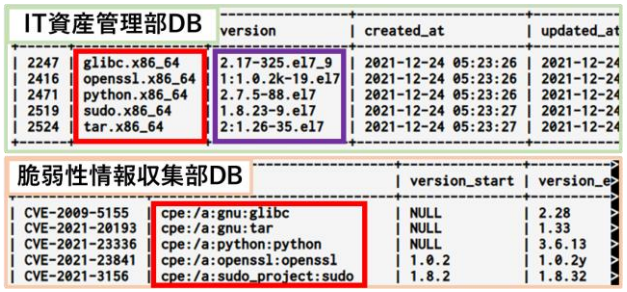

図 4　DB に登録されている内容

6．おわりに

開発している影響算出部の影響算出機構について述べた．現在，脆弱性を持つソフトウェアを検出する機能と，アクセス制御ポリシーを決定する機能の実装ができた．通知機能の実装は要件定義を行っている．今後の課題として，アクセス制御ポリシーの妥当性の評価などを考えている．

参考文献

[1] PCI-SSC(Payment Card Industry Security Standards Council), “Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards”, https://www.pcisecuritystandards.org/ (2022 年 2 月 15 日閲覧).