脆弱性対策のためのセキュリティ保護システム“BEYOND”における更新支援機構の開発

最所研究室 18T313 衣川達

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．

BEYOND では，脆弱性を持つ機器をアクセス制御し，管理者や所有者へその旨を通知するが，脆弱性を解消する作業の方法が決まっていない．アクセス制御によって隔離された環境下では外部へ接続することができないため，パッチを適用することができず，更新が行われなくなる問題が発生する．その問題を解消するため，本研究では機器の更新を支援する更新支援部を開発することにした．

2. 本機構における要件

本機構が対象機器のパッチ適用を支援する要件として，以下の 3 点が挙げられる．

① 隔離された環境下でのパッチ適用

外部へのアクセスを禁止した環境では，パッチを入手できない．

脆弱性を持つソフトウェアに対するパッチを本機構が収集し，対象機器へ提供する．

② 更新手順の簡易化

パッチの適用には接続先設定の変更や更新後の状態を IT 資産管理データベースへ反映させる操作が必要となる．煩雑な手順は更新の実行が遅れる，またはパッチの適用が行われなくなる原因となるため，手順を簡易化する必要がある．

③ 発見された脆弱性を持つソフトウェアの特定

ソフトウェアを更新すると，仕様の変更などにより動作に支障が出る場合がある．不必要なソフトウェアを更新すると，動作不良を起こす可能性が高まるため，古いバージョンであっても脆弱性がなければ更新を行わず，必要最低限の更新のみを行う．

以上の要件を満たす機構を開発する．

3. 更新支援部の概要

本研究で使用する BEYOND の概要を図 1 に示す．BEYOND では，脆弱性情報収集部がインターネットから脆弱性情報を収集し，IT 資産管理部が組織内の機器から機器情報を収集する．それらの情報から影響算出部で組織内の機器が持つ脆弱性を検知する．

本機構の概要を図 2 に示す．

本機構では，組織内部でのみ接続できるサーバにパッチを用意し，外部ネットワークとの通信が遮断された状態で脆弱性を解消する．

① 影響算出部からアクセス制御を行った機器の情報が通知
② 脆弱性を持つソフトウェアの情報を IT 資産管理データベースへの問い合わせ
③ データベースで取得した情報から，更新を実行するスクリプトを作成し，対象機器へ公開
④ 取得するためのファイルパスは影響算出部へ通知
⑤ 機器の所有者には制御内容と更新方法を通知
⑥ 所有者は通知された情報を基にスクリプトを取得，実行することでソフトウェアの更新
⑦ 更新後のソフトウェアの情報が更新支援部へと送信
⑧ 更新支援部から IT 資産管理部へとソフトウェアの情報を中継
⑨ IT 資産管理データベースへと反映

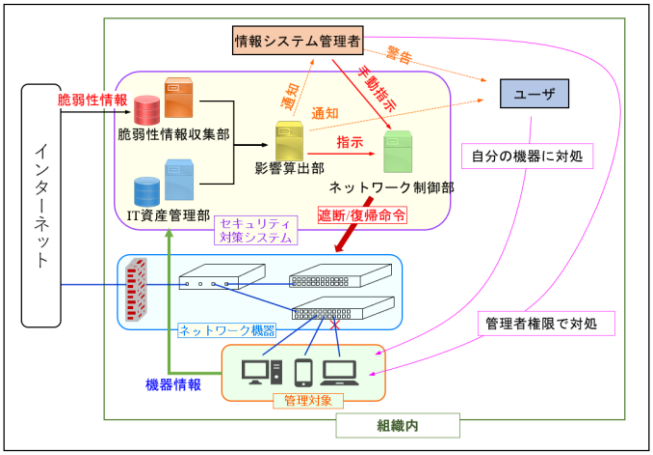

図 1 BEYOND の概要

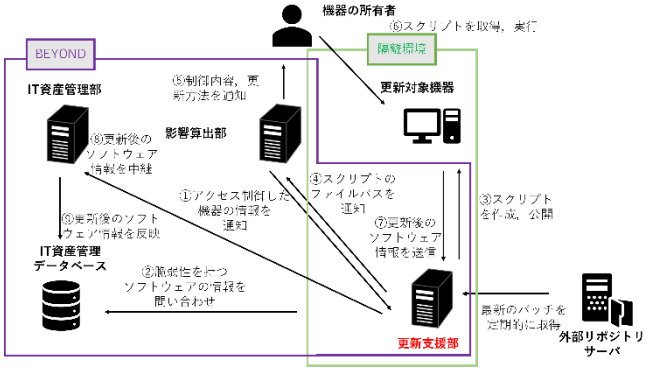

図 2　開発支援機構の概要

4.　更新支援部の実装

本研究では，Linux を対象にして開発を行った．

4.1　ファイル配布サーバ

パッチの取得には apt-mirror というツールを用いて外部の apt リポジトリサーバをミラーリングする．cron を用いて apt-mirror を定期的に実行することで最新のパッチを取得する．配布には web サーバを用い，HTTP 通信によって行う．生成したスクリプトの配布もこのサーバを用いる．

4.2　更新ソフトウェア特定機能

本機能では，影響算出部から受け取った機器 ID を基に IT 資産管理データベースから脆弱性を持つソフトウェアの情報を取得する．データベースにはインストールされているソフトウェアの情報とインストールされている機器 ID の情報が入っているテーブルと，脆弱性を持つソフトウェアの ID とインストールされている機器の ID が入っているテーブルがある．この 2 つのテーブルを機器 ID で結合し，更新が必要なソフトウェアの名前を抽出する．apt で指定するソフトウェア名にするため，抽出したソフトウェア名の整形処理を行う．

4.3　スクリプト生成機能

スクリプトの生成には Python を用いる．スクリプトのテンプレートを用意し，接続先の URL，機器の OS を示す Ubuntu の開発コード，更新ソフトウェア特定機能で取得したソフトウェア名をテンプレートの変数に挿入する．スクリプト生成のトリガーや更新後のソフトウェア情報の中継は webAPI を実行する．

5.　更新支援部の評価

本節では，本機構の機能評価を行った結果を示す．外部へアクセスできない状態で更新が可能であるか，スクリプト実行時に更新が必要なソフトウェアのバージョンが上がっているか，更新が不要だが古いバージョンであるソフトウェアが更新されていないかで評価する．評価対象とする機器の OS は Ubuntu20.04 である．インストールされているソフトウェアは mysql と apache の脆弱性を持つバージョン，fakeroot と expat の脆弱性は持たないが最新ではないバージョンである．その他の初期からインストールされているソフトウェアは全て最新の状態にした．

影響算出部により脆弱性が検出されたことをトリガーとしてスクリプトが生成され，評価対象の機器でスクリプトを実行すると mysql と apache のみが更新されたことを確認できた．本実験で生成したスクリプトを図 4 に示す．このスクリプトでは，apt がファイルを取得するための接続先の設定を変更する部分，IT 資産管理データベースから抽出したソフトウェア名を用いて更新を実行する部分，IT 資産管理部で使用されているプログラムを用いて更新後のソフトウェア情報を送信する部分で構成されている．

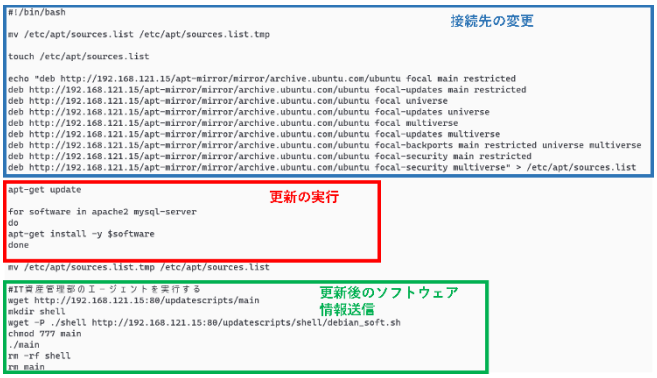

図 3　生成したスクリプト

6.　おわりに

本稿では，セキュリティ保護システム“BEYOND”においてソフトウェアの更新を支援する機構の開発を行った．本機構を開発したことにより，BEYOND によってアクセス制御された機器に対して生成したスクリプトを実行することで更新を可能とした．

今後の課題として，Linux の他の OS や Windows，mac への対応やパッチ適用前に試験環境を用意し，正常に動作するかを検証する機能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