2X-04

脆弱性情報を利用したセキュリティ対策支援システムにおけるサービス情報管理のための IT 資産管理機構の開発

西岡 大助† 楠目 幹† 竹原 一駿† 細川 洋輔† 喜田 弘司† 最所 圭三†
香川大学†

1. はじめに

近年，脆弱性を利用したサイバー攻撃による被害が深刻な問題となっている．システムが持つ脆弱性に対する根本的な対策は，パッチを当てることであり，パッチが配布されるまでの間はシステムを停止させるなどの対策をとるしかない．そこで，我々は公開された脆弱性情報と組織内のネットワークに接続された IT 資産情報に基づいて，脆弱性を持つ機器のネットワーク制御を行うセキュリティ対策支援システムの開発を行っている[1]．当システムを用いることにより，脆弱性のある機器を速やかに検出し，自動的にネットワークから遮断・隔離することが可能である．

しかしながら，管理している機器(管理対象機器)が提供しているサービス次第では，脆弱性が検出されても即座に停止することが困難な場合がある．これまで開発してきた IT 資産管理機構[2]で収集した情報では，即座に停止できるかどうかの判断ができず，それには提供しているサービスの情報が必要であると考えた．本稿では管理対象機器が提供しているサービス情報を管理するための機能を提案し，管理対象機器の管理者がサービス情報を登録するためのインタフェースについて述べる．

2. セキュリティ対策支援システム

我々のセキュリティ対策支援システムは，脆弱性情報収集部，IT 資産管理部，影響算出部，ネットワーク制御部によって構成される(図 1)．

①脆弱性情報収集部にてインターネット上に公開されている脆弱性情報を収集しデータベース(以下 DB)化する．②IT 資産管理部にて組織内のネットワークに接続されている機器情報を取得し DB 化する．③影響算出部にて，収集された情報から脆弱性の対策を算出し，④即座な保護が必要である場合はネットワーク制御部へ指示を出す．⑤ネットワーク制御部では，与えられた指示に基づいて，脆弱性を持つ機器に対して外部および内部ネットワークからの遮断，検疫ネットワークへの隔離，復帰などのアクセス制御を行う[3]．

本研究で開発を行っている IT 資産管理機構は，IT 資産管理部で組織内の機器情報を収集するシステムである．情報の取得には Web とエージェントと呼ばれるソフトウェアを用いる．組織のネットワークの利用者(ユーザ)は初めてネットワークに接続する際に，検疫ネットワークにて機器のハードウェア情報を登録し，エージェントをインストールする．ハードウェア情報として，脆弱性が発見された際にネットワーク制御を行うための情報である，機器の MAC アドレス，IP アドレスを登録する．エージェントは管理対象機器にインストールされているソフトウェアの名前とバージョンを取得し，IT 資産管理機構に送信する．IT 資産管理機構は，送られてきたソフトウェア情報を DB に登録し，そのソフトウェアが安全であれば，ユーザに対して内部ネットワークの利用を許可する．

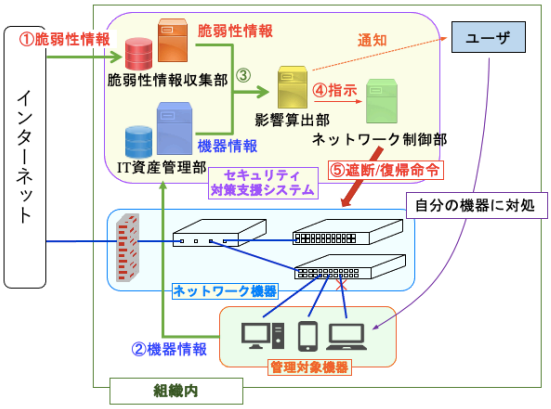

図 1. セキュリティ対策支援システムの構成

3. サービス情報を用いたセキュリティ対策

2 章で述べた，従来の IT 資産管理機構で収集した情報を用いて，脆弱性の検出と脆弱性を持つ機器のネットワーク制御を行うことができた．しかしながら，サーバなどの外部にサービスやデータを提供している機器は，脆弱性が検出されても即座に停止することができない場合が多い．現在収集している情報だけでは，機器が提供しているサービスがわからず，停止の判断を行うことができないため，停止できない機器に対しての対策もできない．

上記の問題を解決するために，IT 資産管理部の機能を拡張し，管理対象機器のサービス提供の有無と提供している場合その詳細を収集できるようにする．収集する情報として，提供に使用しているソフトウェア，サービスの提供範囲，機器を停止できるか(停止できる期間)や IP アドレスの情報を集める．それにより，停止できる機器については機器へのアクセスを遮断，停止できない機器については公開範囲の制限を行う，または脆弱性を持つ機能のみを停止した

Development of IT Asset Management Mechanism for Service Information Management in Security Measure Support System Using Vulnerability Information
† Daisuke NISHIOKA, Motoki KUSUME, Ichitoshi TAKEHARA, Yosuke HOSOKAWA, Koji KIDA, Keizo SAISHO・Kagawa University

りするなどの対策が可能になる．ユーザには情報の登録を条件に，登録された IP アドレスでのサービス提供を許可する．これにより，組織内で提供されている全てのサービスの管理が可能になる．

例として大学の教務システムと研究室の Web サーバで脆弱性が見つかったことを想定した時の制御例を図2に示す．教務システムは外部に公開されており，大学の履修登録や成績登録を行うシステムであり，停止させると業務に影響が出るため停止できない．この場合，ファイアウォールで外部から遮断し，内部からのアクセスのみを可能にすることで，内部からの攻撃によるリスクはあるものの，リスクを最小限に抑えることができる．また，研究室の Web サーバは組織内のみに公開されており，サービスの緊急度は低いためいつでも停止可能である．この場合，研究室の Web サーバへのアクセスを完全に遮断することで，内部からの攻撃も完全に遮断する．

メンテナンスの時間や曜日を停止できる期間に指定することで，その期間のみネットワーク制御の方針を変えることもできる．また，サービス提供に使用する IP アドレスとポート番号を取得することで，ポート単位での制御も可能となる．

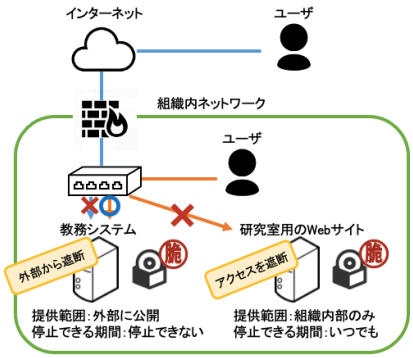

図 2. ネットワーク制御の例

4. サービス情報登録インタフェース

管理対象機器が提供するサービス情報を収集するために，Web で情報取得を行う機能を開発した．サービス情報を登録するためのインタフェースを図3に示す．提供する機器，使用するソフトウェアの項目はユーザの持つ機器情報から動的にメニューを作成する．サービス種別，提供範囲，停止できる期間については，運用の際に作成しておく．以下は，本稿で提案した対策を行う際に必要な情報である．

①使用するソフトウェア: 管理対象機器にインストールされているソフトウェアの一覧の中から，サービス提供に使用するソフトウェアを選択する．通常，サービスの提供には複数のソフトウェアを利用するが，その全てを選択することは困難であるため，Web サーバにおける httpd など，最も主要なソフトウェアのみを選択する．

②提供範囲: サービスの公開範囲を指定する．例えば，組織内部のみでの公開や，外部に公開するなどのパターンが考えられる．

③停止できる期間: サービスを停止することができるかどうか指定する．また，停止できない機器もメンテナンスのために停止する場合もあるため，その場合はメンテナンスの期間を指定する．時間での指定(◯◯時～△△時)，曜日での指定(◯曜日のみ)，年単位での指定(年間◯時間まで)などが考えられる．

④提供に使用する IP アドレスとポート: サービスの提供に使う IP アドレスとポートを指定する．インターネット上に公開するサービスはグローバル IP アドレス，組織内部のみに公開するサービスはプライベート IP アドレスを登録する．よく使われることが多いポート番号(HTTP:80 番など)はプルダウンメニューで用意しておき，それ以外の番号の場合は入力を促す．

5. おわりに

脆弱性情報に基づいたセキュリティ対策支援システムの開発を行っている．本稿では，開発している IT 資産管理機構におけるサービス情報管理機能について述べた． 今後は，セキュリティ対策支援システム全体を統合し，評価実験を行う．

参考文献

[1] 楠目幹，喜田弘司，最所圭三．“脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能の実装及び脆弱性評価機能の実装”, 電子情報通信学会技術研究報告, Vol.119, No.140, ISEC2019, pp.1-6, 2019

[2] 西岡大助，楠目幹，竹原一駿，喜田弘司，最所圭三．“脆弱性情報を利用したセキュリティシステムにおける IT 資産管理”，令和 2 年度電気・電子・情報関連学会四国支部連合大会講演論文集，pp.16-3,2020.

[3] 竹原一駿，楠目幹，西岡大助，喜田弘司，最所圭三．“脆弱性情報を用いたセキュリティシステムにおけるネットワーク制御機構の開発”，令和 2 年度電気・電子・情報関連学会四国支部連合大会講演論文集，pp.16-4,2020.