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に関する研究

16T286　竹原 一駿 （最所研究室）

近年，組織において，情報資産を管理する機器が増えている．それらの機器には脆弱性が存在することがあり，悪意を持つ者が修正パッチの適用前に攻撃することがある．その対策として，本研究では，発見した脆弱性を持つ機器をネットワークからの隔離などの制御システムを構築する．

1　研究背景

近年，ゼロデイ攻撃と標的型攻撃を組み合わせたサイバー攻撃が増加している [1]．通常，脆弱性への対処は，ベンダーにより配布されるパッチの提供を待つ必要がある．攻撃者は，この期間に，発見された脆弱性を悪用して攻撃を行う．攻撃を受けた機器が，ネットワークを通じた，情報資産の流出や改竄などを行う可能性がある．しかし，公開されたすべての脆弱性に対して，対策を行うことは難しく，機器が提供するサービス次第では，即座にシステム停止などの対策が難しい．

一方，情報技術の発展により，企業などでは，社員が自身の情報機器を持ち込み，職務に用いる取り組み，BYOD(Bring Your Own Device) が増えている [2]．これらの機器は，組織のネットワークに接続して使用される．

このような状況で，組織のネットワークに存在する情報資産を守らなければならない．従来のゼロデイ攻撃への対策では，パッチの配布に依存するため，ベンダーによるパッチ配布までは，対策が取れない．そのため，組織内の機器に対して，パッチの配布に依存せず，脆弱性情報を基に対策を行うセキュリティシステムの構築が望まれる．

2　研究目的

我々の研究室では，公開された脆弱性情報をデータベースにて管理する機構 [3] や，組織のネットワークに接続している機器の構成やソフトウェアなどの情報をデータベースにて管理する機構 [4] の研究を行っている．これらを用いて，収集された脆弱性情報と機器情報を基に，脆弱性が存在する機器に対して，アクセス制御を行うことで，被害の拡大防止を目的とするセキュリティシステムの構築を行う．本研究では，このセキュリティシステムを構成する，脆弱性が存在する機器のアクセス制御を行うネットワーク制御機構の開発を目的とする．

3　セキュリティシステムの構成

本システムは，機器情報収集部，IT 資産管理部，影響算出部，ネットワーク制御部で構成される．全体のシステム構成を図 1 に示す．

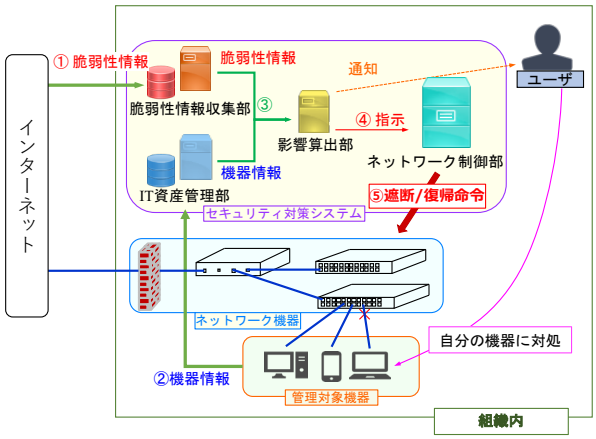

図 1: 全体のシステム構成

脆弱性情報収集部

JVN iPedia にて公開された脆弱性情報を基に，対象製品やソフトウェア，ベンダ，深刻度をデータベースに格納する．公式ベンダなどのパッチ配布に依存せず，公開後速やかに脆弱性情報を一元に集約する．

IT 資産管理部

組織に持ち込まれた個人のパソコンやサーバなどの機器における，所有者，MAC アドレス，OS などをデータベース上で一元に管理する．エージェントを用いることで，定期的に機器情報を収集する．また，機器に保存する個人情報に応じて，重要度を登録する．

影響算出部

機器によっては，組織にとって，重要な情報を保存しており，重要度が高い機器がある．これらの機器は，ゼロデイ攻撃から優先的に保護しなければならない．また，脆弱性によっては，遮断や隔離などの対策が必要がない可能性がある．そこで，脆弱性情報収集部に

よる脆弱性の深刻度と，IT 資産管理部による持ち込み者の重要度を基に，該当機器が接続するネットワークをどのように制御するか判定する．判定のパターンの一例としては，表 1 が考えられる．

表 1: 遮断の判定パターン例

重要度 \ 深刻度	高	低
高	遮断する	遮断する
低	遮断する	遮断しない

4　ネットワーク制御部

4.1　概要

本研究で構築する，セキュリティシステムにおけるネットワーク制御機構について述べる．ネットワーク内において，機器は，Firewall(以下:FW)，L2 スイッチに接続されている．影響算出部から，該当機器の制御方針と MAC アドレスを与えられると，それに応じて遮断や隔離を行う．

4.2　外部ネットワークとの遮断と復帰

脆弱性による攻撃を防ぐために，外部ネットワークから遮断する．該当機器の MAC アドレスより，IP アドレスを得る．該当機器に固定 IP アドレスが振られている場合は，IT 資産管理データベースより，IP アドレスを取得する．動的 IP アドレスでは，MAC アドレスを基に，DHCP サーバより IP アドレスを検索する．該当の IP アドレスを持つ機器と外部ネットワークとの通信を遮断するルール (遮断ルール) を生成する．FW に対して遮断ルールを適用する．それにより，FW より外部とのネットワークを遮断する．復帰時には，遮断ルールの削除を行う．

4.3　内部ネットワークとの隔離と復帰

該当機器による，内部ネットワークに存在する他の組織の機器への通信を遮断するために，該当機器を内部ネットワーク検疫ネットワークへ隔離する．隔離には，VLAN を用いる．L2 スイッチに保存されている，“FDB”(ForwardingDataBase) を用いることで，現在接続している機器の MAC アドレスと，接続ポートの番号を取得できる．該当機器の MAC アドレスを基に接続しているポート番号を得る．L2 スイッチに命令し，接続しているポート番号を検疫ネットワークに所属させることで，内部ネットワークから隔離する．復帰時には，ポートを内部ネットワークに所属させる．

4.4　接続ポートの監視と追従

所有者が，機器の使用中に，内部ネットワークから隔離されたことに気づかず，L2 スイッチの別のポートへ接続することが考えられる．そこで，FDB を用いて，該当機器の MAC アドレスを監視することで，接続ポートの変更を検出する．そして，変更前のポートを内部ネットワークに復帰，変更後のポートを検疫ネットワークに隔離する．これにより，概要機器の接続は常に検疫ネットワークに隔離される．以上の実行結果を図 2 に示す．

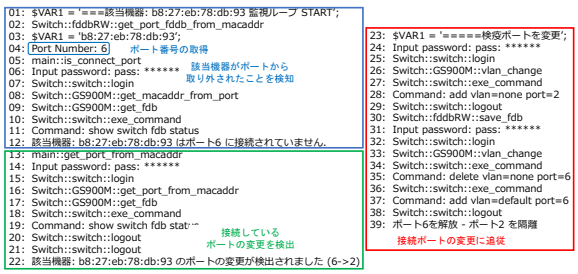

図 2: ポートの監視と追従する実行結果

5　おわりに

本稿では，開発した，脆弱性情報を用いたセキュリティシステムにおける，ネットワーク制御部について述べた．

今後の課題としては，脆弱性解決後の復帰と，無線 LAN 環境への対応が考えられる．IT 資産管理部や影響算出部は，内部ネットワークへ設置される．そのため，該当機器が，検疫ネットワークに隔離された後に脆弱性の対応を行っても，その情報を伝える手段が無い．また，近年は無線 LAN 環境を提供する組織や，無線 LAN 前提で機器を運用することも少なくない．今後は，以上の実運用面における課題を検討する．

参考文献

[1] “修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について：IPA 独立行政法人情報処理推進機構”. https://www.ipa.go.jp/security/virus/zda.html. 2019/09/14.

[2] “BYOD とは？コスト削減とセキュリティ対策などのメリットデメリットについて解説”. https://orange-operation.jp/posrejihikaku/workstyle/12301.html. 2019/09/15.

[3] 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設計”. 電子情報通信学会技術研究報告, Vol. 119, No. 140, pp. 1–6, 2019.

[4] 西岡大助. “BYOD に対応した IT 資産管理システムの開発”. 学士論文, 香川大学, 2020.