様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １８ 日現在

機関番号：８２６３６
研究種目：若手研究(B)
研究期間：2017～2019
課題番号：１７Ｋ１２６９９

研究課題名（和文）端末及びネットワーク機器の脆弱性自動監視・管理技術に関する研究開発

研究課題名（英文）Automated vulnerability monitoring and management techniques for networked computers

研究代表者

高橋　健志（Takahashi, Takeshi）

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所サイバーセキュリティ研究室・研究マネージャー

研究者番号：５０６００１６０

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究では、フォーマットの異なる複数のオンラインデータベースの情報を連携し、脆弱性管理の自動化技術を検討した。具体的には、フォーマットの異なる情報を連携する技術、各端末内にインストールされているソフトウェア情報をユニークな識別子に自動変換する技術、その識別子を用いて関連する脆弱性情報を取得する技術、その脆弱性の深刻度に応じてイントラネット上のスイッチの設定を動的に変更する技術を構築した。これらを連携することにより、IT資産の一覧情報管理、脆弱性の検知、初動対応の自動化を自動にて実現する技術を構築した。

研究成果の学術的意義や社会的意義
サイバースペースが社会的インフラになった今日では、サイバーセキュリティの担保はすべての組織、また個人にとって、必要不可欠である。しかしながら、必要なオペレーションをすべての組織で実施するには人的リソースに課題があり、自動化することが求められている。特に、本研究では、脆弱性管理というセキュリティオペレーションの一つに着目し、その自動化の実現可能性を示すことに成功した。

研究成果の概要（英文）：In this study, we proposed a technique that links online databases with different format, with which we introduced a technique that automates vulnerability management operations inside an organization. In particular, we constructed a technique that discovers and links various information with different format, a technique that derives a unique identifier for each of the assets installed inside terminals, a technique that locates vulnerability notes relevant to the assets, and a technique that changes configuration of network switches on the Intranet based on the severity of the vulnerability. With these techniques, we demonstrated the feasibility of automating the maintenance of asset information list, detection of vulnerabilities, and automated initial countermeasures.

研究分野：セキュリティオペレーションの自動化

キーワード：サイバーセキュリティ　オペレーション自動化　脆弱性管理　資産管理　情報検索　オントロジー

１．研究開始当初の背景

セキュリティ対策の重要性は強く認識されつつあるが、それを実施するのに十分な人材の質・量を確保できず、セキュリティ対策の実施が不十分な組織が多数存在する。今後の人材育成も重要であるものの、時間的及び予算的制約などから、現時点では各組織の中ではセキュリティ技術者の数をなるべく増やさずにセキュリティ対策を効率化する必要があり、セキュリティ対策の自動化技術の研究開発が注目されている。本問題は学術界だけでなく産業界でも強く課題認識されており、各種学会や IETF などの標準化団体において、学術界と産業界の双方からの参加者が活発に議論を重ねているのが研究開発当初の状況である。

２．研究の目的

本研究では、セキュリティ対策の自動化の中でも特に脆弱性情報の蓄積・管理と活用に主眼を置き、各種脆弱性情報の中からシステム管理者が把握すべきもののみをリアルタイムで特定・伝達する技術を検討する。本分野においては、オンラインのオープンな脆弱性データベースがいくつか提供され始めてきているものの、それを活用したセキュリティ管理・対策の自動化については、未だ発展途上の状況にあり、特に、フォーマットの異なる複数のデータベースの情報を活用した手法は、現時点では提供されていない。また、いくつかの脆弱性管理商品が存在しているものの、それらは人的資源により構築した各社独自のデータベースを活用しており、より広い情報を活用・再利用する技術、また人的資源への依存を最小化する技術が求められている。

３．研究の方法

本研究のアプローチは、オープンな各種脆弱性情報を監視すると同時に自組織の IT 資産情報を監視し、その双方をリアルタイムかつ自動的に紐づけられる点に特徴がある。また、その情報とポリシーに従い、セキュリティ対策の初動対応を実現する。具体的には、情報とポリシーに従い、IT 資産のセキュリティ状況を把握し、状況に応じたシグナリングを SDN 技術を用いて実施することで、組織内のネットワーク機器の設定を更新し、初動対応を実現する。

４．研究成果

本研究ではフォーマットの異なる複数のオンラインデータベースの情報を連携し、脆弱性管理の自動化技術を検討した。具体的には、フォーマットの異なる情報を連携する技術、各端末内にインストールされているソフトウェア情報をユニークな識別子に自動変換する技術、その識別子を用いて関連する脆弱性情報を取得する技術、その脆弱性の深刻度に応じてイントラネット上のスイッチの設定を動的に変更する技術を構築した。これらを連携することにより、IT 資産の一覧情報管理、脆弱性の検知、初動対応の自動化を自動にて実現する技術を構築した。上記のそれぞれについて、以下に報告する。

(1) フォーマットの異なる情報を連携する技術

セキュリティオペレーションに必要な情報は、その情報の種別ごとに異なるオンラインレポジトリにて提供され始めている。現時点ではそれらの情報を手動でオペレータが活用している事例が多いものの、これらを連携することにより、セキュリティオペレーションの自動化を実現していくことを目指している。そのため、これらのオンラインデータベースを連携し、必要な情報を発見できる技術を構築した。具体的には、これらのオンラインレポジトリに対し定期的にその情報を問い合わせ、そのインデックスを集約し、同時にスキーマの異なるオンラインレポジトリ群を横断検索できる技術を構築した。本成果は研究成果発表[1]にて公開済みである。

(2) 各端末内にインストールされているソフトウェア情報をユニークな識別子に自動変換する技術

脆弱性管理を実現するためには、まずは組織内の各端末にインストールされている OS を含むソフトウェア情報の一覧を取得する必要がある。そのため、各端末にて動作する Agent ソフトを構築した。本 Agent ソフトは主に Windows 端末内のレジストリを読み込み、インストールされ

ているソフトウェア情報の一覧情報を収集する。それらの情報はアセット管理サーバに集約されるが、そのサーバ上にて CPE-ID と呼ばれるソフトウェアの共通識別子に変換する。その変換を実施するにあたり、公式辞書、準公式辞書、プライベート辞書を用意し、収集したソフトウェア情報(自然言語で記述)と突き合せることにより、最も近しい CPE-ID を選択する技術を構築した。

(3) 関連する脆弱性情報を取得する技術

脆弱性の存在は NVD などのオンラインレポジトリに公開されているが、そのレポジトリ上には、影響を受けるソフトウェア識別子の一覧が CPE-ID のリストという形式で記載されている。そのため、上記項目にて決定した CPE-ID と突き合せることにより、関連する脆弱性情報を取得する技術を構築した。CPE-ID にはワイルドカード表記なども許容されているため、様々な表現の揺らぎにも対応できる情報引き当て方式を実装した。

(4) 脆弱性の深刻度に応じてイントラネット上のスイッチの設定を動的に変更する技術

イントラネット上に脆弱性を持つソフトウェアが上記により検知された際には、その脆弱性の深刻度に応じて、イントラネット上のスイッチのフィルタリングルールを変更する技術を構築した。脆弱性の深刻度は、CVSS スコアを用い、ある一定以上のスコアを持つ脆弱性の存在が発見された際には、Ansible にて記述した設定情報をネットワーク上のスイッチに配信することにより、スイッチの設定を変更することに成功した。これにより、脆弱性のあるソフトウェアを持つ端末への通信をブロックする等の初動対応が自動的に実装可能となった。

(5) 上記の技術群を連携して IT 資産の一覧情報管理、脆弱性の検知、初動対応の自動化を自動にて実現する技術

上記のすべての技術を連動することにより、IT 資産の一覧情報管理、脆弱性の検知、初動対応の自動化について、そのフィージビリティを確認した。その結果は、研究成果発表[2][3]にて公開済みである。

研究成果発表

[1] T.Takahashi, B.Panta, Y.Kadobayashi, K.Nakao, "Web of Cybersecurity: Linking, Locating, and Discovering Structured Cybersecurity Information," International Journal of Communication Systems, Wiley, December, 2017.DOI:10.1002/dac.3470
[2] T.Takahashi, H.Kanehara, M.Kubo, N.Murata, D.Inoue, "Toward Automated Vulnerability Handling," Coordinating Attack Response at Internet Scale Workshop, Internet Society, February, 2019
[3] 高橋健志, 牛込龍太郎, 鈴木未央, 井上大介, “脆弱性情報の自動監視に基づく警告・初動対応自動化技術の構築,”ICSS2019-93, 信学技報, 2020 年 3 月

5．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

1．著者名 Takahashi Takeshi、Panta Bhola、Kadobayashi Youki、Nakao Koji	4．巻 31
2．論文標題 Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information	5．発行年 2017年
3．雑誌名 International Journal of Communication Systems	6．最初と最後の頁 e3470～e3470
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/dac.3470	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　1件）

1．発表者名 高橋健志，牛込龍太郎，鈴木未央，井上大介
2．発表標題 脆弱性情報の自動監視に基づく警告・初動対応自動化技術の構築
3．学会等名 電子情報通信学会情報通信システムセキュリティ研究専門委員会
4．発表年 2020年

1．発表者名 Takeshi Takahashi, Hideaki Kanehara, Masaki Kubo, Noboru Murata, Daisuke Inoue
2．発表標題 Toward Automated Vulnerability Handling
3．学会等名 Coordinating Attack Response at Internet Scale Workshop（国際学会）
4．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考