6-2　ネットワーク上の IT 資産に関する脆弱性情報自動配信システム

高橋健志

各組織は常日頃から IT 資産の脆弱性を管理する必要があるものの、そのために必要なリソースを十分割けない組織も多い。そこで本稿では、脆弱性情報のうちそれぞれの組織に関連するもののみをリアルタイムに自動取得する方式を提案する。本方式は IT 資産情報を識別子へと自動変換し、それを用いて必要な脆弱性情報を取得するところにその特徴がある。また、プロトタイプ実装も紹介し、今後の発展に向けた課題についても議論する。

1　はじめに

組織内のセキュリティを維持するためには、管理ネットワーク上の IT 資産の抱える脆弱性について、なるべくリアルタイムにて把握する必要がある。しかしながら、そのような対応を人手で実施するにはかなりの労力を要し、十分な人的リソースを割くことが困難な組織も多く存在するのが現状である。脆弱性の有無をリアルタイムで把握するどころか、自組織に必要な脆弱性情報にリーチできていない組織も多く存在する。また、脆弱性情報は常にその更新に気を配る必要があるが、それができていない組織は更に多い。

脆弱性管理をするためには、まずは、自組織内に存在する IT 資産を把握する必要がある。IT 資産の洗い出しは ISMS などでもその重要性が明言されているため、大企業などでは対応できている組織も多く存在するが、小規模組織などでは対応が後手に回っている。

また、一度把握したとしても、時間の経過とともに変化する IT 資産の変化を、本来リアルタイムで追従できることが望ましい。これらの IT 資産管理、また付随する脆弱性管理について、人的リソースを増やすことなく自動化により実現する技術の発展が求められている。

1.1　関連研究

提案方式は、各種関連研究の成果を活用し、本稿の問題認識である組織内での IT 資産・脆弱性管理の省力化に貢献する。本節では、これらの関連研究の概略を紹介する。なお、詳細については文献 [1] の第 2 章、もしくはそれぞれの参考文献を参照いただきたい。

a）IT 資産管理ツール : IT 資産情報を収集するツールは既に様々なものが存在している。情報収集源としてよく用いられるもののひとつにレジストリ情報があるが、これは OS 付属ツールにより収集可能である。Windows 8 付属の reg.exe はそのひとつであり、CUI にてレジストリ情報を収集可能である。また、Windows PowerShell にも Get-ChildrenItem というコマンドレットが用意されており、やはり CUI にてレジストリ情報を取得可能である。OS 付属ツール以外にも各種ソフトウェア管理ツールは存在し、それらの多くはレジストリ以外からも積極的に情報を収集する統合ツールである。

b）オープンな情報リポジトリ・スキーマ : 脆弱性情報については、いくつかの組織が蓄積した情報をオンライン・リポジトリという形で提供を開始している。それらのうち著名なものとして、NVD[2] や JVN[3] が存在している。また、それらのリポジトリをひとつの巨大なデータベースとして横断検索を実現する知識ベースを、筆者らは提案し、そのプロトタイプを構築してきた [1]。

c）情報スキーマ : 上述のリポジトリの多くは標準化された XML スキーマを利用して情報が記述されている。上述の NVD では、脆弱性情報を検索するひとつのキーとして、当該脆弱性が影響を及ぼす IT 資産 ID が CPE[4] 形式にて記載されている。IT 資産の ID は、CPE や SWID[5] といった規格が成立しており、それに準拠した ID リスト（= 辞書）も存在している。情報を蓄積するためのスキーマに加え、情報を交換するためのスキーマも規格化されており、例えばインシデント情報を共有するためのスキーマ IODEF[6] とその拡張技術 IODEF-SCI[7] が存在する。IODEF-SCI では各種 XML 情報を交換することが可能となる。

1.2　我々のアプローチ

様々な IT 資産情報収集ツールが存在するものの、

OS 付属ツールの reg.exe や PowerShell 以外の多くのものは proprietary なツールであり、また収集した情報に欠けている情報を補完する技術・情報についても proprietary なものが利用されている。さらには、保有する IT 資産の脆弱性情報の自動取得も、proprietary な脆弱性情報を利用している。proprietary な技術や情報を利用することにより、信頼性の低い情報の活用を避けることができるものの、ツール提供元が情報を準備・精査・提供しない限り、新たな IT 資産・脆弱性情報に対応することはできない。オープンな情報の流通が進み始めた現在、オープンデータを最大限利用することにより、情報のスケーラビリティを担保し、またシステムの仕様をすべて公開したフリーソフトを構築することにより、セキュリティ自動化に向けた活用を促進したいと考えている。

1.3　本稿の貢献

本研究ではオープンデータを用い、イントラネット管理の省力化をアセット管理と脆弱性管理の自動化により実現する。まず、アセット管理として、社内ネットワーク内のネットワーク情報、PC、スマートフォン等の IT 機器に関する情報を定期的に収集する。そして、様々なセキュリティ関連情報を蓄積している知識ベースに問い合わせることにより、収集した情報の ID 化・構造化を実施する。次に脆弱性管理として、社内ネットワークに存在している IT 機器に関しての脆弱性の有無を確認する。具体的には、収集した IT 資産情報の ID をキーに、知識ベース内に保存されている脆弱性情報の有無を確認する。対応する未対応の脆弱性情報が確認された際には、すぐに管理者へ警告メッセージを発信し、管理者の迅速な対応を可能とする。また、それと並行し、ネットワークが自律的に初動対応（Triage）を実施するアーキテクチャを考えているものは、本稿の範囲外とし、本稿では初期検討結果を共有するものとする。なお、信頼性が必要な情報については既存技術を併用することを考えており、提案システムは既存技術を補完するものであり、代替するものではない。

本稿の初期検討結果より、オープンな規格と情報を活用することで、リアルタイムに脆弱性の存在に対して警告を発することが可能であることを示す。これにより、組織内のセキュリティオペレーションの省力化が推進可能であることを示す。また、セキュリティオペレーションの自動化を目的とした各種情報スキーマ制定活動が盛んであるが、それらのスキーマを実際に用いた具体的な省力化ツールを構築することにより、これらの活動の重要性を明確化する。なお、本稿は著者の論文 [8] の要約であり、詳細については当該論文を参照いただきたい。

2　システムアーキテクチャ

提案システムは、常に IT 資産情報を確認し、その情報を ID に変換する。また、その ID を元に知識ベース内の脆弱性情報を問い合わせ、引き当たる脆弱性情報があった場合には警告を提供するものである。本節では、まず提案システムに必要なロールを定義し、次にそれらのロールが連携して動作するプロセスの概要を示す。

2.1　ロールモデル

図 1 に、提案システムの構成例を示す。提案システ

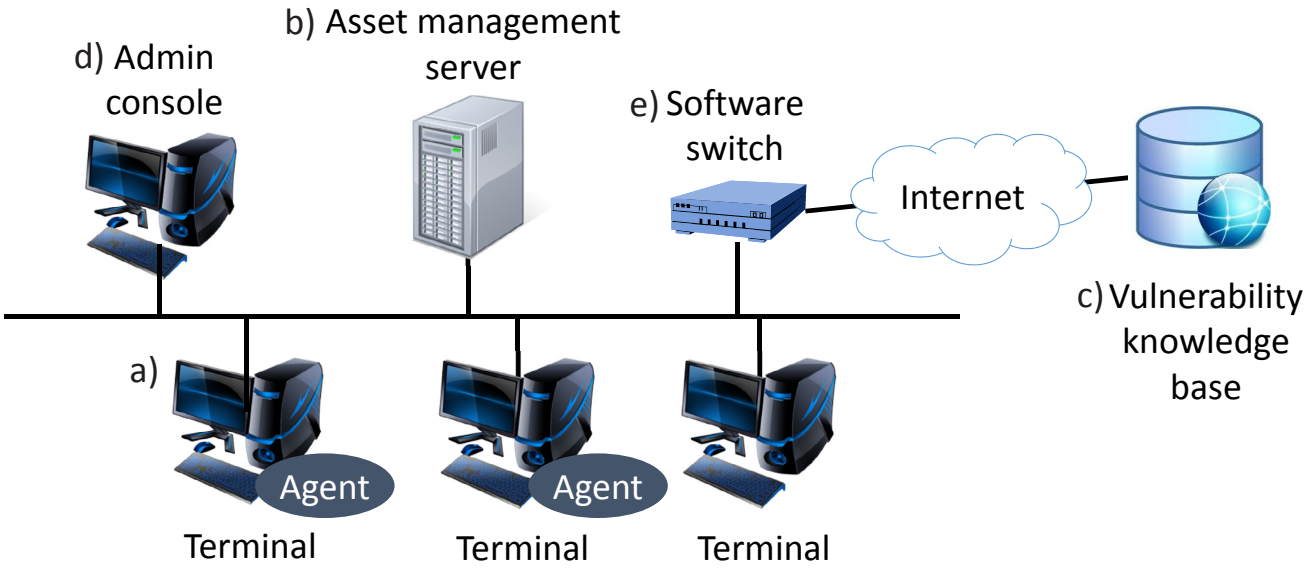

図 1　提案システムの構成例

ムには、端末、アセット管理サーバ、知識ベース、管理者端末、ソフトウェアスイッチという 5 種類のロールが必要である。

a）端末：各組織の中に存在する端末で、一般的に、従業員が業務のために利用する端末のことである。通常は Agent と呼ばれるソフトウェアモジュールがインストールされているが、中にはそうでないものも存在する。

b）アセット管理サーバ：Agent が収集した情報、またアセット管理サーバ自身が収集する情報など、組織内の各種情報を収集・蓄積するサーバである。本ロールは、知識ベースと通信することにより各 IT 資産情報の ID を特定し、当該 IT 資産情報と一緒に保存する。そして、本 ID をキーとして知識ベース内の脆弱性情報の有無を問い合わせ、必要に応じて管理者向けの警告メッセージを作成・発信する。

c）知識ベース：セキュリティに関する各種情報を蓄積しているデータベース [1] である。本稿ではこの中の、CVE/CVRF 形式で記述されている脆弱性情報及び CPE-ID と IT 資産情報の対応を記した CPE 辞書のみを利用する。

d）管理者端末：システム管理者の利用端末であり、脆弱性に関する異常が発見された際に警告が送付される端末でもある。今回は端末と同一のネットワークセグメントに置いているが、実際には携帯電話ネットワークを介して別ネットワークに存在していても良い。

e）ソフトウェアスイッチ：管理ネットワークセグメントの境界線となるネットワーク機器であり、スイッチやルータなど、各種形態をとることが可能である。本稿では本ロールに特別な役割を課してはいないものの、今後、初動対応の自動化を考える際には、本ロールがトラフィック制御などを実施する。

3　提案システムのプロセス概要

図 2 に、提案システムのプロセス概要を示す。本システムでは、3 段階の処理を実施したのちに、必要に応じて警告メッセージを発信するプロセスを確立している。まず、提案システムは接続されているネットワーク上の IT 資産に関する情報を収集する。次に、収集した情報から管理すべき IT 資産の識別子を生成し、その識別子を用いて知識ベースに脆弱性情報を問い合わせる。もし、脆弱性情報が引き当てられることがあれば、提案システムが管理している IT 資産の中に脆弱性が存在していることを意味するため、警告メッセージを発信する。

上記の流れの中で、IT 資産情報の識別子と脆弱性情報の引き当てについて、**3.1** に詳述する。

3.1　IT 資産情報の識別子の引き当て

IT 資産を一意に特定するための識別子について、CPE や SWID などの規格が存在するが、今回は NVD でも利用されている CPE を活用する。本システムでは、CPE 辞書をテキスト検索することにより、IT 資産情報に対応する CPE 識別子を引き当てている。すなわち、Agent が OS 名やインストールされたアプリケーション名等の端末情報を収集し、アセット管理サーバに送信すると、それを受信するアセット管理サーバはその端末情報に記載されているアプリケーション名を元に知識ベースに CPE-ID の問い合わせを実施する。このテキスト検索で完全一致するケースは少ないため、本プロトタイプでは検索結果の一致率を数値化し、その割合が閾値（設定ファイルにより値を事前に指定）を超えた場合に一致したと判定し、CPE-ID を引き当てている。CPE-ID が引き当てられた際には、本情報を端末情報と共に保存・蓄積している。

レジストリなどから収集される IT 資産情報の中には、アルファベットではなく漢字や仮名・カタカナ表記の情報も存在するが、CPE は多言語対応しており、既に CPE 辞書には日本語表記のものも多数存在する。そのため、本プロトタイプが収集する IT 資産情報に含まれる日本語表記の情報についても、対応する CPE-ID を取得することも可能である。

3.2　脆弱性情報の引き当て

3.1 の手続きにより自動生成した CPE-ID を用いてセキュリティ脆弱性検証を行う際には、端末情報のソフトウェア情報に記載された CPE から NVD 要素である <vuln:product> で一致する XML を検索する。

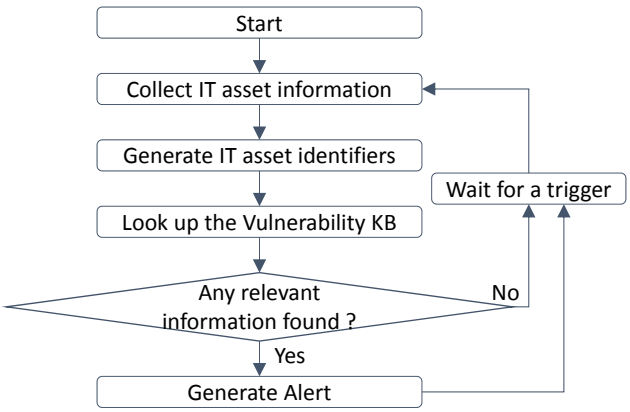

図 2　提案システムのプロセス概要

一致するNVDがあれば、脆弱性有と判断し、IODEF-SCI形式の警告を出力する。

4 情報スキーマ

提案システムは、情報が正しく構造化されていることを前提に動作している。そのため、すべての情報についてスキーマを指定もしくは定義し、その正しい利用を順守する必要がある。

4.1 IT資産情報

提案システムでは、収集したIT資産情報を構造化して保存する。その際に利用するスキーマとして、Asset Identification[9]やARF[10]などの規格化されたIT資産情報スキーマも活用可能であるものの、今回のプロトタイプ構築を考える上ではこれらの規格は過剰スペックなため、独自スキーマを利用した。今後、収集すべき情報が拡大した場合、また、他の組織と情報を共有する必要性などが生じたケースについては、これらの規格化されたスキーマの利用を改めて検討するものとする。

4.2 警告メッセージ

本システムは組織内のIT資産に関連する脆弱性情報が発見された際には、警告メッセージを発信するが、我々は本メッセージのスキーマにIODEF-SCIを利用している。本メッセージには、その脆弱性のCVE-IDとIT資産を特定するCPEの両方を埋め込んでいる。

IODEFは組織間でインシデント情報を交換するために作られた情報構造規格であるため、送信者の情報を書くフィールドなど、必要なフィールドが用意されているほか、拡張性に優れている。また、IODEF-SCIを用いることで、IODEF文書の中にCVEやCPEなどを埋め込むことが可能になる。そのため、IODEF-SCIを利用することは今回の目的に叶っているため、IODEF-SCIを本メッセージのスキーマとして利用した。

5 プロトタイプ構築

本節では、提案方式のプロトタイプを紹介する。OSやそのバージョンにより、Registryなどの情報構造なども異なるため、本プロトタイプでは、Windows 7を管理対象として実装した。但し、Windows XP, 8, Linux系のOSについても、一部対応可能な実装とした。

本プロトタイプは各端末の情報を収集し、サーバにその情報が蓄積される。保存されている端末のリストは図3のとおり閲覧可能であり、本図中の特定の端末のIDをクリックすることにより、図4に示す当該端末のIT資産情報を取得できる。なお、各端末はAgentモジュールをインストールしたタイミングで情報をサーバに送信するため、図3に表示される端末

端末一覧画面

TermID	IP	Update	Insert		
080027667EE0	192.168.56.102	2016-02-18T01:06:36	2016-02-18T01:06:36	OK	CPE detail
0800278E56AC	192.168.56.101	2016-02-18T01:01:18	2016-02-18T00:43:54	OK	CPE detail

図3　端末一覧画面

図4　管理されているIT資産情報

については既に IT 資産情報がサーバに保存されている。

図 4 を見ると、各種情報の中に、CPE タグと CVE タグが存在するが、これらの情報はアセット管理サーバ、そして知識ベースが提供したものであり、それ以外の情報は、Agent などを通じて端末から収集した情報である。新たなソフトウェアが端末に保存される度にすべての情報は更新される。同様に、知識ベース側に新たな脆弱性情報が登録された際にも、この CVE タグは更新される。

脆弱性が発見された際には、警告メッセージが発信されるが、現在の実装では、電子メールにて送信される。実際、これらの警告メッセージは、管理者が社外にいてスマートフォンから読むことを前提にして作られている。その警告メッセージの画面は図 5 のようになる。

6 まとめ

本稿では、オープンな脆弱性情報とツールを利用して、組織内の IT 資産及び関連する脆弱性に関する管理の自動化に向けた検討状況を共有した。提案システムでは、IT 資産情報の ID 引き当てとそれに対応する脆弱性情報の引き当てという 2 段階の知識ベース検索をする手法を取り、そのフィージビリティを検証した。しかしながら、現時点ではいまだ課題も多く（文献 [8] 第 4 節参照）、特に、IT 資産情報の引き当て精度と脆弱性情報のワイルドカード表記対応は喫緊の検討課題である。また、脆弱性情報を取得した後の初動対応について、SDN を用いた自動化技術についても今後検討していく所存である。

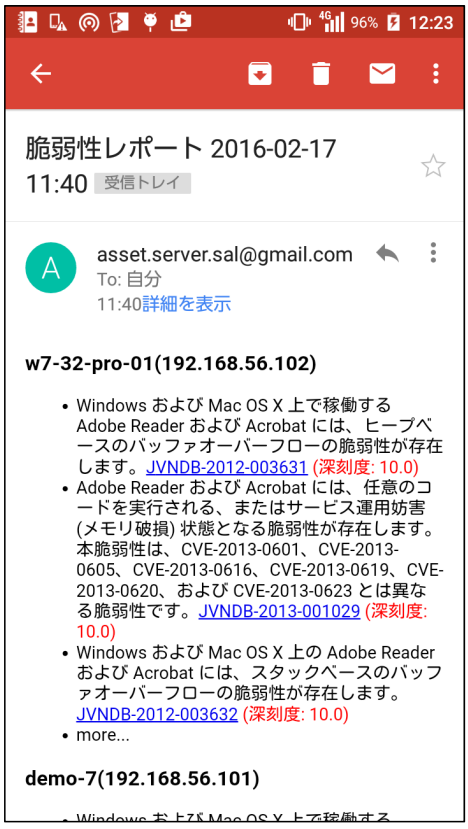

図 5　管理者への警告メッセージ

謝辞

本研究を実施するにあたり、様々なご支援を頂いた中尾康二主管研究員及び平和昌研究所長に深く感謝する。

【参考文献】

1 T. Takahashi, Y. Kadobayashi, “Reference Ontology for Cybersecurity Operational Information,” The Computer Journal, 2015.
2 National Institute of Standards and Technology, “National Vulnerability Database Version 2.2,” 2014. [Online]. Available: http://nvd.nist.gov/.
3 JPCERT/CC and IPA, “Japan Vulnerability Notes,” 2014. [Online]. Available: http://jvn.jp.
4 International Telecommunications Union, “Common platform enumeration,” ITU-T Recommendation X.1528, 2012.
5 International Organization for Standardization/International Electrotechnical Commission, “Software asset management -- Part 2: Software identification tag,” ISO/IEC 19770-2:2009, 2009.
6 The Internet Engineering Task Force, “The Incident Object Description Exchange Format,” RFC 5070, dec. 2007.
7 The Internet Engineering Task Force, “An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information,” RFC 7203, April 2014.
8 T. Takahashi, D. Miyamoto, K. Nakao, “Toward Automated Vulnerability Monitoring using Open Information and Standardized Tool,” IEEE International Conference on Pervasive Computing and Communications, 2016.
9 National Institute of Standards and Technology, “Specification for Asset Identification 1.1,” NIST Interagency Report 7693, 2011.
10 National Institute of Standards and Technology, “Specification for the Asset Reporting Format 1.1,” NIST Interagency Report 7694, 2011.

高橋健志　（たかはし　たけし）
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
主任研究員
博士 (国際情報通信学)
サイバーセキュリティ、通信プロトコル