学術情報処理研究 No.20
2016年9月

学内サーバの脆弱性診断と診断結果の解析方法
Server Vulnerability Check and Analytical Method of their Diagnoses in a University.

相羽俊生，川原智徳，高橋至，小田謙太郎
古屋保，下園幸一，佐藤豊彦，升屋正人，森邦彦
Shunsei AIBA, Tomonori KAWAHARA, Itaru TAKAHASHI, Kentarou ODA
Tamotsu FURUYA, Kouichi SHIMOZONO, Toyohiko SATO, Masato MASUYA, Kunihiko MORI

info@cc.kagoshima-u.ac.jp

鹿児島大学学術情報基盤センター

Computing and Communications Center, Kagoshima University

概要

鹿児島大学では、学内のサーバについて、2013 年度より一部の部局を対象とした脆弱性診断を開始した。また、2015 年度からは脆弱性診断専用のシステムを構築、運用している。本稿では、脆弱性診断システムの構築から診断実施までの手順、および発生したトラブル等について述べるとともに、サーバに存在する脆弱性の状態を視覚的に把握するための診断結果の解析方法について述べる。

キーワード

情報セキュリティ、脆弱性診断、Nessus

1.はじめに

サーバの脆弱性は、情報セキュリティ上の欠陥として定義される。サーバが脆弱性を利用した攻撃を受けることで、コンピュータウイルスへの感染や、不正アクセスといった情報セキュリティ事故を引き起こす。例えば、組織のウェブサーバが外部から不正アクセスを受け、ウェブサイトに不正プログラムを仕込まれると、ウェブサイト訪問者へコンピュータウイルスの感染やフィッシングサイトへの誘導による金銭的損害などの被害を与える。このような場合、不正アクセスを受けた組織が一転して加害者となることから、組織に対する不信感やイメージの低下など、大きな事態に発展する可能性がある。サーバを運用する組織は、情報セキュリティ事故を未然に防ぐために、脆弱性への対策をしっかり講じておかなければならない。2013 年、当大学においてもウェブサーバが不正アクセスを受け、部局のウェブサイトが改ざんされるという事案が発生したが、その原因のひとつとして、サーバに脆弱性が存在していた可能性が十分に考えられる。インターネット上に公開される外部向けのサーバは、非公開のサーバに比べ攻撃を受ける頻度が高いため、脆弱性の有無については特に注意する必要がある。

大学内のサーバおよびネットワークを取り巻く環境には、一般的に次のような特徴がある。

- 歴史的経緯から、多くのグローバル IP アドレスを保有している。
- 教育、研究の自由を尊重する文化があり、ネットワーク利用に関する制約が少ない。
- 研究室や部局の独立性が高く、セキュリティ対策に必要な IT ガバナンスを徹底しにくい。

つまり、グローバル IP アドレスが開放的な環境で利用できることを意味している。したがって、大学内には、情報セキュリティ上、注意を要するサーバ等がいくらか存在するのではないかと想定される。ある報道によると、多数の大学において、グローバル IP アドレスを割り当てられたプリンタ複合機が不適切な公開設定になっており、インターネットを通じて外部から内部情報にアクセスできる状態になっていた、などと報じられている[1]。

このような中、大学での情報セキュリティ事故を未然に防ぐための取り組みのひとつとして、大学内のネットワークに接続されているサーバを発見し、脆弱性の有無について検査する脆弱性診断が有効であることが報告されている[2-5]。

当大学においても情報セキュリティ対策の一環として、2013 年度からコンサルティング業者に委託し、学内のサーバに対する脆弱性診断を開始した。そして、2015 年度には脆弱性診断専用のシステムを自前で構築し、毎月診断を実施している。自前でシステムを構築する主な利点として、費用が低く抑えられる点と、日程や回数に制限なく柔軟に診断を実施できる点が挙げられる。

本稿では、脆弱性診断システムの構築から実施までの手順について述べ、次に診断結果のデータ処理およびサーバにおける脆弱性の状態を視覚的に把握することを目的とした解析手法について述べる。

2.脆弱性診断システムの構築

2.1.脆弱性診断ツール（Nessus）

当大学には、グローバル IP アドレスを割り当てられたサーバが多数存在する。そこで、それらに対して効率よく診断を実施するために、脆弱性診断ツールとして定評のある Nessus [6]を採用し、脆弱性診断システムを構築することとした。

Nessus は、サーバ等に存在する種々の脆弱性を、ネットワーク経由で診断するツールであり、特定の脆弱性に対応した数多くのプラグインから構成されている。プラグインは、脆弱性の有無について判定するだけでなく、脆弱性が存在する場合には Risk Factor（深刻度）、対応する共通脆弱性識別子（CVE）および解決策などの情報を提示する。プラグインの情報は Nessus の販売元である Tenable Network Security 社によって定期的に追加･更新されており、2016 年 6 月 30 日時点で 80,264 個のプラグインが存在する。なお、プラグインは、プラグイン ID によって一意に識別される。表 1 にプラグインの例を示す。

プラグインによって診断された脆弱性の深刻度は、表 2 に示すように、共通脆弱性評価システム（CVSS）基本値に応じ、4 段階の深刻度に分類される。表 1 のプラグインの例によって診断された脆弱性の場合 CVSS 基本値が 6.8 と評価されていることから、深刻度は Medium となる。基本的に、深刻度が High 以上の脆弱性は早急な対応が必要とされている。

表 1　プラグインの例

プラグイン ID	90509
名称	Samba Badlock Vulnerability
CVSS 基本値	6.8
深刻度	Medium
CVE	CVE-2016-2118
プラグイン登録日	2016/3/23

表 2　CVSS 基本値と深刻度の対応

CVSS 基本値	深刻度
10.0	Critical（緊急）
7.0～9.9	High（高）
4.0～6.9	Medium（中）
0.0～3.9	Low（低）

2.2.診断システムの構築

脆弱性診断システムは、レンタルサーバ運営ベンダが提供する学外の仮想専用サーバ（VPS）上に構築した。表 3 にシステムの構成を示す。

表 3　脆弱性システムの構成

サーバ	学外 VPS
CPU	仮想 4 コア
メモリ	4 GB
OS	Cent OS
脆弱性診断ツール	Nessus Professional

構築したシステムのセキュリティ対策として、システムへ接続する際のアクセス元 IP アドレスを制限した。また、脆弱性診断に関する操作は、Nessus のウェブインタフェースを介して行うため、システムにログインする際にウェブフォームから送信されるユーザ名とパスワードを SSL 通信で保護する目的で、ウェブサーバに SSL 証明書をインストールした。

2.3.全学ファイアウォールの設定変更、および対外接続部監視サービスへの事前通知

当大学の学内ネットワークでは、ファイアウォールやセキュリティベンダによる対外接続部監視サービスなどによって、不審な通信の検知や遮断を行うなどのネットワークセキュリティ対策を講じている。

したがって、当大学自らによる脆弱性診断であっても、不審な通信と検知・遮断されることから、診断を行うことができない。そのため、予め計画された脆弱性診断に関連する通信を、ネットワークセキュリティ対策から除外する目的で、ファイアウォールへの設定変更を行うとともに、セキュリティベンダへ診断日時と診断元 IP アドレスについて事前に通知した。図 1 に脆弱性診断の実施概略図を示す。

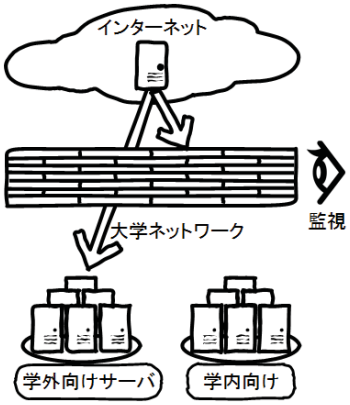

図 1　脆弱性診断の実施概略図

3.脆弱性診断の実施

3.1.診断対象サーバ

診断対象のサーバは、当初、グローバル IP アドレスを割り当てられている学外公開用のサーバを想定していた。しかし、プリンタ複合機やネットワークカメラなど、意図せず学外公開状態になってしまっている機器、および管理者不在のまま稼働し続けているような、いわゆる「野良サーバ」が存在する可能性も完全には否定できない。そのため、診断はネットワークセグメント単位で実施することとした。既知のサーバの IP アドレス単位で診断するのではなく、ネットワークセグメント単位を診断対象とすることで、既知のサーバの脆弱性を診断できると同時に、未知のサーバ等についても発見および診断することができるからである。これらの要件をふまえた Nessus の基本設定項目を表 4 に示す。

表 4　Nessus の基本設定項目

Scanner Templates
Basic Network Scan
Discovery
- Ping Methods:
全て実施しない（ARP,TCP,ICMP を外す）
- Port scan range:
[default]から[all]へ変更

構築したシステムによる脆弱性診断は、2015 年 4 月より、当大学の一部の部局を対象に開始し、診断の実施頻度は 2015 年 8 月を除き、毎月 1 回とした。実施日は、予定の数日前に部局のネットワーク責任者へ通知し、サーバへアクセスが集中する繁忙期などと重複することがないよう調整の上、決定した。時間帯は、不測の事態が発生した場合に備え、迅速に対応が可能な営業日の日中を選択した。

本稿における診断対象の IP アドレスは 1,640 ある。ただし、2015 年 12 月～2016 年 3 月までの 4 ヶ月間は、診断システムの操作ミスにより、一部の IP アドレスが診断対象から外れたため、その間は 1,362～1,589 の IP アドレスしか診断できなかった。そのため、データ解析の際、診断できなかった IP アドレスのサーバが比較対象に含まれる場合は、統計データとして不適切である。なお、2016 年 4 月には通常の運用に復帰した。

3.2.発生したトラブルおよび設定値の検討

脆弱性診断の開始初期は、診断実施中にレンタルサーバ運営ベンダから VPS の利用を停止され、診断システムへアクセスできなくなるというトラブルが 2 回発生した。

1 回目は、脆弱性診断に伴うポートスキャン等の通信内容が、VPS の不正利用と見なされ、緊急停止されたものであった。これに対し、先方に次の 2 点について事情を説明することで、停止解除の運びとなった。

- 停止された時間帯に実施した脆弱性診断は、予め計画されたものであること。
- 脆弱性診断は、当大学のネットワークに対してのみ実施しており、それ以外のネットワークに対しては今後も実施しないこと。

しかし、1 回目の停止解除から約 1 ヶ月後、2 回目となる停止を受けた。理由は、脆弱性診断システムから大量のセッションが張られたことで、VPS の共有リソースが大きく消費され、自動停止されたものであった。これに対し、Nessus の Performance Options の設定において、サーバの同時診断数、および同時 TCP セッション数を、初期値から、より小さい値へ変更した。表 5 に Performance Options の設定変更と診断時間の関係を示す。この設定変更により、全ての診断が完了するまでの所要時間が平均 63.5 分から 425 分へと約 6.7 倍になったが、同様のトラブルは発生しなくなった。学外の VPS を脆弱性診断の用途で

利用する場合、通信内容や通信量が利用停止措置の引き金となる可能性があるため、十分な注意と配慮が必要である。

表 5　Performance Options の設定変更と診断時間

	変更前	変更後
Max simultaneous hosts per scan	30	10
Max number of concurrent TCP sessions per host	-	10
Max number of concurrent TCP sessions per scan	-	10
平均診断時間（分）	63.5	425

4.診断結果の解析

4.1.診断結果のデータ処理

脆弱性診断の結果は、その特性上、サーバ管理者などの関係者へ迅速に報告する必要がある。また、過去に対策が必要な脆弱性が診断されたサーバでは、講じられた対策が脆弱性の解消に有効であったかどうかを検証するために、過去の結果との比較も必要である。Nessus には、診断結果を確認する方法として、ウェブインタフェース上のレポートを直接参照する方法と、データ出力機能を使う方法の 2 通りが用意されている。しかし、ウェブインタフェース上のレポートを直接参照する方法では、これらの要件を満たすことができない。そのため、データ出力機能によって得られた診断結果ファイルを、別途データベースに蓄積し、処理を行うこととした。

診断結果のデータ出力機能では、HTML, PDF, CSV, Nessus, Nessus DB の 5 種類のファイル形式による出力に対応している。それぞれの形式を比較検討した結果、CSV 形式が最も汎用性に優れていたことから、CSV 形式の結果ファイルを基にデータベースへ取り込み、その後の処理を行うこととした。なお、CSV 形式の結果ファイルには、次の 13 項目

[Plugin ID], [CVE], [CVSS], [Risk], [Host], [Protocol], [Port], [Name], [Synopsis], [Description], [Solution], [See Also], [Plugin Output]

がセットされており、一部の値は空白の場合もあり得る。

図 2 に一連のデータ処理の流れを示す。まず、Nessus のデータ出力機能により出力した CSV 形式の結果ファイルを、MS Excel 形式のファイルへ変換する。変換が必要な理由は、[Description]や[Plugin Output]の値として、任意の数のカンマが含まれる場合があり、各項目の値を単純にカンマ区切りで分離することができないからである。

次に、MS Excel 形式のファイルを関係データベースへ取り込む。データベースは MySQL を使用した。取り込まれるレコード数は 1 回の診断結果あたり約 30,000 件である。

次に、[Host], [Plugin ID], [Risk], [Port]でグループ化することで重複データを 1 つにまとめる。Nessus から出力された CSV 形式の結果ファイルでは、1 つのプラグインに複数の CVE が対応している場合、そのプラグインによって診断された脆弱性については、プラグイン ID が同じであっても、CVE ごとにレコードとして出力する。つまり、[CVE]だけが異なり、残りの[Host], [Plugin ID], [Risk], [Port], [Description], [Solution]等の項目の値が全て同じというレコードが複数存在する場合がある。そのため、例えば 4 つの CVE に対応したプラグインの場合、重複データを 1 つにまとめないと、脆弱性が実際は 1 件であるのに、4 件あるかのように集計してしまうことになる。Nessus のウェブインタフェース上のレポートにおいても、重複データをまとめた結果として集計されていることから、ウェブインタフェース上と同じ結果を得るためにもグループ化が必要となる。本稿ではこのグループ化によって得られた件数を脆弱性の件数とする。

次に、DNS で逆引きすることで診断対象サーバの IP アドレスから FQDN を求める。Nessus から出力された CSV 形式の結果ファイルは、サーバの識別情報として、[Host]の IP アドレス情報しか持たない。そのため、関係者へわかりやすい情報として報告する目的で、IP アドレスだけでなく FQDN も併記する。

最後に、MS Excel 形式の集計・報告ファイルとして、各サーバ版、全体集計版を出力する。なお、データベース取込以降の処理は、Java および Java ライブラリの Apache POI [7]を使うことで自動化した。

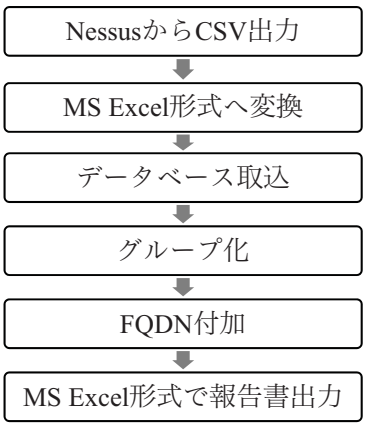

図 2　データ処理の流れ

4.2.診断結果の解析と脆弱性への対応

診断結果は、報告書をもとに各サーバの管理者へ報告する。特に、何らかの脆弱性があると診断されたサーバについては、必要な対策を講じるよう併せて依頼する。依頼を受けた管理者は、セキュリティパッチの適用や、不必要なサービスの停止などの対策を講じる。そして、次回の脆弱性診断により、対策の有効性や新たな脆弱性の有無を確認する。これら一連の対応サイクルを図 3 に示す。

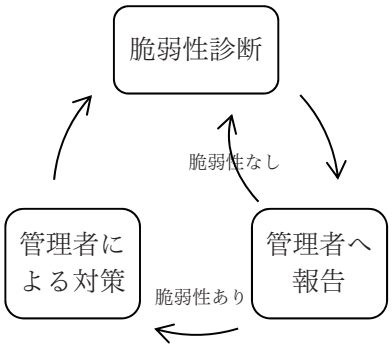

図 3　脆弱性への対応サイクル

管理者へ対策を依頼する際、深刻度が High または Critical の脆弱性については早急な対応が必要とされていることから、原則として次回の脆弱性診断までに必ず有効な対策を講じるよう強調している。一方、Medium や Low の脆弱性については、管理者の判断により許容範囲内として受容される場合もあるが、次回以降の診断結果からも除外などはせずに継続して報告している。

一連の診断の結果、グローバル IP アドレスを割り当てる必要性のない無線 LAN アクセスポイント 1 台が発見されたため、対策として、学外からアクセスできないネットワークへと接続先を変更された。なお、管理者不在のまま稼働しているような「野良サーバ」は 1 台も発見されなかった。

2015 年 4 月から 2016 年 5 月までの期間に診断した全サーバの脆弱性について、月別の合計件数を図 4 に示す。3.1.節で述べたように、2015 年 12 月～2016 年 3 月までの 4 ヶ月間は、一部の IP アドレスのサーバが診断対象から外れたため、件数が明らかに少ない。しかし、この期間を除外して考えても、診断された脆弱性の件数は次第に減少してきていることがわかる。一般的に、新しい脆弱性は次々に発見されており、その総数は増え続けているため、脆弱性への対策を講じなければ、診断される脆弱性の件数も次第に増加するはずである。にもかかわらず、脆弱性の件数が次第に減少してきていることから、全体として、脆弱性への対策が講じられていることを意味する。また、対策の動意付けとして、脆弱性への対応サイクルが効果を上げているものと考えることができる。

しかし、脆弱性への対策を講じることのできない管理不十分なサーバ等が少数でも存在すれば、情報セキュリティ事故は発生する。そのため、全体としての対策状況のほかに、個々のサーバにおいても、脆弱性への対策が講じられているか否かを把握する必要がある。特に多数のサーバを管理している管理者の場合、診断結果報告書の内容を確認するだけでも大変な労力である。労力のかかる作業は、対策が講じられない要因にもなりかねないため、個々のサーバの脆弱性の対策状況について、把握しやすい情報として提供する工夫が必要である。

そこで、脆弱性の新しさを表す指標として、プラグイン ID の情報を追加したバブルチャート（以降、脆弱性チャートという）を作成することで、脆弱性の状態を視覚的に表すことを考えた。図 5 に脆弱性

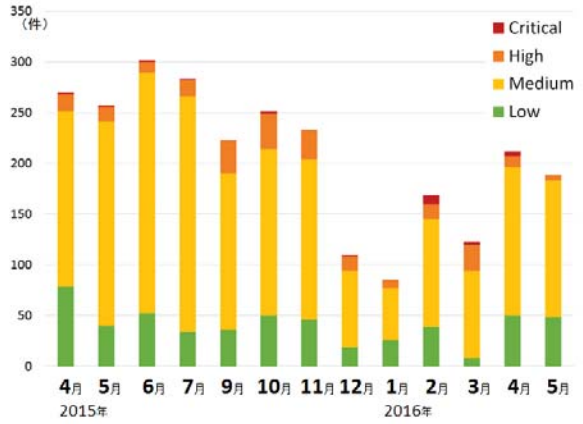

図 4　脆弱性の合計件数

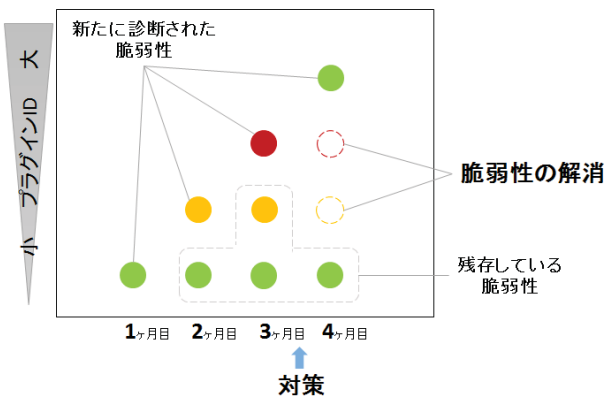

図 5　脆弱性チャートを用いた対策状況の把握例

チャートの例を示す。脆弱性チャートは、縦軸でプラグイン ID、横軸で診断実施年月、色で深刻度を表し、また、同じプラグイン ID の脆弱性が複数存在する場合、バブルの大きさで件数を表す。

プラグイン ID は、Nessus においてプラグインを一意に識別する数字であり、プラグインの登録日順に付番される。したがって、プラグイン ID の値が大きいほど、新たに診断された脆弱性となる。脆弱性チャートを用いることで、新たに診断された脆弱性、対策によって解消した脆弱性、および残存している脆弱性がわかり、サーバにおける脆弱性の対策状況を視覚的に把握することに役立つ。

実際の診断結果を、脆弱性チャートを用いて解析した一例目として、サーバ A について考察する。診断結果によると、このサーバの OS は Mac OS X Server であり、ウェブサーバ用途として Apache, PHP, OpenSSL などが稼働していることがわかっている。図 6 にサーバ A において診断された脆弱性の件数を示し、図 7 にサーバ A の脆弱性チャートを示す。図 6 の棒グラフからは、深刻度の高い脆弱性が比較的多いこと、およびそれらの件数の推移について知ることができるが、脆弱性への対策状況を読み取ることは困難である。一方、同じサーバ A について、図 7 の脆弱性チャートからは、次の状況を読み取ることができる。

- 2015 年 4 月～10 月および 2016 年 2 月～4 月の間に診断された脆弱性は、次回診断時には解消している。脆弱性の報告を受けた管理者によって、有効な対策が講じられた結果、脆弱性が解消したことがうかがえる。
- 2016 年 1 月～2 月の間は、前回診断時の脆弱性が引き続き残存していることから、有効な対策は講じられなかったことがうかがえる。
- プラグイン ID の大きな脆弱性がほぼ毎月、新規に現れているのは、新しい脆弱性が次々に発見される状況であることを示している。

これらのことから、サーバ A は、脆弱性への対策が継続的に講じられており、また、今後も頻回な対策を必要とする環境にあることを示唆している。なお、図 6 と図 7 の両方を確認すると、2015 年 6 月を除き、同じプラグイン ID を持つ脆弱性が 2 件ずつ診断されていることがわかる。この理由は、サーバ A がウェブサービスを HTTP/port:80 と HTTPS/port:443 の 2 つの port で提供しているため、PHP 等に関する脆弱性をそれぞれの port ごとに診断および集計していることによる。

二例目として、サーバ B について考察する。診断結果によると、このサーバの OS は Windows Server 2003 であり、ウェブサービスやリモートデスクトップサービスが稼働していた。図 8 にサーバ B で診断された脆弱性の件数と、脆弱性チャートを示す。脆弱性チャートから、2015 年 4 月の初回診断以降、プラグイン ID の比較的小さな 3 つの脆弱性が残存し続けていることがわかる。その後、2015 年 7 月に実施した診断では、Windows Server 2003 のメーカーサポート切れによる深刻度 Critical の脆弱性が診断されたため、管理者へ改めて報告し、対策としてサーバの停止が行われた。脆弱性が残存し続けるといった兆候に気付いた場合は、なるべく早い段階でサーバの管理状況について管理者へ照会し、脆弱性への対策の重要性が十分に認識されているかどうかを確認する必要がある。脆弱性チャートは、このような兆候に気付くための方法としても有効であると考えられる。

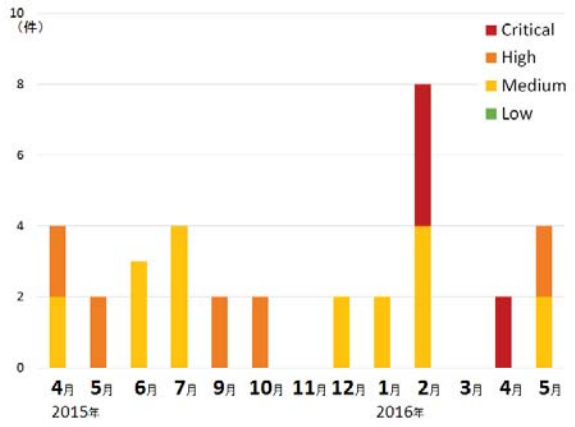

図 6　サーバ A で診断された脆弱性の件数

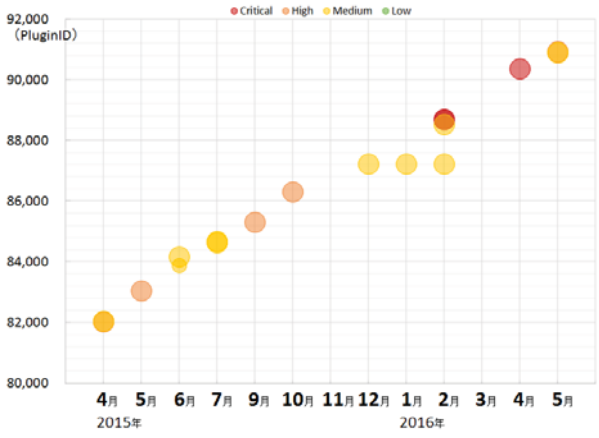

図 7　サーバ A の脆弱性チャート

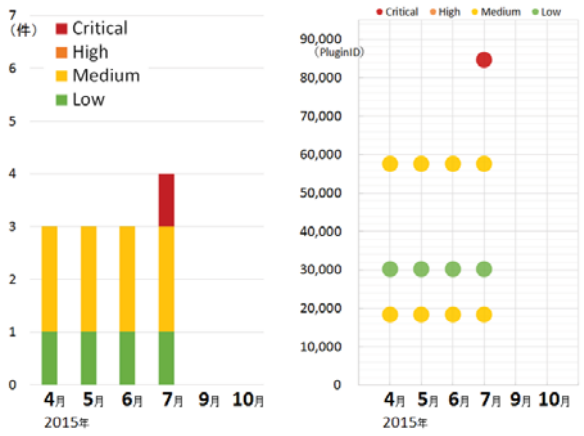

図 8　サーバ B で診断された脆弱性の件数（左）および脆弱性チャート（右）

5.まとめと今後の予定

学内のサーバに対し、2015 年度から専用の脆弱性診断システムを使った脆弱性診断を実施している。診断システムは、脆弱性診断ツール Nessus を学外の VPS 上に構築することで用意した。学外の VPS を利用する際には、診断を受ける大学側の準備だけでなく、診断システムを稼働させている VPS 側に対する配慮も必要であり、そのために設定値を変更するなどの対処を行った。

脆弱性診断の結果は、サーバ管理者へ報告することで、脆弱性への対策が講じられるようになり、その結果、診断される脆弱性の件数は全体として次第に減少してきている。診断結果の解析方法については、当大学の状況に則して検討を行い、脆弱性の新しさを表す指標を追加したバブルチャート（脆弱性チャート）を作成することで、サーバにおける脆弱性の状態を視覚的に把握する方法を考えた。

今後、2016 年度の内部監査として、研究室や部局を含む学内全てのサーバに対し脆弱性診断を実施する予定である。したがって、脆弱性診断の結果は、サーバ管理者だけでなく、監査室の職員や部局の責任者などに対してもわかりやすく報告する必要が生じてくることが想定される。その場合にも、脆弱性チャートによる視覚的な情報を加えることによって、効果的な報告に寄与することが期待できる。

参考文献

[1]「データ流出危機 140 台　大学など 26 校の複合機・プリンター」『朝日新聞』2016 年 1 月 6 日, 朝刊, 1 面

[2] 大隅淑弘, 藤原正和, 濱田貴史, 岡山大学におけるサーバの実態調査と脆弱性検査, 第 23 回情報処理センター等担当者技術研究会報告集, pp.69-74, 2011

[3] 若杉清仁, 高木稔, 学外向けサーバへのサーバ疑似アタック検査について, 第 24 回情報処理センター等担当者技術研究会報告集, pp.85-90, 2012

[4] 田島浩一, 岸場清悟, 近堂徹, 大東俊博, 岩田則和, 西村浩二, 相原玲二, 広島大学におけるセキュリティ脆弱性診断の実施とその評価, 学術情報処理研究 No.18, pp.16-23, 2014

[5] 浅川圭史, 中村文, 永井一弥, 今井美香, 伊藤稔, 長田和宏, 小幡美紀, 鈴木彦文, 不破泰, 学内サーバ管理の問題点と新たなサーバ管理方式について, 第 18 回学術情報処理研究集会発表論文集, pp.1-8, 2014

[6] Tenable Network Security, Nessus Professional, http://www.tenable.com/products/nessus/nessus-professional

[7] The Apache Software Foundation, Apache POI, http://poi.apache.org/