室蘭工業大学における学外向けサーバ検査の実施報告

矢野　大作[1)]

1）室蘭工業大学 情報メディア教育センター

yano@mmm.muroran-it.ac.jp

概要：室蘭工業大学情報メディア教育センターでは従前より、学外に向けたサービスを行うサーバについて擬似アタック検査を行い、脆弱性を指摘することでセキュリティを確保している。この実施方法と 2014 年度の実施結果について報告する。

1　はじめに

本学は、学外より学内ネットワークへの通信は一部を除き Fire Wall（以下、F/W という）で遮断されているが、申請により部局や研究室単位で外部向けの Web サーバや Mail サーバ等の運用を認めている。申請のあったサーバについて脆弱性検査を経てから学外ポートを開放するポリシーの追加設定を F/W に行い、運用開始となる。開始後も継続的にセキュリティ保持がなされているか定期的に脆弱性検査を行っている。

本稿では、この実施方法と 2014 年度の検査結果および傾向について報告する。

2　2014 年度の検査

2.1 検査の実施時期

検査の実施は 5 月および 11 月に定期で計画している。また、ベンダー等で重大なセキュリティホールが発見・報告された際にも随時行い、実施した検査結果として管理者に対策レポート（図 1）を送付している。脆弱箇所がある場合は修正対応を依頼し、管理者のみで対応できないなどの場合は相談にも応対する。

2.2 実施方法

検査には脆弱性診断ツールを利用している。脆弱性診断ツールはそれぞれのサーバに対し、CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）の脆弱性データベースに基づいた擬似アタックを行う機能を有する。さらに擬似アタックの結果に基づいた脆弱性への対策レポートを作成することができる。

なお、本検査は学外からの実施ではなくイントラの検査であるため、実際の F/W を経由した攻撃耐性の評価としてだけでなく、サーバの供給するサービス全般に関わる総合的な

[redacted]	muroran-it.ac.jp	不明

Apache HTTP Server 2.2.29/2.4.12 NULL Pointer Dereference (0-Day)			
監査 ID:	46225		
リスクレベル:	中		
PCI コンプライアンス:	深刻度	コンプライアンスステータス	理由
	低	成功	Default
カテゴリ:	Webサーバ		
解説:	The self-reported banner version of Apache HTTP Server 2.2 or 2.4 installed on the target is a version to 2.2.29 or 2.4.12. Based on this information, it is potentially affected by the a null pointer dereference in protocol.c		
修正方法:	Currently, there are no solutions for this vulnerability.		
関連するリンク:	Apache HTTP Server 2.2.29 / 2.4.12 NULL Pointer (http://seclists.org/bugtraq/2015/Apr/90)		
影響するマシンの数:	1 (100.0% のホストに影響)		
影響する項目:			
	検査した値:	.*APACHE(-ADVANCEDEXTRANETSERVER)?/((2\.2\.2[89]|2\.4\.12)([^0-9].*)?)($|[^0-9])	
	取得した値:	APACHE/2.4.12 (UNIX) PHP/5.6.9	
	コンテキスト:	TCP:80	

図 1　対策レポートの一部

評価ができるため有用であると考えている。

以上のサーバ検査フローを図 2 に示す。

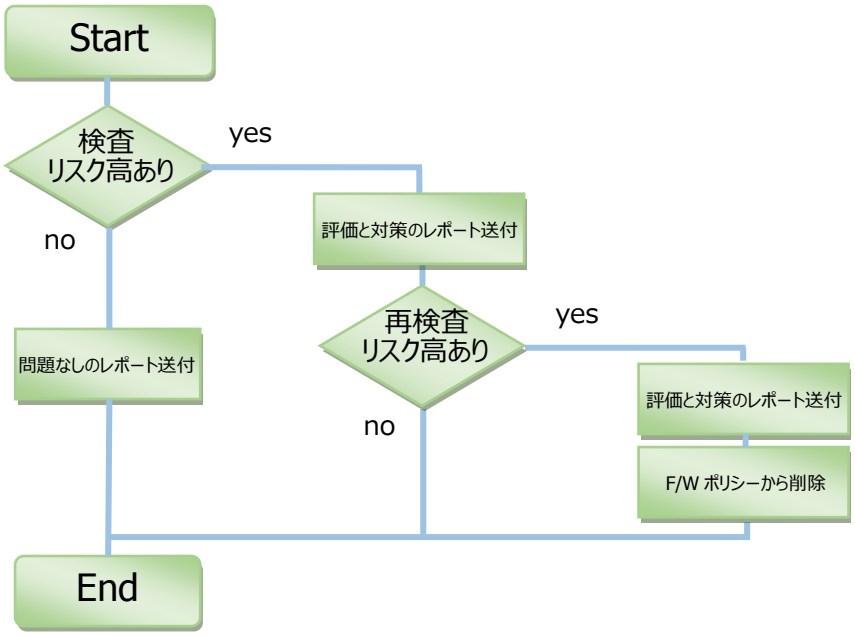

図 2　現在の本学のサーバ検査フロー（1 回）

2.3 2014 年度結果

2014 年度 1 回目の検査結果を図 3 に示す。

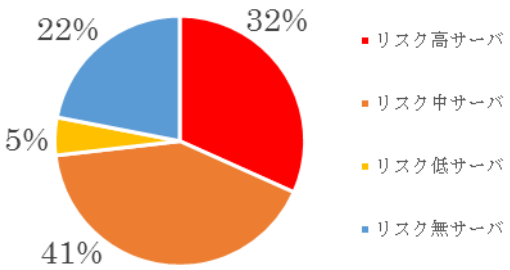

図 3　2014 年度 1 回目（7/22）結果

1 回目検査は、脆弱性診断ツールの導入が 2014 年 4 月であったため、7 月に行った。

図中で、「リスク高サーバ」はリスク高を 1 つでも含むサーバであり、「リスク中サーバ」は中程度のリスクが存在するが、リスク高は無いサーバである。また、「リスク低サーバ」は低程度のリスクが存在するが、リスク高およびリスク中の無いサーバであり、「リスク無サーバ」は全てのリスクが無いサーバである。

1 回目の検査レポートを送付後、修正依頼期限を設け、その直後に行った検査結果（以下、1 回目再検査 1 とする）を図 4 に示す。

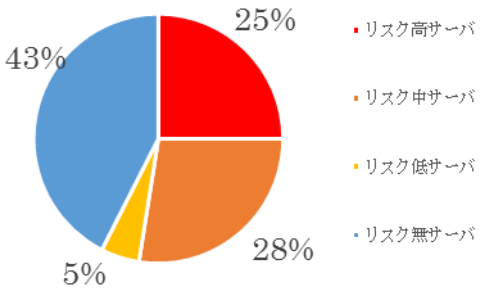

図 4　2014 年度 1 回目再検査 1（10/7)の結果

図 4 において、「リスク高」・「リスク中」の存在するサーバの管理者には再度の修正を依頼した。また、これらのサーバについては 11/28 に再検査を行い、その際に「リスク高」があった場合は、F/W のポリシーから削除し通信遮断する旨を通知している。

2014 年度 2 回目の検査結果を図 5 に示す。

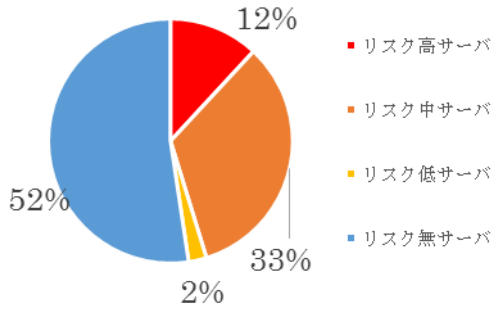

図 5　2 回目（12/19）の結果

2 回目の結果では、検査を行う前に Poodle[1]脆弱性への注意喚起を行ったこともあり、「リスク高」のあるサーバは 12%と少ない。これらサーバについては脆弱性の修正の期限を 1/30 であると通知するとともに個々の管理者と連絡を取って脆弱性対応の可否を聞き、未対応分については現地での対応も行った。

1/30 に行った結果（2 回目再検査 1 とする）を図 6 に示す。

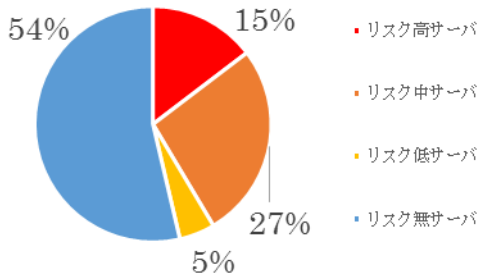

図 6　2014 年度 2 回目再検査 1（1/30）の結果

2 回目で「リスク高」のあるサーバ管理者からの修正相談にも応対しながら行った。「リスク高」の存在するサーバは、全体では 15%と微増しているが、リスク高が無くなったサーバも存在する。

これらのサーバも最終的には F/W のポリシーからの削除通告を行い 2 回目の検査を終了する。

3 おわりに

本学では、検査用ソフトウェアによる検査を 2011 年度より行ってきており、2014 年度は導入初年度であった脆弱性診断ツールを利用して行った。2014 年度は従来通りの実施に加えて、Poodle や FREAK[2]というような通信暗号化方式の技術に関する重大な脆弱性が報告されたこともあり、実際には本報告以外にも検査を行った。そして、その都度必要に応じてサーバ管理者に通知し、連絡を密に取ったため、脆弱性の修正も逐次行われており、セキュリティを意識した運用管理が行われたと考えている。

本学と外部を繋ぐネットワークには 2005 年度より F/W が導入されている。そのため学内と学外とは隔離されているが、全学的サービスとして学外向けサーバを運用する場合、F/W にポリシーを登録することになる。その結果、学内セキュリティが甘くなる場合もありうる。

本学では学外向けサーバの管理責任は学外向けサーバを運用する管理者および実務担当者にある。そのため学外向けサーバの管理者および実務担当者は、たゆみないセキュリティ維持努力が必要である。一方で当センターとしては、常に最新のセキュリティに関する情報の収集に注力してもらえるよう、本脆弱性検査も継続していく必要があると考えている。

参考文献

[1]CVE-2014-3566:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 2015.10.19 アクセス

[2]CVE-2015-0204:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 2015.10.19 アクセス