IPA Technical Watch

IPA Better Life with IT

脆弱性対策の効果的な進め方（実践編）

～脆弱性情報の早期把握、収集、活用のスヽメ～

IPA 独立行政法人**情報処理推進機構**
技術本部 **セキュリティセンター**

目次

はじめに

2014 年は、広く普及し、かつ長く利用されてきた OpenSSL、Apache Struts、GNU bash などのソフトウェアの脆弱性対策情報が多数公表された。これらのソフトウェアは多数の商用製品やオープンソースに組み込まれており、サービスを構成するソフトウェアの一部としても使われることが多い。このため、これらのソフトウェア単体だけではなく、様々なソフトウェアやサービスに影響が波及した。

脆弱性は日々公表されており、システムの管理者やソフトウェアの開発者は公表された脆弱性に対して、バージョンアップなどのソフトウェア更新や開発ソフトウェアへの対策プログラムの組込みなど、時機を逸しない適切な対応が求められる。適切な対応を行う上で重要なポイントは、脆弱性対策情報を迅速に把握、収集すること、そして集めた脆弱性情報の中から自組織・自社製品にとって影響度が高いものから優先的に対策を行うことである。

本書は、そういった脆弱性への対応を行う際に、システムの管理者などが、どのサイトから収集を行うのが良いか、また収集した情報はどのように分析をして対策に活用するのが良いか、という点について、具体的な脆弱性関連情報の収集先や分析手法などの技術情報、およびそれを支援する IPA 提供のサービスやツールについて解説をしたレポートである。

本書の対象読者

・システムの運用管理者
　適用例：運用システムの脆弱性対策を実施している方
・ソフトウェア製品の開発者
　適用例：ソフトウェアの開発において他社またはオープンソースのソフトウェアを組み込んで開発している方
・システムインテグレーター（通称：SIer）
　適用例：顧客に納入したシステム等の脆弱性対策を実施している方

※IPA では、2013 年 9 月に IPA テクニカルウォッチ「脆弱性を悪用する攻撃への効果的な対策についてのレポート」[1]を公開している。このレポートでは、対策要否を判断するための脆弱性の絞り込みや攻撃による被害やリスクを多角的に見る方法に CVSS[2]による評価手法が利用可能であることを概説した。本書では、そのレポートを、より実践的な視点で補完をしたものである。

[1] 2013 年 9 月 26 日公開「脆弱性を悪用する攻撃への効果的な対策についてのレポート」
https://www.ipa.go.jp/about/technicalwatch/20130926.html

[2] 本書では、FIRST(Forum of Incident Response and Security Teams)が 2007 年 6 月に公開した CVSS v2 の評価基準を基に解説を行った。

1. 脆弱性に関わる脅威の状況

1.1. 最近の脆弱性の実情

2013 年に引き続き、多くの脆弱性が 2014 年も公開されている。図 1-1-1 は、IPA が運用する「脆弱性対策情報データベース JVN iPedia」[3]の登録件数の四半期別推移である。累計の登録件数を見ると 2014 年 12 月末時点は 51,499 件となっている。2014 年の登録件数は 8,128 件であり、月あたりは約 677 件、日あたりは約 22 件の脆弱性対策情報が公開されている。

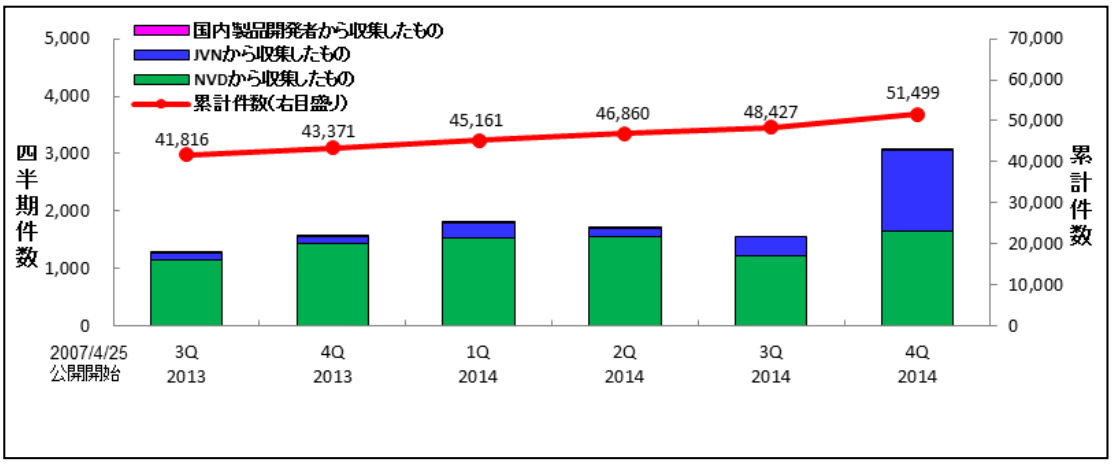

図 1-1-1：脆弱性対策情報データベース JVN iPedia の登録件数の四半期別推移

2014 年は、一般に利用される商用製品やオープンソースにも組み込まれている OpenSSL、Apache Struts、GNU bash などのソフトウェアの脆弱性対策情報が多数公開された。特に OpenSSL や GNU bash の脆弱性の一部は、ハートブリード（英語: Heartbleed）やシェルショック（英語: Shellshock）といった名称でも広く呼ばれており、IT 関連のニュースサイトだけでなく一般のサイトでも大きく取り上げられている。

2015 年 3 月 25 日に公開した「情報セキュリティ 10 大脅威 2015」[4]のランキングでも OpenSSL や GNU bash の脆弱性などの”脆弱性の悪用”に関連するものがランクインしている。いくつかピックアップしてみると、まず、5 位「ウェブサービスからの顧客情報の窃取」は、攻撃者により”脆弱性を悪用”され、ウェブサービスから氏名や住所などの顧客情報を窃取される事件が継続的に発生した、というものである。また、7 位「ウェブサイトの改ざん」は、企業や組織のウェブサイトにおいて、利用者が閲覧するだけでウイルスに感染するように”脆弱性を悪用”して改ざんされる、というものである。そして、9 位「脆弱性公表に伴う攻撃」は、OpenSSL や GNU bash などの、広く利用されているソフトウェアの脆弱性公表が相次ぎ、それにあわせてその”脆弱性を悪用”した攻撃による被害も多数発生している、というものである。

[3] 日本国内に加えて海外の情報も日本語に翻訳して公開をしている脆弱性対策情報のデータベース。「脆弱性対策情報データベース JVN iPedia」http://jvndb.jvn.jp/index.html

[4] 「情報セキュリティ 10 大脅威 2015」https://www.ipa.go.jp/security/vuln/10threats2015.html

いずれかの攻撃を受けた場合には、利用者の個人情報を盗まれる、サービス停止させられる、といった被害だけでなく、盗まれた個人情報を利用して成りすましなどにより金銭的な被害が発生する、といった、被害が拡大するケースも多い。

1.2. 2014 年に注目された脆弱性

どのようなソフトウェアにも脆弱性は存在する。これは OpenSSL や GNU bash のように、広く普及し、かつ長く利用されてきた、いわゆる（脆弱性の）枯れたソフトウェアであっても同様である。2014 年はこのようなソフトウェアの脆弱性が発見され、世間でも広く注目された。以下に 2014 年に注目された脆弱性について説明する。

■ OpenSSL 関連の脆弱性

OpenSSL は、認証や暗号に利用されるライブラリである。2014 年に公表された OpenSSL の脆弱性の代表的なものは以下の 2 つである。

1 つは 2014 年 4 月 7 日に公表された脆弱性[5]であり、HeartBleed と呼ばれる。この脆弱性は、OpenSSL を利用しているウェブサーバに細工したリクエストを送信することで、メモリの一部を窃取可能となる。多くのウェブサーバは OpenSSL を利用しており、影響範囲は広い。この脆弱性が悪用された場合、暗号通信のための秘密鍵、ユーザの ID やパスワード、クレジットカード情報等、サーバ内に存在するデータが窃取される可能性がある。この脆弱性は攻撃コードが公開されており、実際に悪用されたことにより、クレジットカード会社のウェブサイトから個人情報が窃取されるインシデントも発生した。

もう 1 つの脆弱性は 2014 年 10 月 16 日に公表された Poodle である。この脆弱性は、中間者攻撃を含む複数の条件を満たした場合、暗号通信の一部を解読される可能性がある。多くのウェブサーバは OpenSSL を利用しており、前述の HeartBleed と同様に影響範囲は広い。ただし HeartBleed は攻撃コードが公開されており、悪用も容易であったが、Poodle は 2015 年 2 月時点で攻撃コードが一般には公開されていない。また、実際に悪用するためには中間者攻撃を前提とするなど、意味のあるデータの解読を現実的な時間内で行うことが難しい脆弱性であった。

■ GNU bash の脆弱性

GNU bash は CentOS 等の各種 Linux ディストリビューションにおいて、標準のシェルに設定されている。2014 年 9 月 24 日に公表された GNU bash の脆弱性[6]は、ShellShock と呼ばれ、脆弱性が存在するコンピュータに対して任意の OS コマンドが実行可能となる。本脆弱性は脆弱性情報の公表とほぼ同時に攻撃コードが公開された。また、ルータや NAS などのネットワーク対応機器の中には、OS に Linux を採用し、GNU bash を使用しているものがあり、このような機器への

[5] 脆弱性の CVE-ID は CVE-2014-0160。CVE の用語解説は 2 章を参照。
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[6] 脆弱性の CVE-ID は CVE-2014-6271 等。CVE の用語解説は 2 章を参照。
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

攻撃も確認[7]されている。ルータや NAS などのネットワーク対応機器は、脆弱性対策情報が公表されたとしても単純にバージョンアップできず、その対策情報を元にネットワーク対応機器の販売元・開発元から対策済みのファームウェアが提供されない限り、対策することができない。このため対策が行えない、または対策を実施するまでに時間がかかるケースもあることが想定される。ネットワーク対応機器に限った話ではないがシステム管理者は、脆弱性公表時に即座にパッチを適用できないケースを想定した運用方針を事前に決めておくことも必要である。

[7] Bash の脆弱性を標的としたアクセスの観測について（第 3 報）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141209-2.pdf

2. 効果的な脆弱性対策を行うには

1 章では、脆弱性対策情報がすでに多数公表されており、攻撃者がその脆弱性を悪用した攻撃をすることで、個人情報が窃取されるなどの被害を受ける可能性があることを解説した。本章では、そういった多数の脆弱性関連情報を自組織の脆弱性対策にどのように活用をすればよいか、といった点について概説を行う。

2.1. 脆弱性情報の収集／脆弱性対策に必要な基礎知識

まず、多数の脆弱性関連情報の内容把握や対策実施に備えて、セキュリティに関する用語や指標のいくつかは事前に理解をしておくことが望ましい。特に重要な用語や指標は以下の 3 つになる。

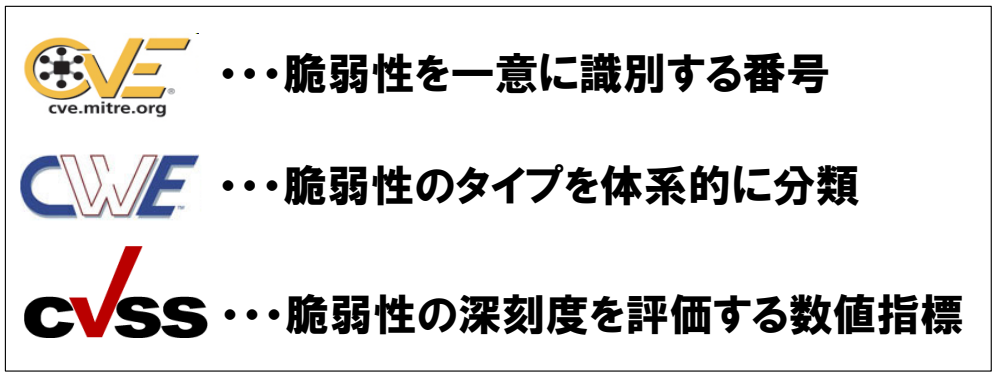

図 2-1-1：セキュリティに関する指標などの用語（特に重要なもの）

① 脆弱性を識別するための CVE

個別製品中の脆弱性に一意の識別番号「CVE 識別番号（CVE-ID）」を付与することにより、組織 A の発行する脆弱性対策情報と、組織 B の発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したりできる。詳細は以下の URL を参照のこと。

参考：共通脆弱性識別子 CVE 概説（Common Vulnerabilities and Exposures）
https://www.ipa.go.jp/security/vuln/CVE.html

② 脆弱性の種類を識別するための CWE

ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準。脆弱性検査ツールなど、ソフトウェアのセキュリティを向上させるためのツールの標準の評価尺度として使用可能。詳細は以下の URL を参照のこと。

参考：共通脆弱性タイプ一覧 CWE 概説（Common Weakness Enumeration）
https://www.ipa.go.jp/security/vuln/CWE.html

③　脆弱性の深刻度を評価するための CVSS

情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法を提供している。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。詳細は以下の URL を参照のこと。（2.2 章でも評価方法等を概説）

> 参考：共通脆弱性評価システム概説（Common Vulnerability Scoring System）
> https://www.ipa.go.jp/security/vuln/CVSS.html

2.2. 効果的な脆弱性対策の進め方

同じ社内システムの脆弱性でも、攻撃者がインターネット経由で悪用できる脆弱性と、脆弱性のあるソフトウェアがインストールされている機器に直接接続してアクセスする必要がある脆弱性とでは、攻撃の容易さという観点からリスクが異なる。同様に、同じウェブサイトの脆弱性でも、個人情報や業務情報を一切持たない告知目的の企業サイトと、オンラインショッピングサイトのような個人情報やクレジットカード情報を保有しているサイトでは、ビジネスへの影響という観点からリスクが異なる。また、脆弱性対策情報の公表後、攻撃が広く行われるようになる前に対策を行えば当該脆弱性に対する攻撃を防ぐことができる。反対に、対策を行わず脆弱性を放置すると、攻撃者や攻撃手法が多様化して攻撃が急増し、被害に遭うリスクも増大する。

つまり、効果的な脆弱性対策とは、全ての脆弱性について闇雲に対策を行うのではなく「被害を受けた際のリスクを考慮して行うこと」、また、「時機を逸さずに行うこと」がポイントとなる。

2.2.1. 収集から分析までの流れ

効果的な脆弱性対策を実施するには、多数の情報から自組織に関連する情報の収集を行い、組織内への影響度合いを早期に判断することが重要となる。以下は情報収集から分析までのイメージになる。

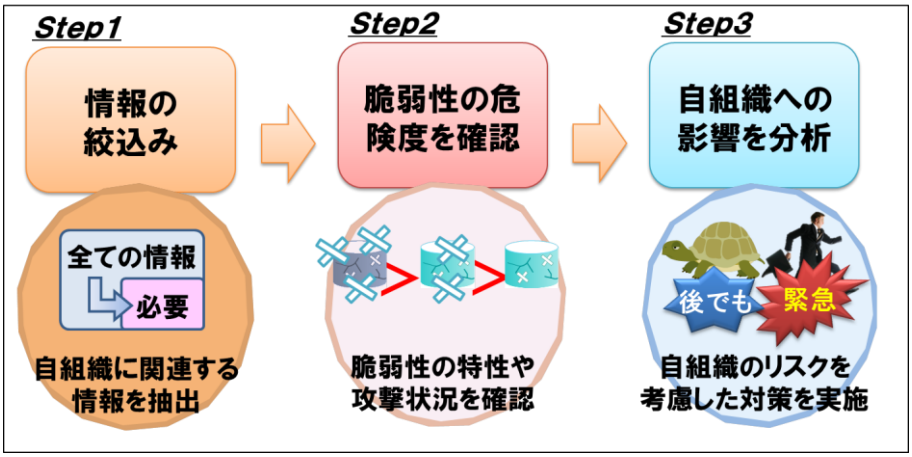

図 2-2-1：情報収集から分析までのイメージ図

①　Step1　情報の絞込み

多数の脆弱性関連情報から自組織に関連していると思われるソフトウェアの情報を収集する。2.2.2 項で紹介する参考 URL などを参照してサイトを選別して収集する、あるいは 3 章で説明す

るIPAの提供するサービスやツールなどを使用して自組織で利用しているソフトウェアの脆弱性対策情報のみを収集する、といった手段がある。

② Step2 脆弱性の危険度(深刻度)を確認

ベンダーや脆弱性関連情報データベースで公開している脆弱性関連情報にCVSS基本値や攻撃状況に関する情報が含まれているかを確認する。それらの情報が含まれている場合にはStep3の分析時に利用する。CVSSの基本的な考え方については2.2.3項「共通脆弱性評価システムCVSSとは」を参照のこと。

③ Step3 自組織への影響を分析

Step1とStep2で収集した情報を元に、該当の脆弱性が自組織のシステムにどの程度の被害を与える可能性があるかを分析する。脆弱性自体の危険度が低い場合でも、対象システムが重要なサービスなどを提供しており、被害による影響が大きい場合などは、自組織への影響が大きくなるケースもあり、またそのサービスの利用者にも影響がある。自組織における評価例については、2.2.4項「CVSSを使って自組織のシステムを評価した例」を参照のこと。

2.2.2. 情報収集に有効なURL一覧

組織内のシステム管理者などは、自組織内で使用しているソフトウェアやそのソフトウェアのバージョン情報を元に、ウェブサイト等から脆弱性関連情報を選別して収集することが効率的である。以下に情報収集のイメージを記載する。

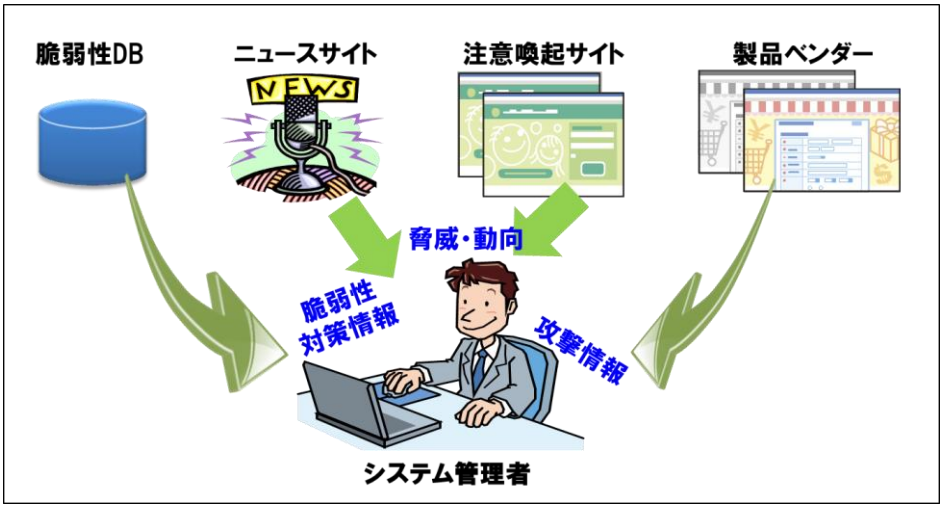

図2-2-2：情報収集のイメージ図

情報収集をする際に参考となる URL の一覧を下表に記載する。自組織に有用なサイトや情報を選別して定常的な情報収集を実施することが重要である。

表 2-2-1：情報収集時の参考ＵＲＬ一覧

種別	URL
脆弱性関連情報データベース	■国内 ・JVN (Japan Vulnerability Notes) http://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia http://jvndb.jvn.jp/ ■海外 ・NVD(National Vulnerability Database) http://nvd.nist.gov/ ・Vulnerability Notes Database http://www.kb.cert.org/vuls/ ・Metasploit (攻撃情報あり) http://www.metasploit.com/ ・Exploit Database (攻撃情報あり) http://www.exploit-db.com/
ニュースサイト	■国内 ・CNET ニュース：セキュリティ http://japan.cnet.com/news/sec/ ・ITmedia エンタープライズ セキュリティ http://www.itmedia.co.jp/enterprise/subtop/security/index.html ・ITpro セキュリティ http://itpro.nikkeibp.co.jp/security/index.html ■海外 ・ComputerWorld Security （米国中心） http://www.computerworld.com/category/security0 ・The Register Security （英国・欧州中心） http://www.theregister.co.uk/security/
注意喚起サイト	■国内 ・IPA：重要なセキュリティ情報一覧 https://www.ipa.go.jp/security/announce/alert.html ・JPCERT/CC 注意喚起 http://www.jpcert.or.jp/at/ ・警察庁：警察庁セキュリティポータルサイト http://www.npa.go.jp/cyberpolice/ ■海外 ・米国：US-CERT http://www.us-cert.gov/ncas ・米国：ICS-CERT http://ics-cert.us-cert.gov/
製品ベンダー	■定例アップデート ・マイクロソフト　TechCenter （毎月第 2 火曜日 更新） http://technet.Microsoft.com/ja-jp/security/default.aspx ・オラクル　Critical Patch Update　（年 4 回 1,4,7,10 月の 17 日に近い火曜日） http://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html
	■クライアント製品など ・アップル http://support.apple.com/kb/HT1222?viewlocale=ja_JP ・アドビ （Adobe Reader/Adobe Flash Player など） http://helpx.adobe.com/jp/security.html ・Mozilla （FireFox/ThunderBird など） http://www.mozilla-japan.org/security/known-vulnerabilities/

種別	URL
	■サーバ、ネットワーク製品など ・シスコ　– セキュリティアドバイザリ http://www.cisco.com/cisco/web/support/JP/loc/security/index.html ・HP - サポートセンター https://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/secBullArchive ・日立 –セキュリティ情報 http://www.hitachi.co.jp/hirt/security/index.html ・富士通 - セキュリティ情報 http://www.fujitsu.com/jp/support/security/ http://software.fujitsu.com/jp/security/ ・NEC - NEC 製品セキュリティ情報 http://jpn.nec.com/security-info/ ・IBM –重要セキュリティ情報 http://www-06.ibm.com/jp/services/security/info/index.html ・Red Hat – Errata https://rhn.redhat.com/errata/
	■セキュリティ製品など ・シマンテック –セキュリティアップデート http://www.Symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory
	■オープンソースなど ・Apache Foundation http://httpd.apache.org/　（Apache HTTP サーバ） http://tomcat.apache.org/　（Apache Tomcat） http://struts.apache.org/　（Apache Struts） ・ISC　（Internet Systems Consortium） http://www.isc.org/downloads/bind/　（BIND） http://www.isc.org/downloads/dhcp/　（DHCP） ・OpenSSL http://www.openssl.org/

2.2.3. 共通脆弱性評価システム CVSS とは

脆弱性関連情報の収集後、自組織への影響度を把握するために、共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）を脆弱性対策の優先度付けなどに活用をすることが可能である。CVSS による評価方法のイメージは図 2-2-3 を参照のこと。

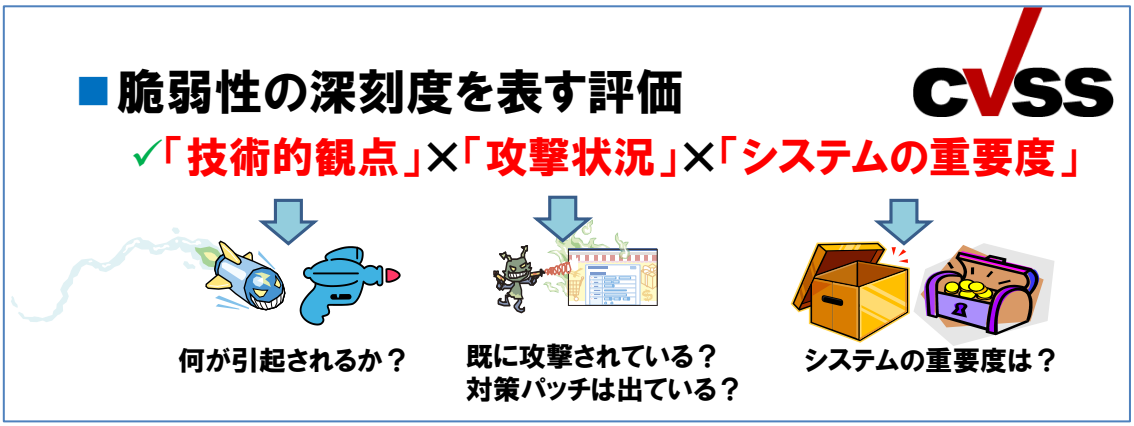

図 2-2-3：CVSS による評価方法のイメージ図

図 2-2-4 は CVSS の評価基準の一覧をイメージで表したものである。0.0 から 10.0 までのスコア値で脆弱性の危険度を評価し、値が大きいほど、攻撃が容易で、攻撃を受けた際の影響（損害）が大きいことを意味している。

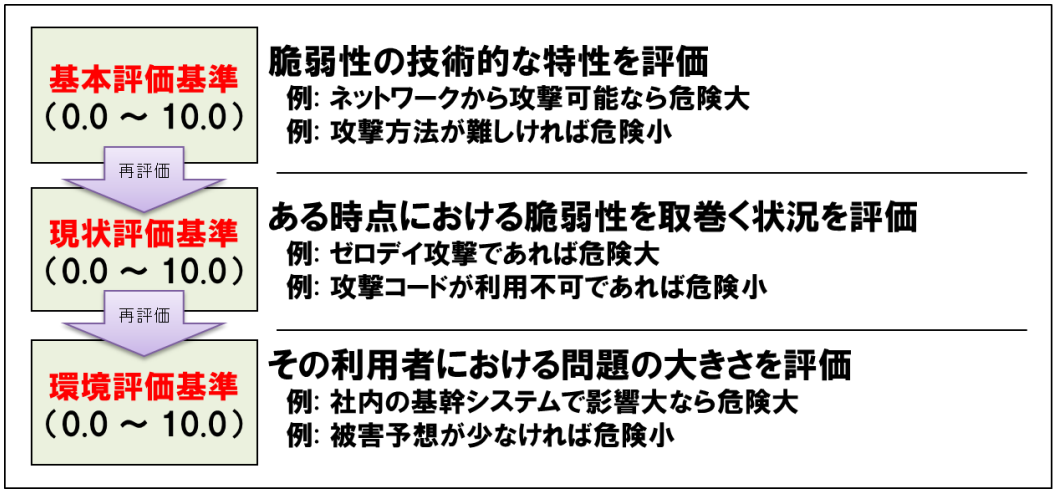

図 2-2-4：CVSS の評価基準の一覧イメージ

CVSS の詳細説明は、「共通脆弱性評価システム CVSS 概説」
https://www.ipa.go.jp/security/vuln/CVSS.html　も参照のこと。

① 基本評価基準

脆弱性そのものの特性を評価する基準である。通常はセキュリティ関連組織やベンダーなどが評価を行うため、システム管理者側では評価は行わない。

表 2-2-2 に基本評価基準の評価項目一覧を記載する。評価項目毎の選択肢から脆弱性の技術的な特性（ネットワークから攻撃可、機密情報は漏えいするが改ざんやサービス停止などの影響はない、等）を把握することも可能である。

表 2-2-2：CVSS 基本評価基準の評価項目一覧

危険小 ⟷ 危険大

	評価項目	選択肢・ポイント		
攻撃の難易度	どこから攻撃可能であるか 攻撃元区分 (AV Access Vector)	ローカル L	隣接N/W A	ネットワーク N
	攻撃する際に必要な条件の複雑さ 攻撃条件の複雑さ (AC Access Complexity)	高 H	中 M	低 L
	攻撃するために認証が必要であるか 攻撃前認証要否 (Au Authentication)	複数 M	単一 S	不要 N
攻撃による影響	機密情報が漏えいする可能性 機密性への影響 (C Confidentiality Impact)	なし N	部分的 P	全面的 C
	情報が改ざんされる可能性 完全性への影響 (I Integrity Impact)	なし N	部分的 P	全面的 C
	業務が遅延・停止する可能性 可用性への影響 (A Availability Impact)	なし N	部分的 P	全面的 C

② 現状評価基準

脆弱性の評価時点の深刻度を評価する基準である。時間の経過とともに攻撃や対策を取り巻く状況も変化するためスコア値は一定の値にはならない。現状評価基準を算出するセキュリティ関連組織やベンダーは少ないため、通常は「未評価」という選択肢の利用がより現実的である。

表 2-2-3 に現状評価基準の評価項目一覧を記載する。「未評価」という選択肢を行った場合には、それぞれの評価項目において危険度が最も大きいものを選択したことと同じ意味になる。

表 2-2-3：CVSS 現状評価基準の評価項目一覧

危険小 ⟷ 危険大

評価項目	選択肢・ポイント			
攻撃コード・攻撃手法が実際に利用可能であるか 攻撃可能性 (E Exploitability)	未実証 U	実証可 P	攻撃可 F	容易 H
対策がどの程度利用可能であるか 対策のレベル (RL Remediation Level)	正式 O	暫定 T	非公式 W	なし U
情報の信頼性 情報信頼性 (RC Report Confidence)	-	未確認 UC	未確証 UR	確認済 C

※すべての項目で未評価 (ND:この項目を評価しない) という選択肢があります。

③ 環境評価基準

製品利用者の環境も含め、最終的な脆弱性の深刻度を評価する基準である。攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価する。

この基準による評価結果は、脆弱性に対して想定される脅威に応じて、製品利用者毎に変化する。事前にシステム毎の環境評価を実施しておくことで、迅速なスコア値の算出が可能となる。

表 2-2-4 に環境評価基準の評価項目一覧を記載する。すべての評価項目を使用して評価をするのは手間がかかるため、一部の評価項目で簡易に評価を実施する方法を後述する。

表 2-2-4：CVSS 環境評価基準の評価項目一覧

危険小 ⟷ 危険大

	評価項目	選択肢				
影響範囲	**システムからの二次的被害の可能性** 二次的被害 (CDP Collateral Damage Potential)	なし N	軽微 L	中程度 LM	重大 MH	壊滅的 H
影響範囲	**システムの影響範囲** システム範囲 (TD Target Distribution)	-	なし N	小規模 L	中規模 M	大規模 H
情報の重要度	**システムにおける機密性の重要度** 機密性の要求度 (CR Confidentiality Requirement)	-	-	低 L	中 M	高 H
情報の重要度	**システムにおける完全性の重要度** 完全性の要求度 (IR Integrity Requirement)	-	-	低 L	中 M	高 H
情報の重要度	**システムにおける可用性の重要度** 可用性の要求度 (AR Availability Impact)	-	-	低 L	中 M	高 H

※すべての項目で未評価 (ND:この項目を評価しない) という選択肢があります。

2.2.4. CVSS を使って自組織のシステムを評価した例

自組織のシステムの CVSS 評価を実施するにあたって、ここまでの評価項目すべてを選択して分析をすることは非常に労力がかかるため現実的には実施が困難なことがある。このため、現状評価は評価を行わず、リスクを最大と判断して、環境評価はその一部のみを使ってスコア算出をする、という方法をとることで、労力を抑えて評価することができる。自組織のシステムを評価する事例を以下に記載する。

通常、CVSS による環境評価を実施する場合は、表 2-2-4「CVSS 環境評価基準の評価項目一覧」にある、5 つの評価項目(二次的被害、影響範囲、機密性・完全性・可用性の重要度)を評価する必要がある。図 2-2-5 は、IPA 内で評価実施の検証をした際の環境評価基準の事例である。 2 つの評価項目(二次的被害、影響範囲)のみネットワークセグメント別に 4 パターンに分け評価を行い、機密性・完全性・可用性は未評価固定として環境評価を行っている。組織の規模やシステムの構成によっては、パターン数を増減することも有効である。

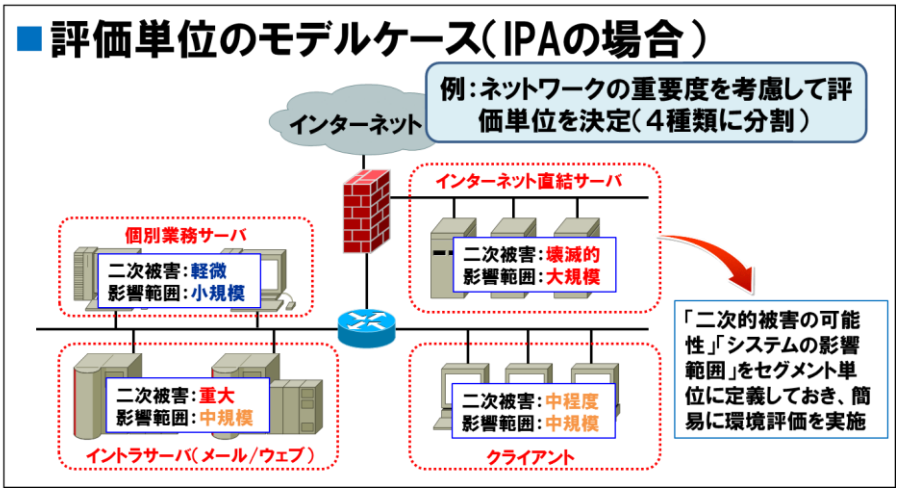

図 2-2-5：環境評価のイメージ（IPA の場合）

表 2-2-5 は、図 2-2-5 の環境評価基準の評価項目を比較した一覧になる。ネットワークセグメントの重要度に応じて選択肢が変化していることが見てとれる。

表 2-2-5：環境評価 評価項目の比較イメージ（IPA の場合）

■インターネット直結サーバ

評価項目	選択肢				
システムからの二次的被害の可能性	なし	軽微	中程度	重大	**壊滅的**
システムの影響範囲	-	なし	小規模	中規模	**大規模**

■イントラサーバ(メール/ウェブ)

システムからの二次的被害の可能性	なし	軽微	中程度	**重大**	壊滅的
システムの影響範囲	-	なし	小規模	**中規模**	大規模

■クライアント

システムからの二次的被害の可能性	なし	軽微	**中程度**	重大	壊滅的
システムの影響範囲	-	なし	小規模	**中規模**	大規模

■個別業務サーバ

システムからの二次的被害の可能性	なし	**軽微**	中程度	重大	壊滅的
システムの影響範囲	-	なし	**小規模**	中規模	大規模

図 2-2-6 は、図 2-2-5 と表 2-2-5 の評価パターンを元にして環境値を算出した例である。基本値を 5.0、現状値を「未評価」という選択をした場合、システムの重要度が最も高い「インターネット直結サーバ」は環境値が 7.5、重要度が最も低い「個別業務サーバ」は環境値が 1.4 になる。

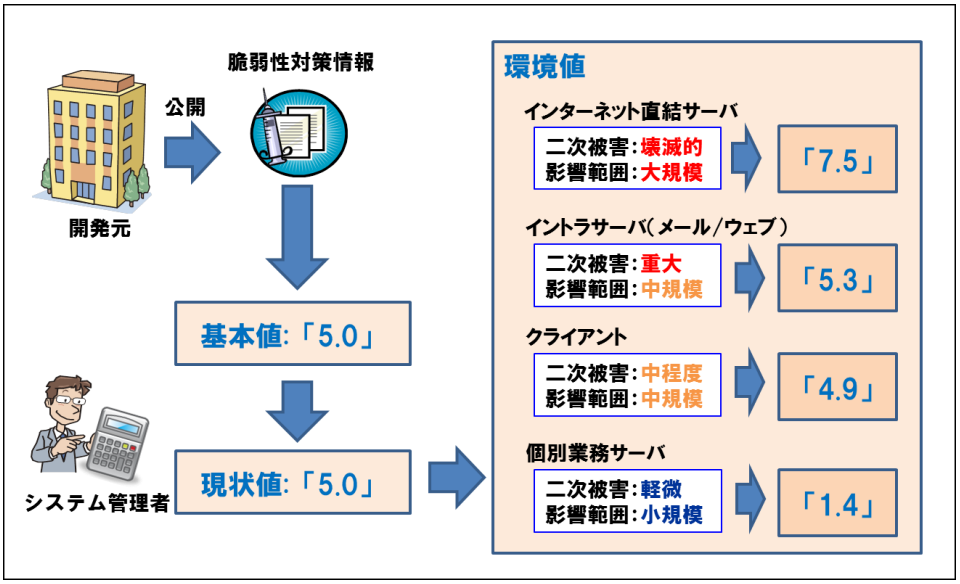

図 2-2-6：環境値の算出イメージ（IPA の場合）

この算出した環境値を対策時の優先度判断に利用することで、効果的な脆弱性対策に活用をすることが可能になる。例えば 7.0 以上のスコア値は即日対応が必須、4.0 以上 7.0 未満は 3 日以内の対応が必須、などの判断材料として利用をすることが可能である。

もし即日対応が必須で、適用するパッチが提供されていない場合は、攻撃された際の被害や影響を考慮して、パッチが適用できるまで一般へのサービス公開を停止する、あるいは、公開先を限定することで被害を最小限に食い止めるようにする、といった想定をしておくことが重要である。

3. IPA 提供のサービス等を活用した脆弱性対策

脆弱性情報は日々公開され、脆弱性を放置すると時間とともに被害にあうリスクが高まっていく。本来であれば、自組織・製品に関わる公開されている全ての脆弱性に対策を行う必要がある。しかし、通常の運用の中ですべての脆弱性に対策を行うには、パッチの適用に関わる動作検証など膨大な時間とコストがかかってしまう。そのため、2 章 図 2-2-1 の Step1～Step3 を意識した脆弱性対策が重要となる。本章では、それらを意識した脆弱性対策を行う上で役立つ IPA 提供のサービスやツールの概要および活用方法を紹介する。

3.1. IPA が提供するサービス・ツール一覧

IPA では脆弱性対策情報の早期把握、収集、活用のそれぞれのフェーズに役立つ支援ツールやサービスを公開している。以下に一覧を記載する。

表 3-1-1：IPA が提供する脆弱性対策支援サービス・ツールの抜粋

フェーズ	目的	サービス・ツール名	関連リンク等
早期把握	脆弱性情報の収集（緊急度・危険度高）	IPA 重要なセキュリティ情報	https://www.ipa.go.jp/security/announce/about.html（概要）
			https://www.ipa.go.jp/security/announce/alert.html（一覧）
			https://twitter.com/ICATalerts/（twitter @ICATalerts）
	脆弱性情報の受信（組織内への案内等）	サイバーセキュリティ注意喚起サービス icat	https://www.ipa.go.jp/security/vuln/icat.html
収集	脆弱性情報の収集（すべての脆弱性）	脆弱性対策情報データベース JVN iPedia	http://jvndb.jvn.jp/
			https://twitter.com/jvnipedia/（twitter @JVNiPedia）
	脆弱性情報の収集（自組織すべて）（システム毎）（開発製品毎）	MyJVN 脆弱性対策情報収集ツール	http://jvndb.jvn.jp/apis/myjvn/mjcheck3.html（Adobe Air 版）
			http://jvndb.jvn.jp/apis/myjvn/mjcheck.html（Adobe Flash 版）
活用	自組織への脆弱性の影響度を確認	CVSS 計算ソフトウェア	http://jvndb.jvn.jp/cvss/ja.html
	PC の主要ソフトウェアが最新かを確認	MyJVN バージョンチェッカ	http://jvndb.jvn.jp/apis/myjvn/vccheck.html（JRE 版）
			http://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html（.Net Framework 版）

上記のサービス・ツールを活用することで、効率的な脆弱性対策情報の収集や危険度の判断を行うことができる。次節より、システム管理者やソフトウェアの開発者の脆弱性対策に特に有効な「IPA 重要なセキュリティ情報」「脆弱性対策情報データベース JVN iPedia」「MyJVN 脆弱性対策情報収集ツール」「CVSS 計算ソフトウェア」について概要および活用方法を解説する。

3.2.「IPA 重要なセキュリティ情報」- 緊急性の高い脆弱性情報の収集に -

■概要

利用者が多いソフトウェアにおいて、現在攻撃が発生している緊急度の高い脆弱性を「緊急」レベル、影響度は広いが攻撃が発生していないと判断した脆弱性を「注意」レベルとして対策方法等を含めて情報を発信する。発信方法として、ウェブサイトでの公開やメール、twitter での配信を行っている。

図 3-2-1：重要なセキュリティ情報

■活用方法

① 定期的に IPA の HP を確認する。または、メール配信の登録や twitter をフォローし情報を随時受け取れるようにする。

重要なセキュリティ情報一覧：https://www.ipa.go.jp/security/announce/alert.html
Twitter　：https://twitter.com/ICATalerts/
メール配信登録　：https://www.ipa.go.jp/about/mail/index.html

② ①の情報から新着情報を確認した場合、その新着情報の詳細情報を確認する。

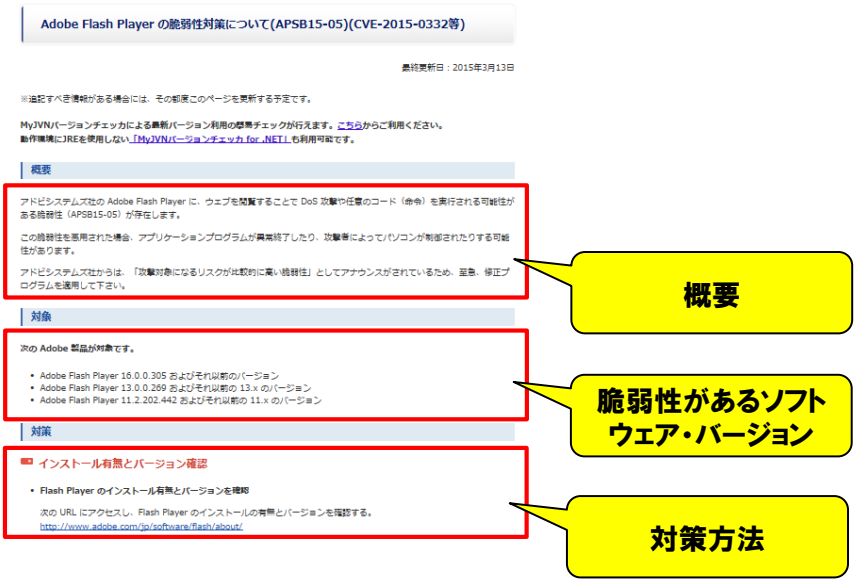

図 3-2-2：重要なセキュリティ情報の詳細ページ

③ 自組織のシステムや開発製品に影響がある脆弱性であった場合、記載されている対策方法に従い対策を実施する。

3.3.「脆弱性対策情報データベース JVN iPedia」- 日々の脆弱性の収集に -

■概要

国内外の脆弱性対策情報を収集・蓄積しているデータベース。脆弱性の概要やCVSS値､関連リンク等を掲載している。CVSS 値を確認することで、脆弱性自体の深刻度を確認することができる。2015 年 3 月末時点で 53,000 件以上のデータを蓄積している。

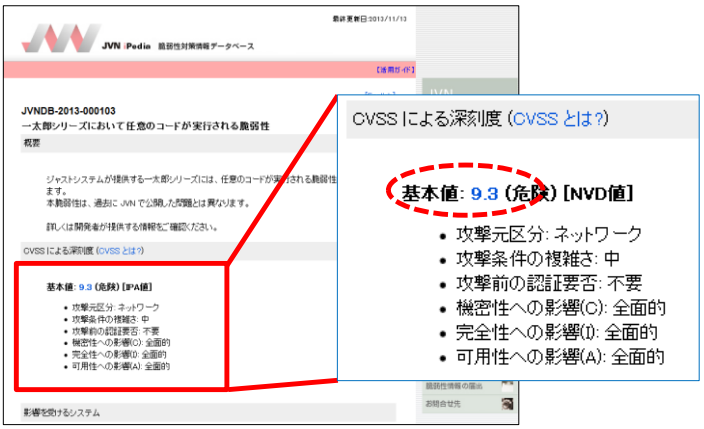

図 3-3-1：JVN iPedia

■活用方法

① JVN iPedia の検索ページにアクセスし、キーワードまたは、自組織・開発製品で利用しているソフトウェアを指定して検索を実施する。

JVN iPedia 検索ページ：

http://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja

図 3-3-2：JVN iPedia 検索ページ

② 表示された脆弱性対策情報一覧から詳細を確認し、脆弱性の概要や CVSS 値、影響を受けるソフトウェアやそのバージョン、対策方法等を確認する。

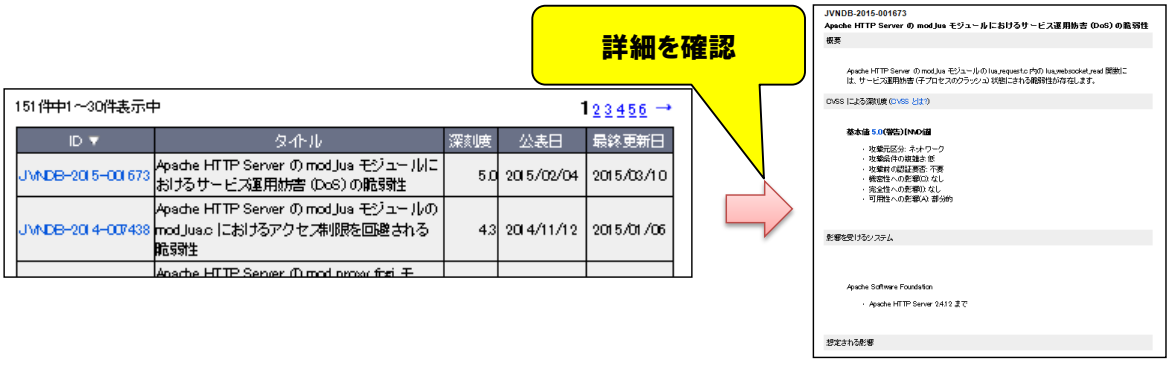

図 3-3-3：JVN iPedia 検索ページから詳細情報の確認

3.4.「MyJVN 脆弱性対策情報収集ツール」- 自組織に関わる脆弱性の収集に -

■概要

JVN iPedia で収集・蓄積している脆弱性対策情報に対して自組織に関係のあるソフトウェアや CVSS 値が高い脆弱性などの条件を指定し、脆弱性対策情報を抽出することができるツール。自組織に関わる脆弱性で対策の優先度が高い脆弱性を抽出し、効率的に脆弱性の収集を行うことができる。

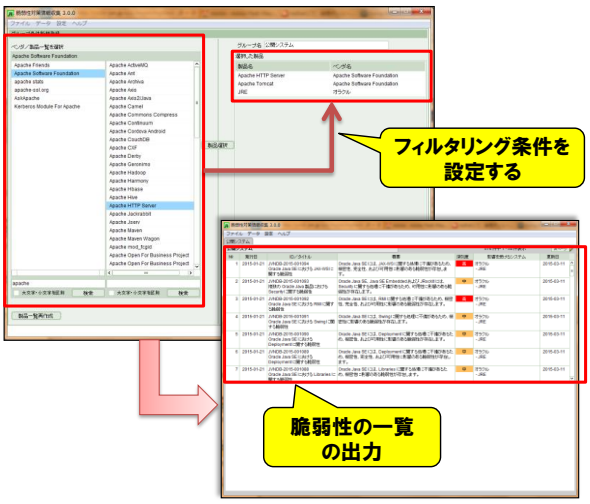

図 3-4-1：MyJVN 脆弱性対策情報収集ツール

■活用方法

① IPA の HP より MyJVN 脆弱性対策情報収集ツール Adobe Air 版（通称、mjcheck3）をダウンロードし、起動する、または、ブラウザ上で Adobe Flash 版（通称、mjcheck）を起動する。

Adobe Air 版　　：http://jvndb.jvn.jp/apis/myjvn/mjcheck3.html

Adobe Flash 版　：http://jvndb.jvn.jp/apis/myjvn/mjcheck.html

② 収集したいベンダーの製品名やフィルタリングするキーワードを設定する。（以降図は mjcheck3 版）

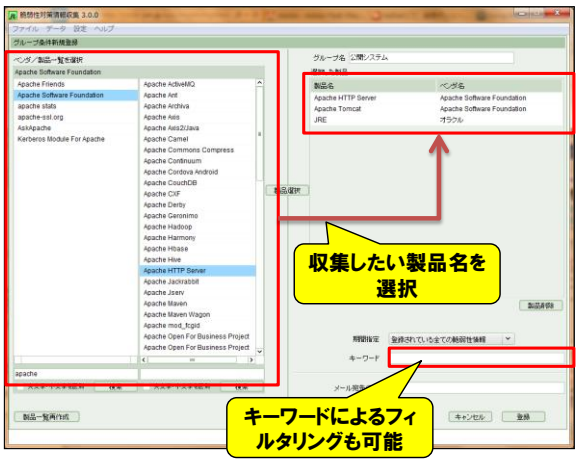

図 3-4-2：MyJVN 脆弱性対策情報収集ツール　フィルタリング条件の指定

参考）フィルタリング例

・サーバ環境でよく使われる製品を収集したい

表 3-4-1：サーバ環境でよく使われる製品一覧

ベンダー名	製品名
Apache Software Foundation	Apache HTTP Server
Apache Software Foundation	Apache Tomcat
Apache Software Foundation	Apache Struts

オラクル	JRE
オラクル	MySQL
ISC, Inc.	BIND
OpenSSL Project	OpenSSL
The PHP Group	PHP

・クライアント環境でよく使われる製品を収集したい

表 3-4-2：クライアント環境でよく使われる製品一覧

ベンダー名	製品名
アドビシステムズ	Adobe Flash Player
アドビシステムズ	Adobe Reader
オラクル	JRE
Mozilla Foundation	Mozilla Firefox
Mozilla Foundation	Mozilla Thunderbird
Google	Google Chrome
マイクロソフト	Internet Explorer

③ ②で指定したフィルタリング条件に基づいて情報が収集される。上部の一覧を選択することで下部に脆弱性の詳細が表示され、より詳しく情報確認することができる。

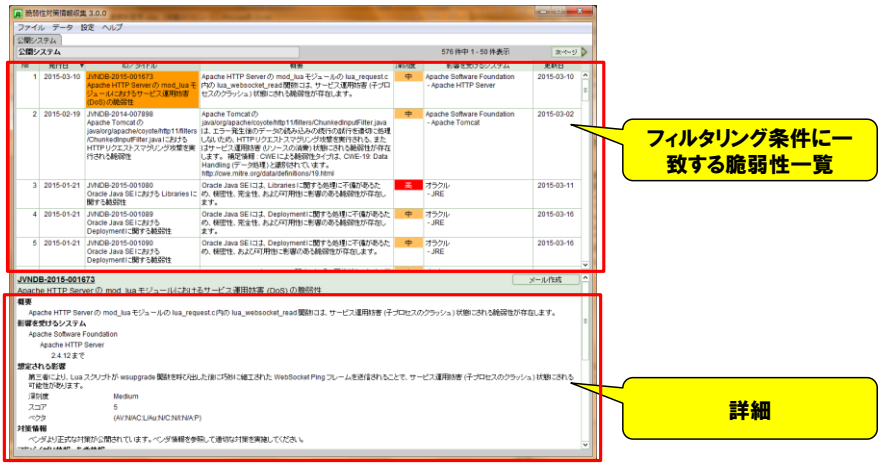

図 3-4-3：MyJVN 脆弱性対策情報収集ツール脆弱性一覧

④ 詳細を組織内に展開したい場合は、メール生成機能により、脆弱性の内容が記載されたメールを自動生成することができる。

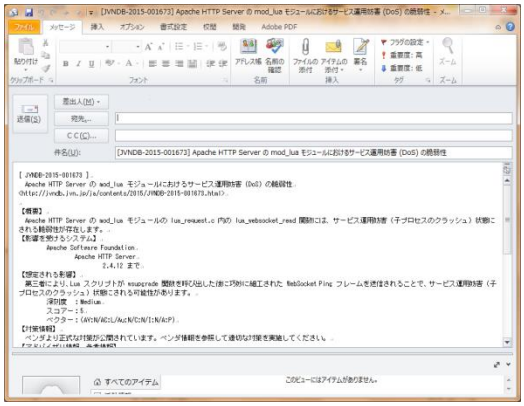

図 3-4-4：脆弱性情報のメール自動生成

3.5.「CVSS 計算ソフトウェア」- 脆弱性の自組織への影響度の確認に -

■概要

脆弱性の危険度を数値化した CVSS の計算を行うツール。脆弱性対策情報の公開時にセキュリティ関連組織やベンダーから公表されるのは CVSS 基本値のみとなるケースが多く、CVSS 現状値や CVSS 環境値は組織毎に算出する必要がある。本ツールを利用することで、複雑な CVSS 値の計算を評価項目から選択するだけで簡単に計算することができる。

図 3-5-1：CVSS 計算ソフトウェア

■活用方法

① JVN iPedia の検索ページにアクセスし、CVSS を確認したい脆弱性を検索し詳細画面を開く。

② 詳細画面の CVSS 値の箇所から CVSS 計算ソフトウェアを起動する。CVSS 計算ソフトウェアでは基本値が入力された状態で起動される。

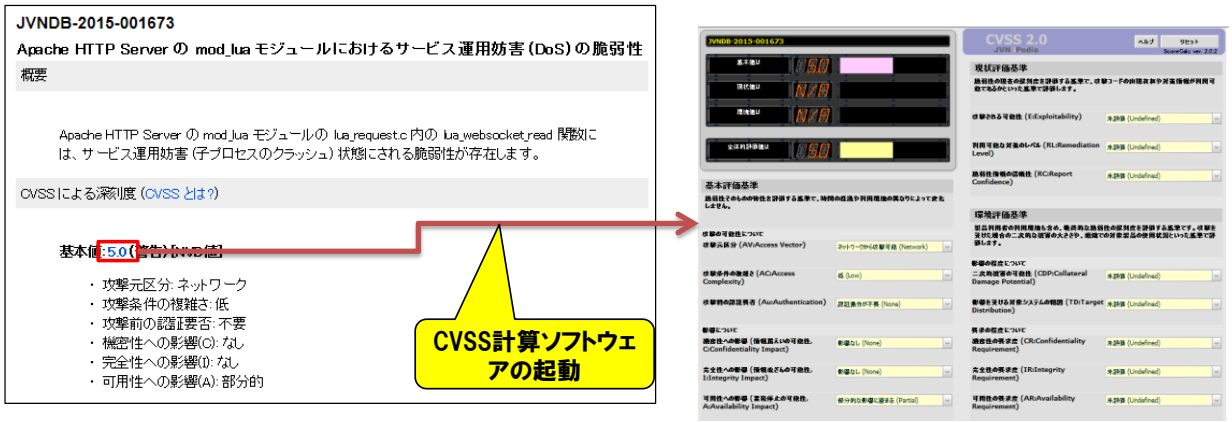

図 3-5-2：CVSS 計算ソフトウェアの起動

③ 該当する現状評価項目や環境評価項目を選択し、現状に即した現実的なスコア値を算出することができる。

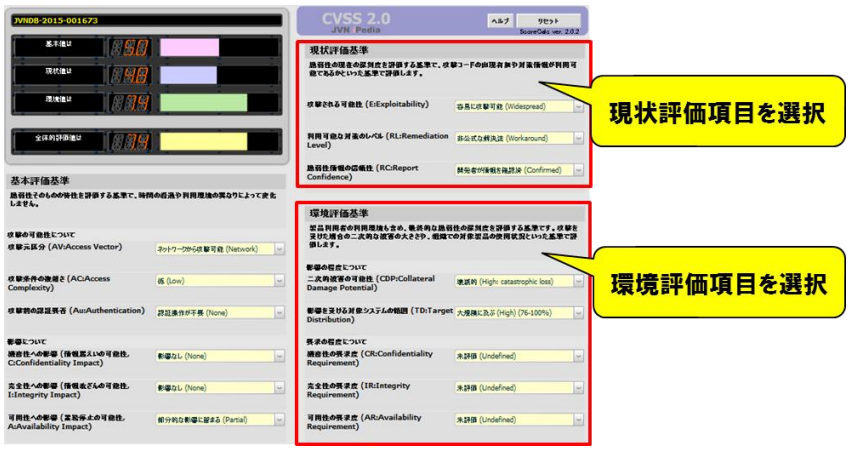

図 3-5-3：現状評価と環境評価を含めた計算例

おわりに

本書では、効果的な脆弱性対策を行うために、情報収集や自組織のシステムにおける脆弱性対策の優先度付けの方法などについて、解説を行った。

脆弱性は日々発見され、攻撃者が悪用できる新たな脆弱性は増え続ける。昨今では脆弱性の発見から攻撃に使われるようになるまでに掛かる時間は短縮されてきており、時機を逸しない対策の重要性は益々高くなっている。

そうした状況の中、組織の脆弱性対策の取組みを支援するべく、自動化の取組みも国内外で進められている。組織内のシステム管理者やソフトウェア開発者は、利用可能な技術やサービスを有効に活用しつつ、（仮に）攻撃には遭っても被害を回避できる、実効性のある対策を実現して欲しい。

本書が、効果的な脆弱性対策を実施するうえでの一助になることを期待している。

IPA テクニカルウォッチ

「脆弱性対策の効果的な進め方（実践編）」

～脆弱性情報の早期把握、収集、活用のスヽメ～

[発　　行] 2015 年 3 月 31 日
[著作・制作] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター
[執　筆　者] 斉藤 良彰、亀山 友彦