IPA Technical Watch

脆弱性対策の効果的な進め方（実践編）第 2 版

～脆弱性情報の早期把握、収集、活用のスヽメ～

独立行政法人情報処理推進機構
セキュリティセンター

目次

更新履歴

公開日	版	内容
2015/03/31	第 1 版	・新規公開
2019/02/21	第 2 版	・統計情報、事例などの更新 ・各種参考情報の更新 ・CVSS に関する解説を v2 から v3 へ更新

はじめに

本書は、2015 年 3 月に公開した「脆弱性対策の効果的な進め方（実践編）」[1]を、昨今の脆弱性を取り巻く状況を踏まえて新しい情報を紹介する目的で改訂したものである。広く普及し、かつ長く利用されてきたソフトウェアの脆弱性情報は多数公表されており、その数は年々増加傾向にある。多数の商用製品やオープンソースのソフトウェアに含まれている脆弱性も多く、当該脆弱性が悪用された攻撃事例も確認されており、組織における大きな脅威となっている。

脆弱性は日々発見されているため、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み込みなど、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かつ効率的に把握、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、どのように情報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」[2]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[3]による評価手法が利用可能であることを概説した。本書は、そのレポートに基づき、より実践的な視点での脆弱性対策について記載したものである。

[1] 2015 年 3 月 31 日公開「脆弱性対策の効果的な進め方（実践編）」
https://www.ipa.go.jp/security/technicalwatch/20150331.html
[2] 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
[3] 本書では、FIRST(Forum of Incident Response and Security Teams)が 2015 年 6 月に公開した CVSS v3 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. 昨今の脆弱性を取り巻く状況

発見される脆弱性は年々増加傾向にある。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」[4]に登録されている脆弱性対策情報件数の四半期別推移である。累計の登録件数を見ると 2018 年 12 月末時点は 92,674 件となっている。2018 年も多くの脆弱性対策情報が公開されており、年間 14,264 件、月平均では約 1,190 件の情報が登録されている。本資料第 1 版公開当時、2014 年の年間登録件数は 8,128 件であり、当時と比較すると約 1.75 倍となっている。

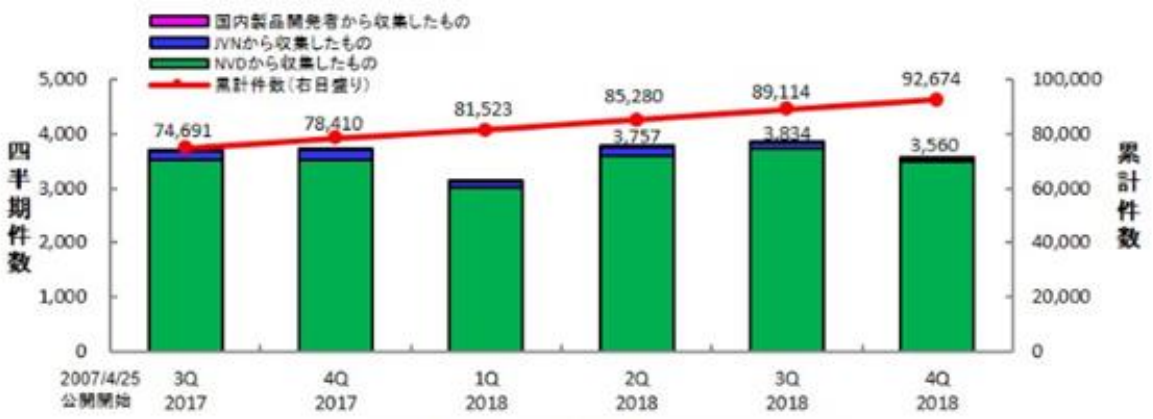

図 1-1-1：脆弱性対策情報データベース JVN iPedia の登録件数の四半期別推移

昨今では、ウェブアプリケーションを開発するためのオープンソースのフレームワークとして広く普及しているソフトウェア（Apache Strut2 など）や、コンテンツマネジメントシステム（CMS）などに関する脆弱性や、それを悪用した攻撃事例が複数公表されており、広く注目される傾向にある。このようなウェブサーバの動作に関連するソフトウェアについて脆弱性が発見された場合、当該サーバが外部公開されているケースも多いため、インターネット経由での攻撃を受ける危険性が高い。また、機微な情報を取り扱っている場合は、重大な情報漏えいの被害などに発展することも考えられる。

1.2. 昨今の広く注目された脆弱性

どのようなソフトウェアにも脆弱性は存在しうる。特に、広く普及しているソフトウェアにおいて脆弱性が発見されて悪用された場合、被害は広範囲に及ぶ可能性があるため、より注目される傾向にある。以下に、昨今の広く注目された脆弱性やそれを悪用した攻撃事例などについて概要を記載する。

[4] 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」
https://jvndb.jvn.jp/index.html

■ Apache Struts2 の脆弱性

ウェブアプリケーションを開発するためのオープンソースのフレームワークとして広く普及している Apache Struts2 では、脆弱性を悪用され深刻な被害となる事例が多発している。

特に、2017 年 3 月 7 に公表された脆弱性「CVE-2017-5638[5]」が注目を浴びた。本脆弱性は、Apache Struts2 に搭載されている「OGNL（Object Graph Navigation Language）」という式言語に関する脆弱性で、インジェクション攻撃によってリモートで任意のコードを実行される可能性がある。3 月 7 日に本脆弱性を悪用する実証コード（PoC）が公開されたことをきっかけに攻撃が多発した。国内でも実際に複数の組織が攻撃受け、数十万件単位のクレジットカード情報やメールアドレスといった個人情報が窃取される被害が出ている。また、情報の窃取だけでなく、DoS 攻撃用に感染端末をボット化するためのウイルスをダウンロード、実行させようとする事例も確認された。なお、2018 年以降もインターネット上に本脆弱性のあるサーバがないかを探索する通信も引き続き観測されている。被害が拡大した要因としては、実証コードが公開された上に比較的攻撃が容易であったことなどが考えられる。

また、2017 年 9 月 5 日に公表された「CVE-2017-9805」も、悪用されるとリモートで任意のコードを実行される可能性のある脆弱性である。本脆弱性に関しても「CVE-2017-5638」の悪用と類似した攻撃が行われ、サーバを DDoS 攻撃などの踏み台として悪用するためのものと思われるマルウェアをダウンロードさせようとする挙動が観測された。

さらに、2018 年にも「CVE-2017-5638」に類似した脆弱性「CVE-2018-11776」を悪用される被害が出ている。8 月 22 日に本脆弱性が公表された後に実証コード（PoC）が複数公開され、実際にリモートでコードを実行することによって不正に仮想通貨のマイニングを行おうとする挙動が確認された。

■ Oracle WebLogic Server の脆弱性

Oracle WebLogic Server は、多くの企業でウェブサイトや企業アプリケーションの構築などに利用されているソフトウェア製品である。この Oracle WebLogic Server のサブコンポーネントである WLS Security に対して、既知の脆弱性「CVE-2017-10271」を悪用する攻撃事例が 2017 年 12 月に確認された[6]。本脆弱性に対する修正プログラムが 2017 年 10 月にリリースされていたが、当該修正プログラムが適用されていないシステムに対して仮想通貨をマイニングさせるウイルスを仕込まれるという事例であった。

その後、2018 年 4 月 17 日には、リモートで任意のコードを実行されたり、情報を窃取されたりする可能性がある脆弱性「CVE-2018-2628」が公表された。脆弱性公表から 2 日後の 4 月 19 日に実証コード（PoC）が公開されると、その脆弱性を持つシステムを探索する目的と思われる通信が急増した。さらに、ウイルスへ感染させることを目的としたスクリプトをダウンロードさせようとする挙動なども観測されていた。

---

[5] 更新：Apache Struts2 の脆弱性対策について(CVE-2017-5638)(S2-045)(S2-046)
https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html

[6] Oracle WebLogic Server の脆弱性（CVE-2017-10271）を悪用する攻撃事例について
https://www.ipa.go.jp/security/ciadr/vul/20180115_WebLogicServer.html

また、同年 7 月 17 日には、リモートで任意のコードを実行される可能性のある脆弱性「CVE-2018-2893」も公表された。脆弱性公表から 4 日後の 7 月 21 日に本脆弱性を悪用した攻撃が行われていることが確認されている。本攻撃事例も不正に仮想通貨をマイニングさせるウイルスを仕込むことが目的であった。また、同日に公表された脆弱性「CVE-2018-2894」についても、脆弱性公表直後には実証コード（PoC）が公開されており、容易に悪用可能な状態であった。

■ Drupal の脆弱性

2018 年 4 月、オープンソースの CMS である Drupal の脆弱性「CVE-2018-7600」を悪用するための探索行為と思われる通信が、日本国内において観測された。本脆弱性を悪用することで、攻撃対象とするウェブサイトに仮想通貨をマイニングさせるウイルスや、バックドアの設置を試みるなどの挙動が確認されている。

本脆弱性は、2018 年 3 月 28 日に脆弱性情報およびその対策が公表されたもので、別名「Drupalgeddon 2.0」とも呼ばれる脆弱性で、悪用されるとリモートで任意のコードを実行される可能性がある。脆弱性の公表直後は大規模な攻撃は確認されていなかったが、4 月 12 日の実証コード(PoC)の公開後から本脆弱性の悪用に関連するものとみられる通信が多数観測された。

■ Microsoft Windows の脆弱性

2017 年 3 月、Microsoft 製品に関する脆弱性「CVE-2017-0145」などに関する修正プログラム「MS17-010[7]」が公表された。その後、2017 年 5 月に本脆弱性を悪用し、「Wanna Cryptor」と呼ばれるランサムウェアに感染させるという攻撃事例が確認された[8]。当該ランサムウェアはネットワーク経由で感染を広める機能を有しており、修正プログラムが適用されていないシステムを対象にランサムウェアの感染が拡大した。国内を含め世界各国で多くの被害が発生し、広く注目された事例である。

また、2017 年 6 月にも修正プログラム「MS17-010」が適用されていないシステムに対して「Not Petya」と呼ばれるランサムウェアに感染させられてしまう攻撃事例も確認されている。当該ランサムウェアも「Wanna Cryptor」同様、ネットワーク経由で感染を広げることが確認されており、被害が拡大することが懸念された。ただし、結果的には主にウクライナの組織において感染が確認されたもので、日本国内では被害は広がらなかった。

■ CPU の脆弱性

2018 年 1 月、投機的実行機能やアウトオブオーダー実行機能を持つ CPU に対するサイドチャネル攻撃についての情報が公表された[9]。この攻撃手法は「Spectre」、「Meltdown」と呼ばれる 2

---

[7] マイクロソフト セキュリティ情報 MS17-010 – 緊急
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2017/ms17-010

[8] 更新：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

[9] CPU に対するサイドチャネル攻撃
https://jvn.jp/vu/JVNVU93823979/

つの攻撃手法で、前者は脆弱性「CVE-2017-5753」、「CVE-2017-5715」を、後者は「CVE-2017-5754」を悪用する攻撃である。元々は 2017 年から調査が進められていた脆弱性だが、2018 年 1 月に大手 CPU メーカーが当該脆弱性の影響を受けるという見解を示したことで大きな注目を浴びた。

この脆弱性を悪用した攻撃が成功すると、メモリ内の情報が漏えいする可能性がある。「Spectre」、「Meltdown」どちらも世の中のシステムの多くが利用している CPU において影響があり、影響範囲が非常に広範なため注目された脆弱性である。

2. 効果的な脆弱性対策を行うには

1 章では、脆弱性情報は日々公表されており、攻撃者がその脆弱性を悪用した攻撃を行うことで、ソフトウェア利用者が様々な被害を受ける可能性があることを解説した。本章では、日々公開される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。知っておくと役に立つ用語や指標として以下の 3 つがある。

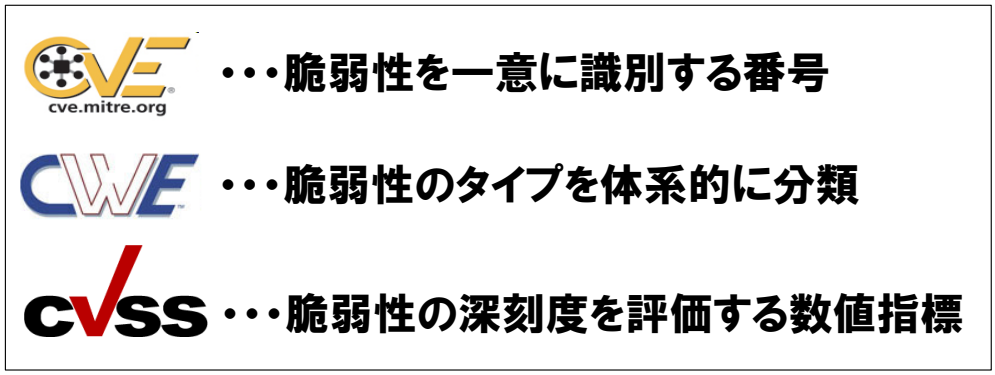

図 2-1-1：セキュリティに関する指標などの用語

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することができる。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 1：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
参考 2：共通脆弱性評価システム CVSS v3 概説(2015 年 7 月 21 日公開)
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.2. 効果的な脆弱性対策の進め方

ある脆弱性について着目した場合、その脆弱性を持つ製品を利用しているシステム環境によってその脆弱性に関連するリスクは異なる。例えば、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悪用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、脆弱性を悪用する実証コード(PoC)の公開有無も攻撃の容易さが異なる一因となる。また、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、攻撃を受けた際のビジネスへの影響という観点からリスクが異なる。

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、攻撃の容易さや攻撃を受けた際の影響など、「リスクを考慮して行うこと」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脆弱性情報の収集を行い、組織への影響度も考慮したうえで早期に対応を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。

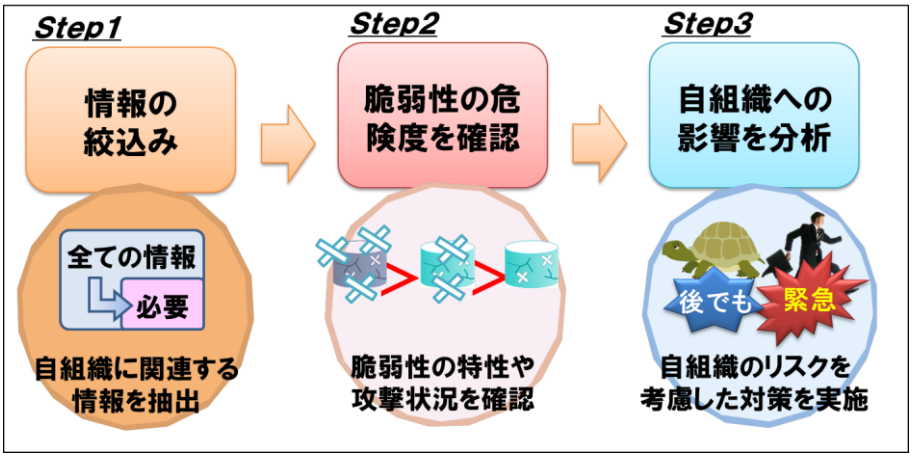

図 2-2-1：情報収集から分析までのイメージ図

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を提供している場合などは、自組織のみならずサービスの利用者にも被害が及ぶなど、被害の影響が大きくなるケースも想定される。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。

自組織のシステムにおける脆弱性対策をするにあたり、脆弱性は日々新たに公開されるため、上記を意識して効率よく情報収集および分析を行うことが望ましい。脆弱性が自組織へ及ぼす影響を分析した結果、システムへのパッチ適用や設定変更などを実施する必要があった場合は、作業計画を立てて検証及び本番システムへの作業実施が必要となる。作業実施までを含めた脆弱性対策のフローについて以下の資料にて一例を解説しているので参照のこと。

参考：脆弱性対策の効果的な進め方（ツール活用編）～脆弱性検知ツール Vuls を利用した脆弱性対策
https://www.ipa.go.jp/security/technicalwatch/20190221.html

2.2.2. 情報収集に有効な URL 一覧

脆弱性に関連する情報を収集するにあたり、製品ベンダーの公開する脆弱性情報や、公的機関の注意喚起サイトおよびニュースサイトなどから効率的に収集することが重要である。

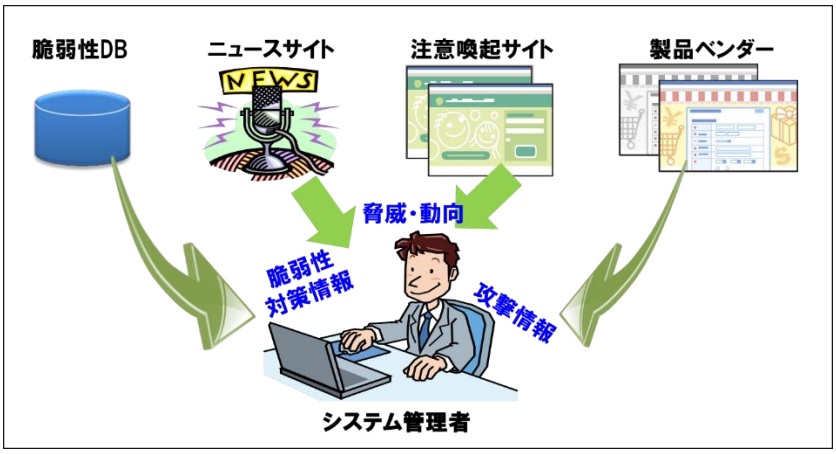

図 2-2-2：情報収集のイメージ図

情報収集をする際に参考となる URL の一例を表 2-2-1 に記載する。

表 2-2-1：情報収集時の参考ＵＲＬ例

種別	URL
脆弱性関連情報データベース	■国内 ・JVN (Japan Vulnerability Notes) https://jvn.jp/ ・脆弱性対策情報データベース JVN iPedia https://jvndb.jvn.jp/ ■海外 ・NVD(National Vulnerability Database) https://nvd.nist.gov/ ・Vulnerability Notes Database https://www.kb.cert.org/vuls/ ・Metasploit (攻撃情報あり) https://www.metasploit.com/ ・Exploit Database (攻撃情報あり) https://www.exploit-db.com/
ニュースサイト	■国内 ・CNET ニュース：セキュリティ https://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 https://tech.nikkeibp.co.jp/genre/security/ ■海外 ・ComputerWorld Security （米国中心） https://www.computerworld.com/category/security/ ・The Register Security （英国・欧州中心） https://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

種別	URL
	https://www.jpcert.or.jp/at/2018.html ・警察庁：警察庁セキュリティポータルサイト https://www.npa.go.jp/cyberpolice/ ■海外 ・米国：US-CERT https://www.us-cert.gov/ncas ・米国：ICS-CERT https://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　セキュリティ更新プログラム ガイド https://portal.msrc.microsoft.com/ja-jp/security-guidance ・オラクル　Critical Patch Update と Security Alerts https://www.oracle.com/technetwork/jp/topics/security/alerts-082677-ja.html
	■クライアント製品など ・Apple セキュリティアップデート https://support.apple.com/ja-jp/HT201222 ・Adobe セキュリティ速報およびセキュリティ情報 https://helpx.adobe.com/jp/security.html ・Mozilla サポートの検索 https://support.mozilla.org/ja/
	■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 https://www.cisco.com/c/ja_jp/support/docs/csa/psirt-index.html ・HP - サポートホーム https://support.hp.com/jp-ja ・日立 –セキュリティ情報 https://www.hitachi.co.jp/hirt/security/index.html ・富士通 - セキュリティ情報 https://www.fujitsu.com/jp/support/security/ https://www.fujitsu.com/jp/products/software/resources/condition/security/ ・NEC - NEC 製品セキュリティ情報 https://jpn.nec.com/security-info/ ・IBM – IBM Support https://www.ibm.com/support/home/?lnk=ushpv18hcwh1&lnk2=support ・Red Hat – Red Hat Product Errata https://access.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 https://www.symantec.com/ja/jp/security_response/securityupdates/list.jsp?fid=security_advisory
	■オープンソースなど ・Apache Foundation https://httpd.apache.org/　（Apache HTTP サーバ） https://tomcat.apache.org/　（Apache Tomcat） https://struts.apache.org/　（Apache Struts） ・ISC （Internet Systems Consortium） https://www.isc.org/downloads/bind/　（BIND） https://www.isc.org/downloads/dhcp/　（DHCP） ・OpenSSL https://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。なお、CVSS には v2 と v3 が存在する。本書では v3 に基づいての解説を行う。

CVSS による評価方法のイメージは図 2-2-3 を参照のこと。

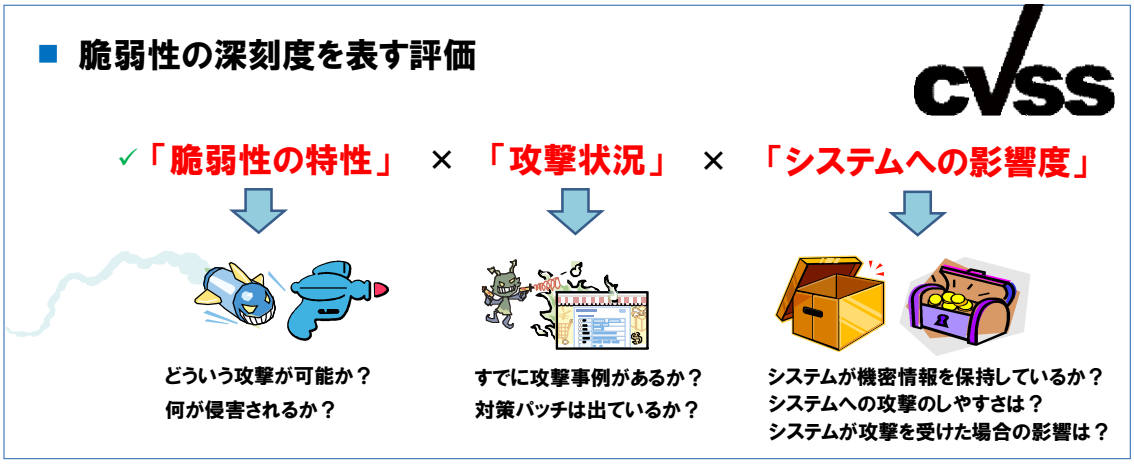

図 2-2-3：CVSS による評価方法のイメージ図

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する。値が大きいほど攻撃が容易であったり、攻撃を受けた際の影響（損害）が大きかったりすることを意味している。

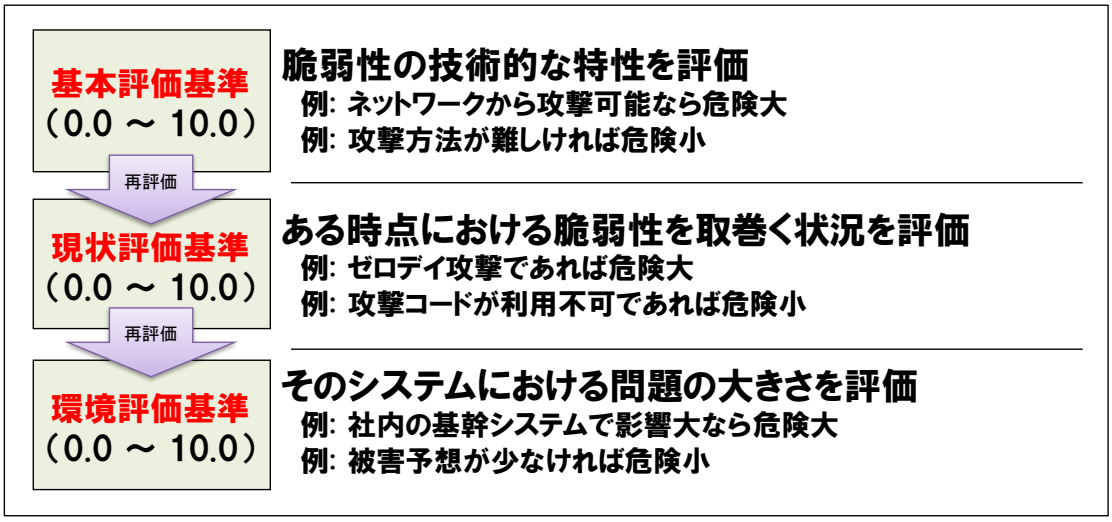

図 2-2-4：CVSS の評価基準の一覧イメージ

CVSS の詳細説明は、下記の情報も参照のこと。

参考 1：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
参考 2：共通脆弱性評価システム CVSS v3 概説(2015 年 7 月 21 日公開)
https://www.ipa.go.jp/security/vuln/CVSSv3.html

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 v3 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）	物理 P	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	低 L
	攻撃する際に必要な特権レベル 必要な特権レベル（PR：Privileges Required）	―	高 H	低 L	不要 N
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル（UI：User Interaction）	―	―	要 R	不要 N
	攻撃による影響範囲 スコープ（S：Scope）	―	―	変更なし U	変更あり C
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	低 L	高 H
	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	低 L	高 H
	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	低 L	高 H

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評価項目は変動する。また、現状評価基準を算出して公開しているベンダーは少ないため、セキュリティ関連組織の公開する情報やニュースなどから脆弱性を悪用した攻撃の動向などに関する情報を収集し、適宜評価を実施する必要がある。

表 2-2-3 に現状評価基準の評価項目一覧を記載する。すべての項目で「未評価」という選択肢があり、それを選択した場合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 U	未確証 R	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）という選択肢がある。

③ 環境評価基準

製品利用者の環境なども含め、最終的な脆弱性の深刻度を評価する基準である。システム環境としてネットワークセグメント間の適切な通信制御を行っているか、ユーザ権限による適切なアクセスコントロールを行っているか、機密情報を保持しているのか、などを加味し脆弱性の影響度を再評価する。

表 2-2-4 に環境評価基準の評価項目一覧を記載する。この基準による評価結果は、脆弱性が組織やシステムに及ぼす影響を評価したものなので、製品利用者やシステム環境ごとに変化する。事前にシステムごとの環境を精査しておき、環境評価基準による迅速な再評価を実施できるように備えておくことが重要である。

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	**どこから攻撃可能であるかの再評価** 緩和策後の攻撃元区分（MAV: Modified Attack Vector）	**物理** P	**ローカル** L	**隣接** A	**ネットワーク** N
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ（MAC: Modified Attack Complexity）	–	–	**高** H	**低** L
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル（MPR: Modified Privileges Required）	–	**高** H	**低** L	**不要** N
	必要なユーザの関与レベルの再評価 緩和策後のユーザ関与レベル（MUI: Modified User Interaction）	–	–	**要** R	**不要** N
	攻撃による影響範囲の再評価 緩和策後のスコープ（MS: Modified Scope）	–	–	**変更なし** U	**変更あり** C
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響（MC: Modified Confidentiality Impact）	–	**なし** N	**低** L	**高** H
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響（MI: Modified Integrity Impact）	–	**なし** N	**低** L	**高** H
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響（MA: Modified Availability Impact）	–	**なし** N	**低** L	**高** H
システムの重要度	**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
	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
	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）という選択肢がある。

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脆弱性対策を実施するにあたり、対象となる脆弱性が自組織に及ぼす影響を評価するためには、脆弱性自体の深刻度のみではなく、自組織のシステム環境における各ネットワークセグメントの重要度やセキュリティ対策状況などを加味して評価する必要がある。

CVSS に照らし合わせると、対象となる脆弱性について基本評価を実施して脆弱性自体の技術的な特性を掴み、現状評価を行うことで評価時点での脆弱性の深刻度を評価する。そして、最終的にその脆弱性に対して自組織における環境評価を実施することで、当該脆弱性が自組織に及ぼす影響を加味した深刻度が算出できる。

ここでは、ある脆弱性について CVSS の評価値を算出するにあたり、自組織において環境評価を行った場合に、各システム状況に応じて最終的な評価値が異なってくる例をモデルケースを用いて概説する。

図 2-2-5 は、環境評価を実施するモデルケースのシステム環境のイメージ図である。

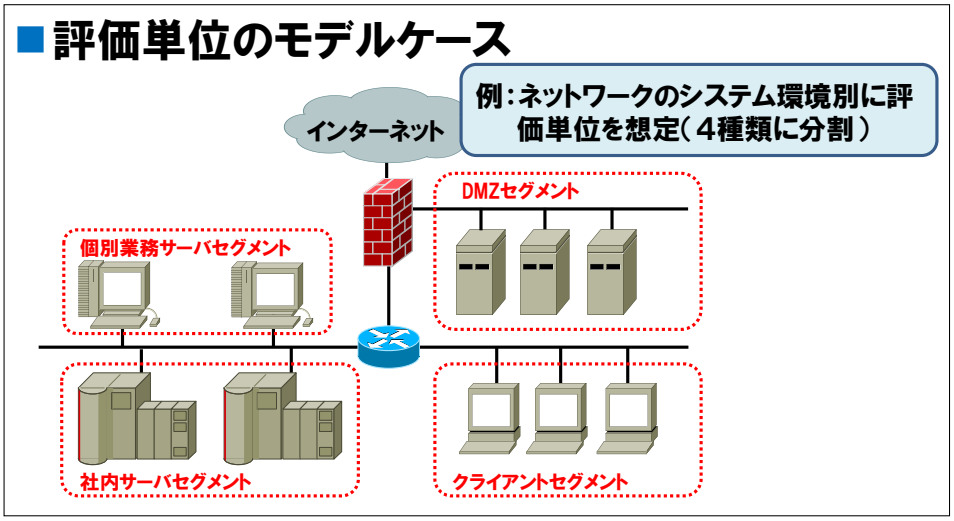

図 2-2-5：モデルケースのシステム環境イメージ

本ケースではファイアウォールによって分割された複数のネットワークセグメントから構成されるシステムを想定する。基本的にはネットワークセグメントごとに配置されるサーバや端末、実装されている機能などが異なり、攻撃のしやすさや攻撃を受けた際の影響度が異なってくる。そのため、本ケースではネットワークセグメントごとに環境評価を実施する。ただし、実際には同一セグメント内においても重要度が異なるシステムが存在するケースも考えられるので、その場合は同一セグメント内でもシステムごとに環境評価を実施しなければならない。

なお前提として、本項ではある脆弱性に対する環境評価の結果がネットワークセグメントごと（システム環境ごと）に変化することを確認する目的であるため、基本評価および現状評価については固定値とする。

また、実際には特定の脆弱性がすべてのネットワークセグメントのシステムに共通して存在するケースは少ないと考えられるが、本ケースでは環境評価結果の比較をしやすくするため、すべてのネットワークセグメントにおいて評価対象の脆弱性が存在していることを前提とする。

各ネットワークセグメントの概要を以下に記載する。

・DMZ セグメント

外部公開している Web サーバや、社外とのメールの中継を行うメールサーバ、インターネット閲覧の通信を中継するプロキシサーバなどが設置されている。インターネットと通信を行う唯一のセグメントである。インターネットと通信を行うセグメントのため、機密情報は保持させていない想定する。

・社内サーバセグメント

社内向けの Web サーバや、DMZ セグメント経由で社外とのメールのやりとりを行うメールサーバなどが設置されている。インターネットとの直接の通信は発生しない。メールなどが保存されているため、一部機密情報を保持している想定。

・個別業務サーバセグメント

組織内で利用する業務用サーバが設置されている。クライアントセグメントの特定の業務端末との通信のみを行い、それ以外の通信は遮断するように通信制御を行っている。顧客情報や業務に関する機密情報などを保持しており、保持する情報の重要度は最も高いと想定する。

・クライアントセグメント

従業員が利用する業務端末が設置されている。個別業務サーバとの通信以外にも社内サーバセグメントへの通信や、インターネット閲覧通信のために DMZ セグメントとの通信も発生する。社内外へのメールの作成など日々の業務を行う業務端末が設置されているセグメントのため、一部機密情報を保持している想定。

(1) モデルケースにおける基本評価

評価する脆弱性の基本評価は、リスクを最大と想定して以下に固定する。

表 2-2-5　モデルケースにて評価する脆弱性の基本評価基準

	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）	物理	ローカル	隣接N/W	ネットワーク
	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）	ー	ー	高	低
	攻撃する際に必要な特権レベル 必要な特権レベル（PR：Privilleges Required）	ー	高	低	不要
	攻撃する際に必要なユーザ関与レベル ユーザ関与レベル（UI：User Interaction）	ー	ー	要	不要
	攻撃による影響範囲 スコープ（S：Scope）	ー	ー	変更なし	変更あり
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）	ー	なし	低	高
	情報が改ざんされる可能性 完全性への影響（I：Integrity Impact）	ー	なし	低	高
	業務が遅延・停止する可能性 可用性への影響（A：Availability Impact）	ー	なし	低	高

(2) モデルケースにおける現状評価

現状評価についても、リスクを最大と想定して以下に固定する。

表 2-2-6　モデルケースにて評価する脆弱性の現状評価基準

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	実証可	攻撃可	容易
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	暫定	非公式	なし
情報の信頼性 情報信頼性（RC：Report Confidence）	-	未確認	未確証	確認済

(3) モデルケースにおける環境評価

図 2-2-5 のモデルケースにおいて、各ネットワークセグメントで環境評価を実施する。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、11 個の評価項目について評価する必要がある。表 2-2-4 の上から 8 項目が影響範囲に関する評価項目であり、基本評価した内容について各システム環境の重要度やセキュリティ対策状況を加味して再評価を行う。その他の 3 項目についてはシステムの重要度に関する評価項目であり、システムが保持する情報の重要度や、システムが遅延・停止した場合の影響度などを加味して再評価を行う。以下にモデルケースの各ネットワークセグメントで環境評価を実施した例を記載する。

① DMZ セグメントにおける環境評価

表 2-2-7：DMZ セグメントにおける環境評価

■DMZセグメントにおける環境評価　危険小 ⇔ 危険大

	評価項目	選択肢			
影響範囲	どこから攻撃可能であるかの再評価 緩和策後の攻撃元区分 (MAV: Modified Attack Vector)	物理 P	ローカル L	隣接 A	**ネットワーク N**
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ (MAC: Modified Attack Complexity)	–	–	高 H	**低 L**
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル (MPR: Modified Privileges Required)	–	高 H	低 L	**不要 N**
	必要なユーザの関与レベルの再評価 緩和策後のユーザ関与レベル (MUI: Modified User Interaction)	–	–	要 R	**不要 N**
	攻撃による影響範囲の再評価 緩和策後のスコープ (MS: Modified Scope)	–	–	変更なし U	**変更あり C**
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響 (MC: Modified Confidentiality Impact)	–	**なし N**	低 L	高 H
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響 (MI: Modified Integrity Impact)	–	なし N	低 L	**高 H**
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響 (MA: Modified Availability Impact)	–	なし N	低 L	**高 H**
システムの重要度	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
	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**
	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**

DMZ セグメントのサーバには機密情報を保持しないため「機密情報が漏えいする可能性の再評価」を「低」とした。同様に、「システムにおける機密性の重要度」も「低」と評価した。外部公開してサービス提供を行っている Web サーバが設置されているため、「システムにおける完全性の重要度」および「システムにおける可用性の重要度」は「高」とした。

② 社内サーバセグメントにおける環境評価

表 2-2-8：社内サーバセグメントにおける環境評価

■社内サーバセグメントにおける環境評価　危険小 ⇔ 危険大

	評価項目	選択肢			
影響範囲	どこから攻撃可能であるかの再評価 緩和策後の攻撃元区分 (MAV: Modified Attack Vector)	物理 P	ローカル L	**隣接 A**	ネットワーク N
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ (MAC: Modified Attack Complexity)	–	–	**高 H**	低 L
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル (MPR: Modified Privileges Required)	–	高 H	低 L	**不要 N**
	必要なユーザの関与レベルの再評価 緩和策後のユーザ関与レベル (MUI: Modified User Interaction)	–	–	要 R	**不要 N**
	攻撃による影響範囲の再評価 緩和策後のスコープ (MS: Modified Scope)	–	–	変更なし U	**変更あり C**
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響 (MC: Modified Confidentiality Impact)	–	なし N	**低 L**	高 H
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響 (MI: Modified Integrity Impact)	–	なし N	**低 L**	高 H
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響 (MA: Modified Availability Impact)	–	なし N	**低 L**	高 H
システムの重要度	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
	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
	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**

社内サーバセグメントはインターネットとは直接の通信を行わず、ファイアウォールを介して社内のその他のセグメントとのみ通信を行う構成のため、「どこから攻撃可能であるかの再評価」を「隣接」とした。またファイアウォールでの適切な通信制御も行っていると判断し、「必要な条件の複雑さの再評価」を「高」と再評価した。また、社内向けの Web サーバや外部とメールのやりとりを行うメールサーバなども設置されているため、機密性、完全性、可用性はいずれも侵害される可能性があるが、ファイアウォールによる適切な通信制御を行っていることを考慮して「機密情報が漏えいする可能性の再評価」、「情報が改ざんされる可能性の再評価」、「業務が遅延・停止する可能性の再評価」をそれぞれ「低」と再評価した。システムの重要度に関する 3 つの評価項目については、メールが停止することによる外部機関との業務継続に与える影響が大きいと判断し、「システムにおける可用性の重要度」のみ「高」とした。

③ 個別業務サーバセグメントにおける環境評価

表 2-2-9：個別業務サーバセグメントにおける環境評価

■個別業務サーバセグメントにおける環境評価　危険小 ⇔ 危険大

	評価項目	選択肢			
影響範囲	どこから攻撃可能であるかの再評価 緩和策後の攻撃元区分 (MAV: Modified Attack Vector)	物理 P	ローカル L	**隣接** **A**	ネットワーク N
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ (MAC: Modified Attack Complexity)	-	-	**高** **H**	低 L
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル (MPR: Modified Privileges Required)	-	**高** **H**	低 L	不要 N
	必要なユーザの関与レベルの再評価 緩和策後のユーザ関与レベル (MUI: Modified User Interaction)	-	-	**要** **R**	不要 N
	攻撃による影響範囲の再評価 緩和策後のスコープ (MS: Modified Scope)	-	-	変更なし U	**変更あり** **C**
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響 (MC: Modified Confidentiality Impact)	-	なし N	**低** **L**	高 H
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響 (MI: Modified Integrity Impact)	-	なし N	**低** **L**	高 H
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響 (MA: Modified Availability Impact)	-	なし N	**低** **L**	高 H
システムの重要度	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**
	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**
	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**

個別業務サーバセグメントはクライアントセグメントの特定の業務端末からのみ通信を行うため、「どこから攻撃可能であるかの再評価」を「隣接」、「必要な条件の複雑さの再評価」を「高」と再評価した。また、業務端末から個別業務サーバへ通信を行う場合、毎回手動での認証操作を必須としているため、「必要なユーザの関与レベルの再評価」を「要」と再評価した。「機密情報が漏えいする可能性の再評価」、「情報が改ざんされる可能性の再評価」、「業務が遅延・停止する可能性の再評価」についてはファイアウォールでの通信制御や個別業務サーバにおけるセキュリティ対策を考慮し、それぞれ「低」と再評価した。システムの重要度に関する 3 つの評価項目については、保持する情報の重要度やシステム停止時に業務継続に与える影響度を考慮し、いずれも「高」とした。

④ クライアントセグメントにおける環境評価

表 2-2-10：クライアントセグメントにおける環境評価

■クライアントセグメントにおける環境評価　危険小 ⇔ 危険大

	評価項目	選択肢			
影響範囲	どこから攻撃可能であるかの再評価 緩和策後の攻撃元区分（MAV: Modified Attack Vector）	物理 P	ローカル L	**隣接** **A**	ネットワーク N
	必要な条件の複雑さの再評価 緩和策後の攻撃条件の複雑さ（MAC: Modified Attack Complexity）	-	-	**高** **H**	低 L
	必要な特権のレベルの再評価 緩和策後の必要な特権レベル（MPR: Modified Privileges Required）	-	高 H	低 L	**不要** **N**
	必要なユーザの関与レベルの再評価 緩和策後のユーザ関与レベル（MUI: Modified User Interaction）	-	-	要 R	**不要** **N**
	攻撃による影響範囲の再評価 緩和策後のスコープ（MS: Modified Scope）	-	-	変更なし U	**変更あり** **C**
	機密情報が漏えいする可能性の再評価 緩和策後の機密性への影響（MC: Modified Confidentiality Impact）	-	なし N	**低** **L**	高 H
	情報が改ざんされる可能性の再評価 緩和策後の完全性への影響（MI: Modified Integrity Impact）	-	なし N	**低** **L**	高 H
	業務が遅延・停止する可能性の再評価 緩和策後の可用性への影響（MA: Modified Availability Impact）	-	なし N	**低** **L**	高 H
システムの重要度	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
	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
	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

クライアントセグメントはインターネットとは直接通信を行わず、ファイアウォールを介して社内のその他のセグメントとのみ通信を行う構成のため、「どこから攻撃可能であるかの再評価」を「隣接」とした。またファイアウォールでの適切な通信制御も行っていることから、「必要な条件の複雑さの再評価」を「高」と再評価した。業務端末では日々業務に関するメール作成や業務資料の作成を行っていることから、機密性、完全性、可用性はいずれも侵害される可能性があるが、ファイアウォールによる適切な通信制御を行っていることを考慮して「機密情報が漏えいする可能性の再評価」、「情報が改ざんされる可能性の再評価」、「業務が遅延・停止する可能性の再評価」をそれぞれ「低」と再評価した。システムの重要度に関する３つの項目については、重要なデータは個別業務サーバにて保持しており、可用性が侵害された場合も代替業務端末が利用できるなど、完全性、可用性についての重要度は低いため、「システムにおける完全性の重要度」および「システムにおける可用性の重要度」をそれぞれ「低」とした。

上記の環境評価結果に基づいて、最終的に各ネットワークセグメントの環境値を算出した結果が図 2-2-6 である。CVSS の基本値、現状値、環境値は、3.5 節にて紹介する「CVSS 計算ソフトウェア」に各々の基本評価、現状評価、環境評価を指定することで算出できる。

基本値、現状値ともに最大のリスクを想定した場合にスコアは 10.0 となる。その後、各ネットークセグメントの環境評価を反映した結果、環境値が最も高かったネットワークセグメントは「DMZ セグメント」で、環境値が最も低かったのは「クライアントセグメント」となった。このように、ひとつの脆弱性に対しても、各ネットワークセグメントの環境を加味することで、各システムにおける最終的な CVSS のスコアは大きく変動することが見て取れる。

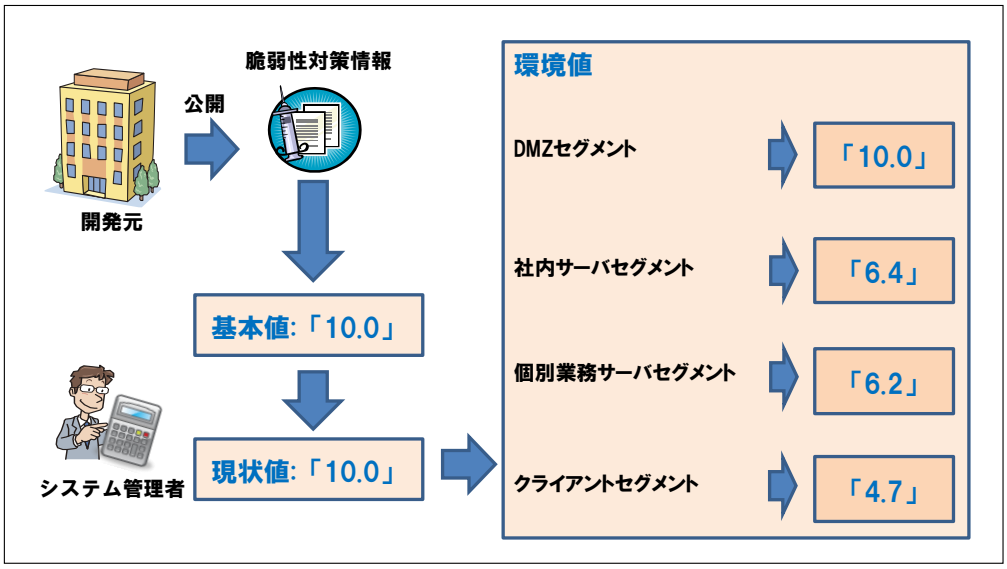

図 2-2-6：環境値の算出結果（モデルケースの場合）

このように算出した環境値は、ある脆弱性が自組織の各システムに及ぼす影響の深刻度をスコアリングしたものといえる。脆弱性対策の方針を決定するにあたってのひとつの判断材料として有用である。

日々の自組織における脆弱性対策の一環として、自組織で利用している製品に関する脆弱性情報の収集を実施した場合、各製品のメーカーや第三者機関などから収集できる CVSS のスコアは基本値のみである場合が多い。基本値は脆弱性そのものの特性をあらわすものなので、実際に自組織において当該脆弱性への対策を実施する優先度や要否の判断については、現状値や環境値までを加味して再評価を行ったスコアを用いなければ非効率的な運用となってしまう懸念もある。

脆弱性対策実施の優先度や要否の判断については、攻撃に必要な実証コードや実際の攻撃事例の有無を確認し、攻撃手法や事例が存在する場合には当該攻撃が自組織のシステムにおいて成功しうるのか、また成功した場合にはどのような影響が考えられるのかなどを考慮することが重要である。

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） 脆弱性情報の受信（組織内への案内等）	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）
		注意警戒情報サービス	https://jvndb.jvn.jp/alert/
	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）
	脆弱性情報の収集（日本で広く利用されているサーバ用オープンソースソフトウェア）	サーバ用オープンソースソフトウェアに関する製品情報およびセキュリティ情報	https://www.ipa.go.jp/security/announce/sw_security_info.html
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。

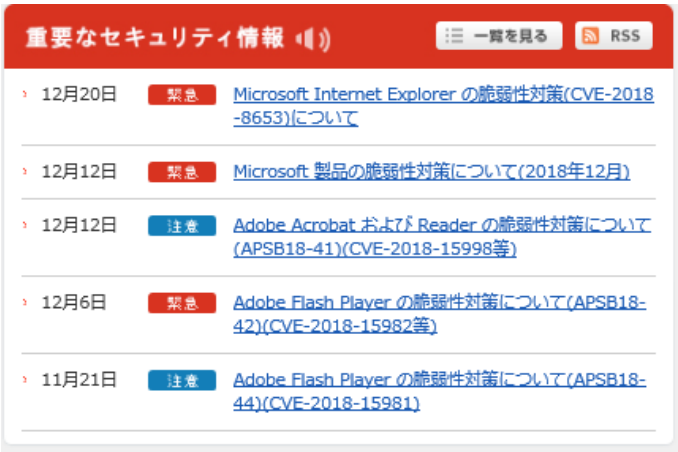

図 3-2-1：重要なセキュリティ情報

■活用方法

① 定期的に IPA のウェブサイトを確認する。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。2018 年 12 月末時点で 92,000 件以上のデータを蓄積している。

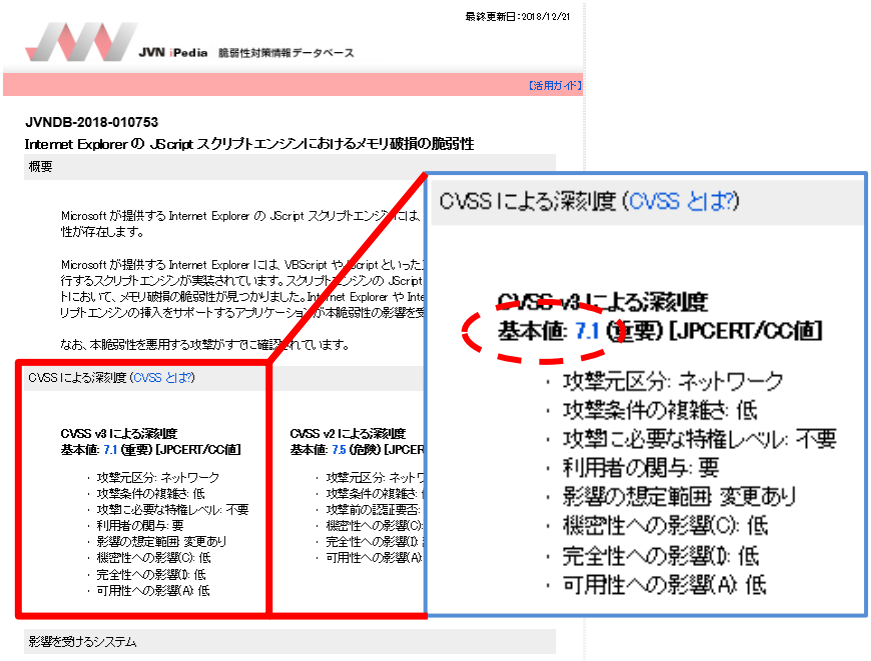

図 3-3-1：JVN iPedia

■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

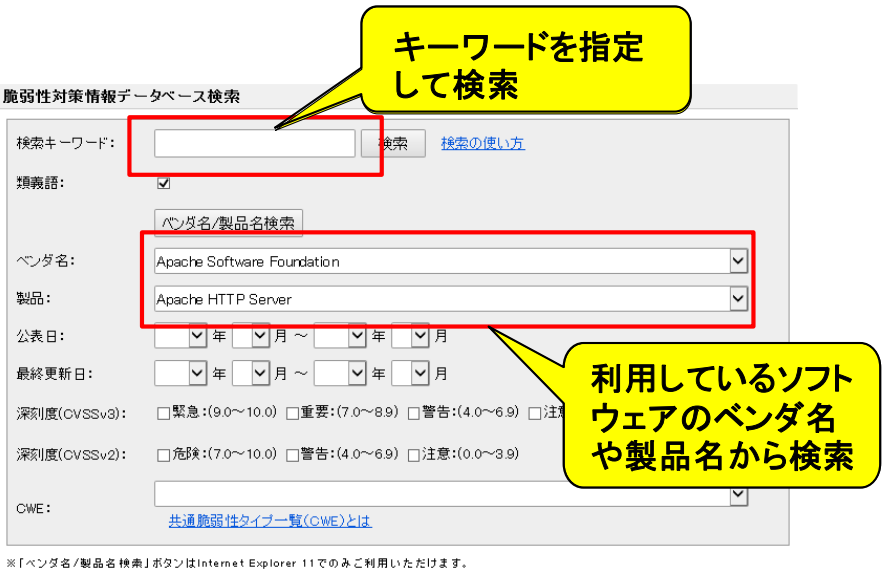

図 3-3-2：JVN iPedia 検索ページ

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。

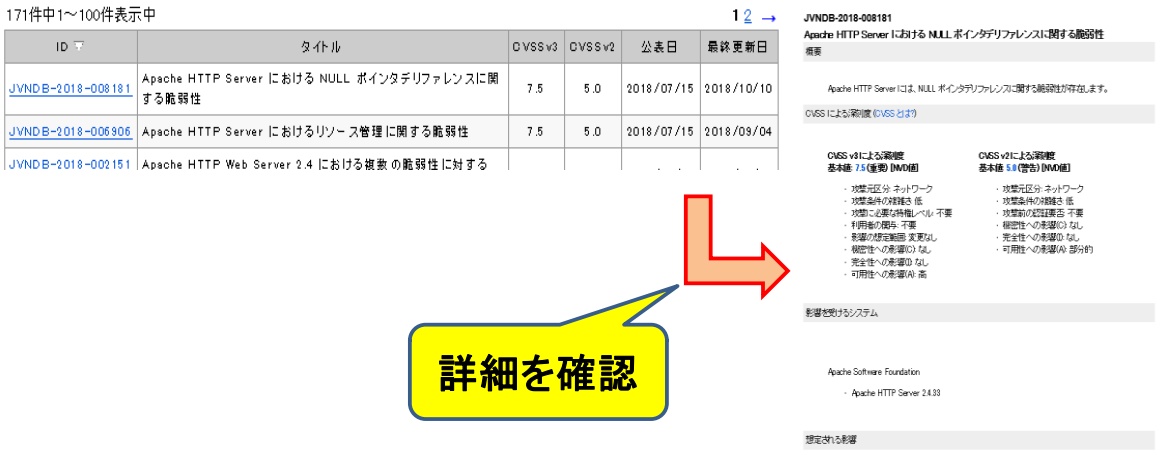

図 3-3-3：JVN iPedia 検索ページから詳細情報の確認

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 のウェブサイトより MyJVN 脆弱性対策情報収集ツール（通称、mjcheck3）をダウンロードし起動する。

mjcheck3　　：https://jvndb.jvn.jp/apis/myjvn/mjcheck3.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。

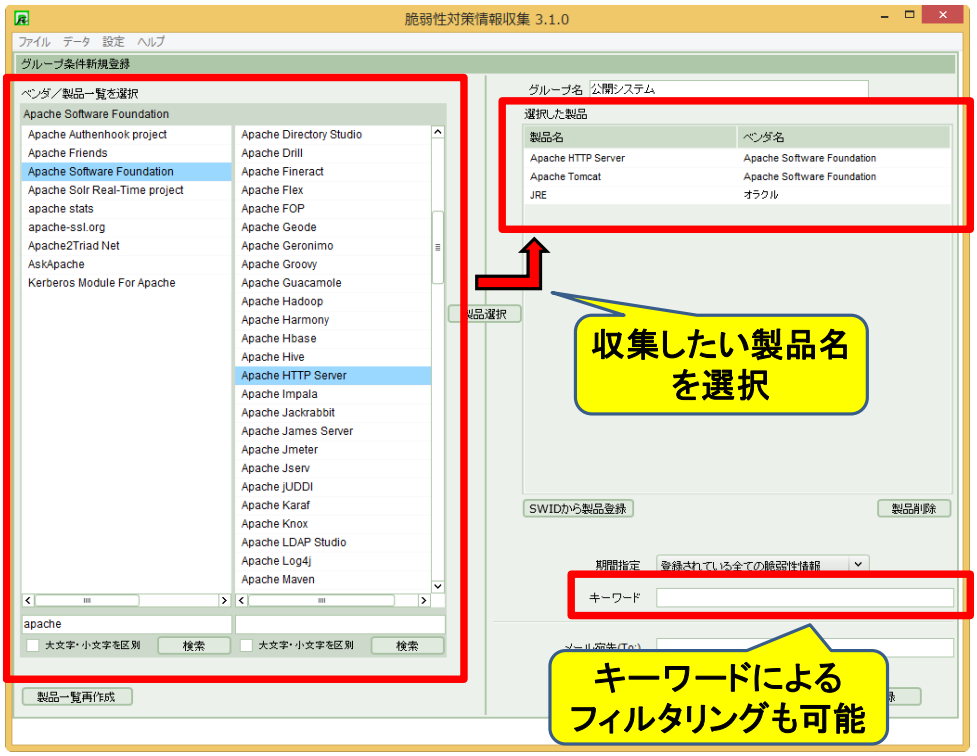

図 3-4-2：MyJVN 脆弱性対策情報収集ツール　フィルタリング条件の指定

参考）フィルタリング例

・サーバ環境でよく使われる製品の脆弱性情報を収集したい

表 3-4-1：サーバ環境でよく使われる製品例

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の脆弱性情報を収集したい

表 3-4-2：クライアント環境でよく使われる製品例

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脆弱性情報が収集される。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、より詳しく内容を確認することができる。

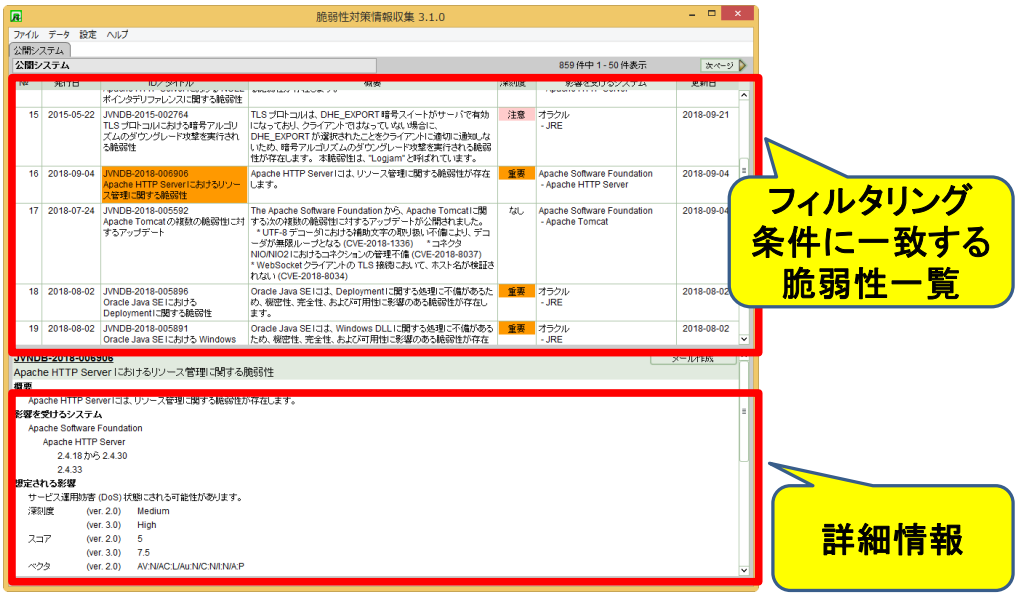

図 3-4-3：MyJVN 脆弱性対策情報収集ツール脆弱性一覧

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。

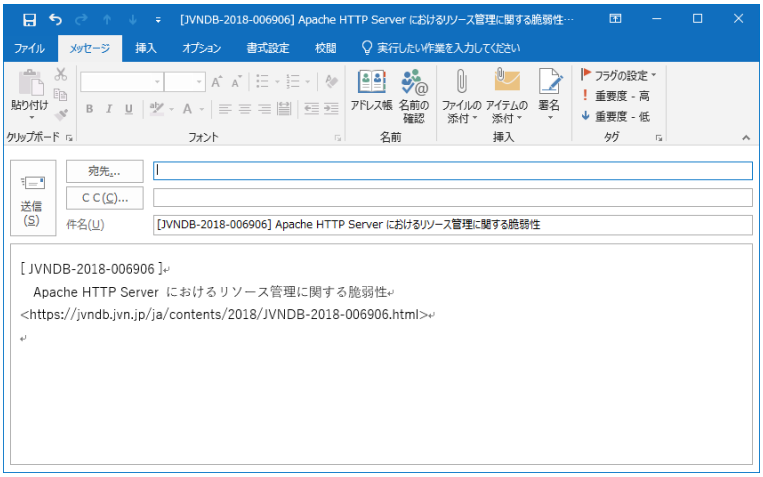

図 3-4-4：脆弱性情報のメール自動生成

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。

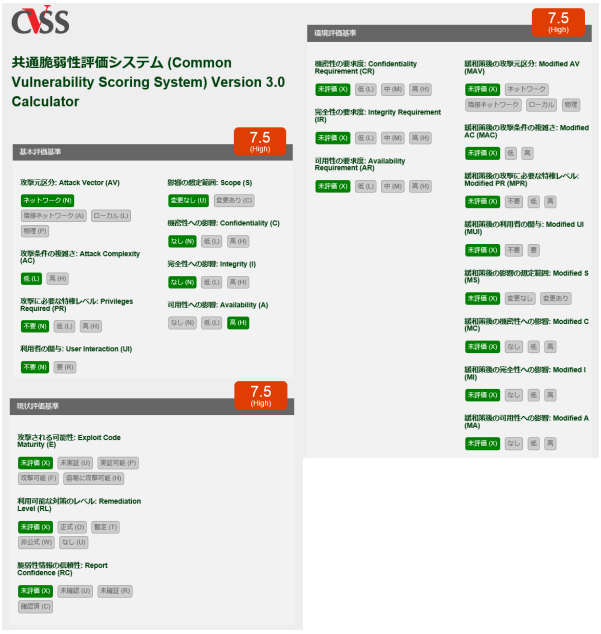

図 3-5-1：CVSS 計算ソフトウェア

■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くなっており、システムへの影響度が大きい脆弱性情報を早期に把握、対策を実施することの重要性は益々高くなっている。

本書の 2 章において、ある脆弱性の深刻度はシステム環境に応じて変化する例を解説した。ここでは現状値（実際の攻撃手法が確立しているか、実際に攻撃事例はあるか）は最大と想定して固定していたが、実際に日々のシステム運用における脆弱性対策の実施要否を判断する材料としては、この現状値はとても重要であると感じている。特に自組織で利用している製品の脆弱性を悪用された被害事例がすでに確認されている場合などは、自組織も同様の被害を受ける可能性は十分に考えられるため、迅速な判断が求められる。現状評価は環境評価に比べ評価項目も少ないのでより迅速な判断に向いている指標であると考える。

本書で解説した内容を自組織の脆弱性対策に活用していただき、効果的な脆弱性対策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）第 2 版」

～脆弱性情報の早期把握、収集、活用のスヽメ～

[発　　行]　2019 年 2 月 21 日
[著作・制作]　独立行政法人情報処理推進機構 セキュリティセンター セキュリティ対策推進部
[執　筆　者]　黒谷 欣史、亀山 友彦