



脆弱性対応における リスク評価手法のまとめ

ver1.1

2024 年 7 月

独立行政法人情報処理推進機構

産業サイバーセキュリティセンター 中核人材育成プログラム 7 期生

脆弱性対応管理プロジェクト

目次

序文	4
はじめに	4
本書の構成	7
本書の対象読者	7
免責事項	7
1 評価指標	9
1.1 リスクの考え方	9
1.2 CVSS v3.1	11
1.2.1 概要	11
1.2.2 特徴	12
1.3 CVSS v4.0	14
1.3.1 概要	14
1.3.2 特徴	16
1.4 SSVC v2.1	17
1.4.1 概要	17
1.4.2 特徴	18
1.5 EPSS	20
1.5.1 概要	20
1.5.2 特徴	20
1.6 KEV	21
1.6.1 概要	21
1.6.1 特徴	22
1.7 評価指標まとめ	23
2 各評価指標を活用したリスク評価	26
2.1 各評価指標の活用検討	26
2.2 SSVC を活用したリスク評価例	29
2.2.1 SSVC 活用リスク評価の概要	29
2.2.2 0 次評価（攻撃の流行度評価）	30
2.2.3 1 次評価（簡易リスク評価）	31
2.2.4 2 次評価（SSVC を活用したリスク評価）	33
2.2.5 まとめ	33
2.3 CVSS 環境値を活用したリスク評価例	34
2.3.1 CVSS 環境値を活用したリスク評価の概要	34
2.3.2 2 次評価（CVSS 環境値を活用したリスク評価）	34
2.3.3 まとめ	35

2.4	資産重要度を活用したリスク評価例	36
2.4.1	SSVC および CVSS 環境値を利用する場合の課題	36
2.4.2	資産重要度を活用したリスク評価の概要	36
2.4.3	事前準備（資産重要度の設定）	38
2.4.4	2次評価（資産重要度を活用したリスク評価）	40
2.4.5	まとめ	41
2.5	1次評価の閾値	42
2.5.1	閾値の必要性	42
2.5.2	閾値の考え方	42
2.5.3	CVSS 基本値の閾値決め	44
2.5.4	EPSS の閾値決め	46
3	運用編	52
3.1	資産重要度を活用したリスク評価における運用例の概要	52
3.2	脆弱性情報の収集	53
3.3	資産重要度を活用したリスク評価	57
3.3.1	資産重要度の設定基準例	57
3.3.2	各評価指標の活用例	57
3.4	脆弱性情報のモニタリング	62
3.5	EPSS スコアのモニタリング及び既知脆弱性評価時の EPSS 閾値	64
3.5.1	モニタリングの必要性	64
3.5.2	既知脆弱性の評価	64
3.5.3	モニタリング 及び 既知脆弱性用の EPSS スコアの閾値	64
3.6	運用上の懸念点	69
4	まとめ	71
	APPENDIX	73
A)	CVSS v3.1 の詳細説明	73
B)	CVSS v4.0 の詳細説明	80
C)	SSVC v2.1 の詳細説明	91
D)	EPSS の詳細説明	104
E)	CVEdetails.com	106
F)	Vulnrichment	110
G)	ICSCoE 参加企業へのアンケート結果	115
	用語集	119
	参考文献	120
	謝辞	121

序文

本プロジェクトは、ICSCoE^{※17} 期生において、実業務で脆弱性対応を行う際に、日々公表される全ての脆弱性に対応しきれないという問題や、CVSS（Common Vulnerability Scoring System）基本値のスコアを脆弱性の対応優先度を決めるために利用するには不十分であると考え、これを解決すべく立ち上げられた。CVSS 基本値が脆弱性そのものの深刻度を評価する点では有用であるものの、脆弱性の悪用状況やユーザの環境情報を考慮していないため、脆弱性対応の優先度を決定するために、単体で使用するのは適切ではないと考えた。また、CVSS や EPSS（Exploit Prediction Scoring System）などのリスク評価値を脆弱性対応の優先度付けに使用する場合、適切な閾値を設定する必要があると判断した。これらを踏まえて、評価値の妥当性や効率的な運用方法がないかという点について、本書のテーマである脆弱性対応の一環としてのリスク評価方法について新たに検討し、我々の考える運用例を本書にまとめている。

セキュリティに対するリスク評価に課題を抱えている組織において、本書が少しでも役に立てば幸いである。

はじめに

近年、脆弱性を突いたサイバー攻撃が増加しており、このサイバー攻撃の脅威から各企業内の資産を保護することが求められている。そのため、各企業の CSIRT^{※2}（Computer Security Incident Response Team）またはセキュリティ関連部署は、自社の IT システム/ネットワーク機器/ICS^{※3}（Industrial Control System）機器等に関わる脆弱性情報を複数の情報源から入手し、各脆弱性に対応する必要がある。しかし、日々新たな脆弱性が発見され、膨大な量の脆弱性情報が公開される中、コストや工数といった運用リソースの観点から、全てに対応するのは困難かつ非現実的である。

こうした状況に対して、どの脆弱性を優先的に対処すべきかを判断するために、それぞれの脆弱性に対してリスク評価を実施し、優先度付けを行う必要がある。これがトリアージと呼ばれる作業である。現状最も一般的な脆弱性のトリアージ用のリスク評価値である CVSS 基本値は広く利用されている一方で、その評価を判断材料にするには懸念がある。これは CVSS 基本値が脆弱性そのものの深刻度しか評価されておらず、脆弱性に対する脅威動向や自社の環境に照らし合わせたリスクを考慮していないためである。評価指標としては、CVSS 基本値以外に CVSS 現状値/CVSS 環境値/SSVC/EPSS/KEV 等が存在しているが、そもそも浸透していないまたは評価指標の活用方法が複雑である等の理由から、利用されている例は少ない。

我々は、上記の傾向を確かめるため ICSCoE に参加経験のある 62 社を対象にアンケートを実施した。以下の図 1~4 は、その結果である。ここではアンケート項目のうち、以下 4 つの質問についての結果を掲載する。

- ① CVSS の評価基準は何を採用しているか
- ② リスク評価を実施する際に「SSVC」を活用しているか
- ③ リスク評価を実施する際に「EPSS」を活用しているか
- ④ リスク評価を実施する際に「KEV」を活用しているか

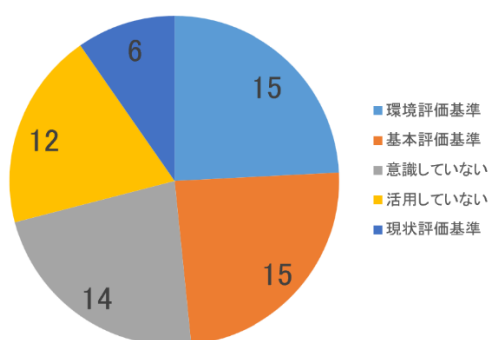


図 1 CVSS の各評価基準の活用状況

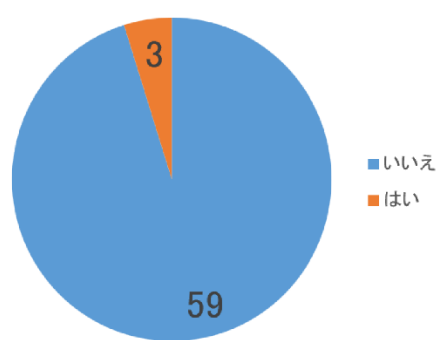


図 2 SSVC の活用状況

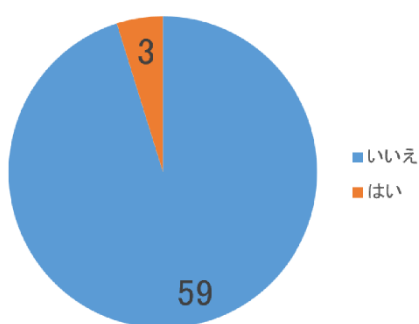


図 3 EPSS の活用状況

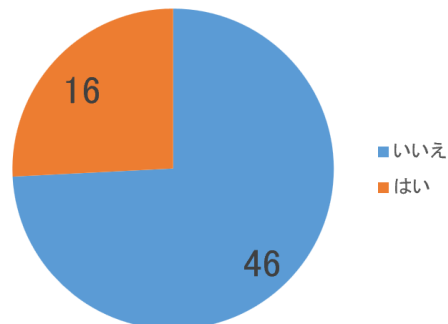


図 4 KEV の活用状況

図 1 については、「基本評価基準」と「環境評価基準」を活用している企業が同じ数となったが、「意識していない」と回答した企業が 14 あった。この回答については概ね基本評価基準を活用しているものと予想されるため、この回答をあわせると最も「基本評価基準」を採用している企業が多いといえる。図 2 及び図 3 からは、EPSS と KEV が共に全体の 5% 程の企業にしか活用されておらず、また図 4 から KEV についても全体の 25% 程の企業にのみ活用されていることが分かる。

これらの調査結果は先述した、CVSS は基本評価基準が主に使われており、その他の評価指標については利用されている例が少ないということを示す資料となり得るだろう。

また、日本特有の製品に対して国外の評価指標を利用すると、国内での脅威情報が考慮されづらい恐れがあり、適切にリスクが評価されない可能性がある。これは脆弱性に対する脅威動向として取り入れられる情報が国外に偏っているためである。国内における脅威動向を考慮したリス

ク評価を実施するには、国内の公的機関およびベンダが情報の鮮度を保ちながら情報を提供する必要があるが、現状はそのレベルにまで至っていない。

そこで本書では、膨大な数の脆弱性に対するトリアージ手法の活用方法を検討する。その前段階として、トリアージで利用する各種評価指標についてまとめる。この中で、各種評価指標の特徴および課題についても言及する。

最後に、本書を通じて各企業のセキュリティ・脆弱性担当者が、自社のリスクを正しく認識し、より適切な脆弱性対処アプローチを実施できるようになることを期待する。

本書の構成

第1章「リスク評価手法」では、CVSS v3.1/CVSS v4.0/SSVC v2.1/EPSS/KEV を紹介し、各手法の特徴についてまとめる。

第2章「リスク評価手法の活用例」では、本書で紹介したリスク評価手法の活用例について説明する。

第3章「運用」では、リスク評価手法の活用例の運用方法について説明する。

第4章「まとめ」では、本書のまとめを記載する。

補足：本書では参考文献及び用語集との紐づけを以下の通り記載する

[x] ：参考文献

※x ：用語集

本書の対象読者

本書は、以下を対象読者としている。

- 各企業のセキュリティ・脆弱性担当者
- 膨大な脆弱情報のトリアージに課題を感じている組織
- 様々な評価指標を学び習得し、組織における脆弱性対応の戦略を立てセキュリティ体制を強化したい組織

免責事項

- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本書に誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的または黙示的な保証や条件は一切ないものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、著者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から2年間とする。



第 1 章

評価指標

1 評価指標

1.1 リスクの考え方

米 MITRE 社では、脆弱性を一意に識別する番号である CVE (Common Vulnerabilities and Exposures) が採番されており、2024 年 5 月時点では 233,151 件が登録されている^[1]。その中で、2023 年に採番されている CVE の数は 26,200 件であり、単純計算で 1 日あたり約 71 件の新規脆弱性情報が登録されている。この日々公開される膨大な脆弱性情報に対して、全てを対処することは現実的ではない。そこで、各脆弱性に対してリスク評価を行い対応する優先度を設定することで、緊急度の高い脆弱性から効率的に対応することが可能である。このリスクの考え方について、本書では以下のとおり定義する。

$$\text{リスク} = \text{脅威} \times \text{脆弱性} \times \text{資産}$$

基本的にリスク評価としては、「脅威」「脆弱性」「資産」の3要素を考慮して実施し、その結果をもとに優先度をつけることが推奨される。

以下で各要素についてどのような判定項目を考慮するかを記述する。

➤ **脅威**

「悪用実績、または Exploit コード^{※4}/PoC コード^{※5}の公開有無」とし、該当の脆弱性に対して攻撃者視点から攻撃可能か、または攻撃される可能性が高いかを考慮されているかどうかを判断する。

➤ **脆弱性**

「脆弱性そのものの深刻度」とし、該当の脆弱性がシステムやデータに与える潜在的な影響の大きさを判断する。これには、攻撃者が脆弱性を悪用した際の影響度（例えば、機密情報の漏洩、システム停止、データの改ざんなど）や、修正の難易度、既知の回避策の有無などの攻撃の価値密度や容易さも含まれる。

➤ **資産**

「該当の脆弱性を保有するシステムの重要度」とし、システム環境ごとに異なる資産の重要度を考慮されているかどうかを判断する。

ここで、リスクを「脅威」「脆弱性」「資産」の3要素で上記の式のように定義している理由について述べる。ISO/IEC 27011:2018^[2]によれば「リスクは多くの場合、ある事象がもたらす結果とそれに関連する「発生確率」の組み合わせで表現される」とされ、これはすなわち影響度と発生確率の掛け合わせで表現できるといえる。影響度は、攻撃が発生したことにより生じる損失の大きさを意味する。発生確率は、該当の脆弱性を利用された攻撃が発生する

可能性を意味する。ここで発生確率には、攻撃される可能性を表す脅威と、該当する脆弱性に対する攻撃の容易さや攻撃の価値密度を表す脆弱性が含まれる。最後に影響度は、システム環境ごとの資産に対する機密性^{※6}・完全性^{※7}・可用性^{※8}を表す資産が含まれる。よって、リスクの発生可能性と影響度は、脅威・脆弱性・資産で表されるため、本書ではこの3要素を用いてリスクを定義している。

本章ではこれらを踏まえ、リスク評価の際に活用する、脆弱性に対する各評価指標の説明を行う。

1.2 CVSS v3.1

1.2.1 概要

共通脆弱性評価システム CVSS (Common Vulnerability Scoring System) は、システムやソフトウェアが持つ脆弱性の深刻度を評価する国際的な指標である。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、ベンダに依存しない共通の評価方法を定量的に示すことが可能である。^[3]

CVSS には 3 つの評価基準が存在する。それらの概要を基本評価基準、現状評価基準、環境評価基準の順に説明していく。

➤ **基本評価基準 (Base Metrics)** ^[3]

脆弱性そのものの特性を評価する基準である。情報システムに求められる 3 つのセキュリティ特性、「機密性(Confidentiality Impact)」、「完全性(Integrity Impact)」、「可用性(Availability Impact)」に対する影響を、ネットワークから攻撃可能かどうかといった、攻撃条件の複雑さはどの程度かといった多様な基準で評価し、CVSS 基本値(Base Score)を算出する。この基準によって算出されたスコアは固定であり、時間の経過や利用環境によって変動しない。ベンダや脆弱性を公表する組織等が、脆弱性の固有の深刻度を表すために評価する基準である。

➤ **現状評価基準 (Temporal Metrics)** ^[3]

脆弱性の現在の深刻度を評価する基準である。Exploit コード/PoC コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値(Temporal Score)を算出する。この基準による評価結果は、脆弱性への対応状況に応じ、時間が経過すると変化する。ベンダや脆弱性を公表する組織等が、脆弱性の現状を表すために評価する基準である。

➤ **環境評価基準 (Environmental Metrics)** ^[3]

ユーザの利用環境も含め、最終的な脆弱性の深刻度を評価する基準である。脆弱性の対処状況を評価し、CVSS 環境値(Environmental Score)を算出する。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、ユーザ毎に変化する。ユーザが脆弱性への対応を決めるために評価する基準である。

これらの評価基準は、必ずしもすべての評価基準を考慮しなくとも、基本評価基準だけを用いて値を算出するといったことが可能である。一方で、CVSS の管理母体である FIRST (Forum of Incident Response and Security Teams) も推奨しているとおり、リスク評価を適切に実施するためには、基本評価基準+現状評価基準に加えて、システム環境を考慮した環境評価基準が必要である。しかしながら、この環境評価基準を算出するにはセキュリティの専門的な知識が必要であり、算出が複雑であるため、利用している企業は少ないのが現状である。この CVSS 環境値算出の全体像は、図 1-1 のとおりである。

CVSSv3.1 の詳細については、Appendix A 節を参照して頂きたい。

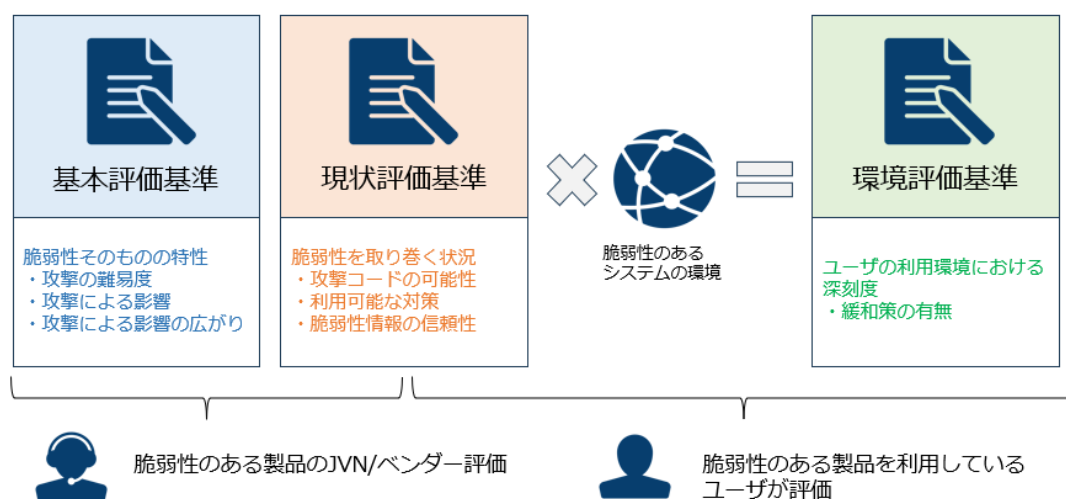


図 1-1 CVSS 環境値算出の全体像

1.2.2 特徴

CVSS v3.1 は、スコアを算出する際の評価基準が明確で透明性が確保された評価指標となっている。しかしながら、算出されるスコアからリスク評価に対する意思決定には直接紐づかないため、評価者側で自ら設定する必要がある。

CVSS 基本値は、リスクではなく脆弱性そのものの深刻度を算出している。公的機関やベンダーで算出される値となるため、企業内でのリスク評価の 1 つとして広く利用されている。そのため、活用法のノウハウが多く存在する利用しやすい評価値となっている。ただし、スコアリングの性質上±0.5 ポイントの誤差が許容されるため、スコアから判定される重大性（Critical/High/Medium/Low）の分類がブレる可能性が存在する。また、脆弱性そのものの深刻度を測定するという特性上、実環境での影響や実際に攻撃を受ける可能性となる脅威に関する評価がなされていない。

CVSS 現状値は、リアルタイムの脅威情報に基づいて、実際に攻撃を受ける可能性の脅威度を算出する。公的機関やベンダーで値が算出される場合もあるが、実際にはその評価が提供

第1章 評価指標

される場合は少ない。そのため、評価者側で脅威情報を確認し、スコアを算出する必要がある。

CVSS 環境値は、実環境に沿ってスコアを評価者側で算出するため、実際のシステムに対して適切にリスク評価が可能である。一方で、実環境を正確に評価するには、評価者側で十分に資産・構成情報を平常時から管理しておく必要がある。これに加えて、評価するための項目の選定時に専門的な知識を有するため、CVSS 環境値の利用は形骸化している。

1.3 CVSS v4.0

1.3.1 概要

CVSS v3.1 の次のバージョンとして、CVSS v4.0 が FIRST より 2023 年 10 月に公開された。CVSS v3.1 と v4.0 では類似する特徴も多いため、1.3 節では CVSS v3.1 との差分にフォーカスを当てて説明する。

CVSS v4.0 では CVSS v3.1 から大きく 5 つの観点で変更が加えられている。

- ① 評価基準に“攻撃の難易度”と“攻撃による影響”を加味
- ② 脆弱性悪用時の影響の広がり具合を表す「スコープ」項目を除去
- ③ 「現状評価基準」を「脅威評価基準」へ名称変更し、3 つあった項目を「攻撃の成熟度」のみに改編
- ④ 脆弱性対応を行う上で有用となる情報を提供する「補助評価基準」の新設
- ⑤ CVSS v3.1 までは計算式から算出していたが、CVSS v4.0 では 270 個のスコア区分に振り分けた後、微調整をして算出（スコア算出方法の変更）

環境評価基準については大きな変化はなかったため、基本評価基準と脅威評価基準の概要について説明する。

➤ 基本評価基準 (Base Metrics)

脆弱性そのものの特性を評価する基準である。情報システムに求められる 3 つのセキュリティ特性「機密性(Confidentiality Impact)」、「完全性(Integrity Impact)」、「可用性(Availability Impact)」に対する影響を、脆弱なシステムとそのシステムに関連する他のシステムに対して複数の項目で評価し、CVSS 基本値(Base Score)を算出する。この基準によって算出されたスコアは固定であり、時間の経過や利用環境によって変動しない。ベンダや脆弱性を公表する組織等が、脆弱性の固有の深刻度を表すために評価する基準であるといえる。

➤ 脅威評価基準 (Threat Metrics)

脆弱性の現在の深刻度を評価する基準である。Exploit コード/PoC コードの出現有無や悪用状況などから評価し、CVSS 脅威値(Threat Score)を算出する。脅威値は、脆弱性への対応状況に応じ、時間経過によって変化する。ベンダや脆弱性を公表する組織等で評価されることもあるが、一般的には評価者側で評価する基準である。

第1章 評価指標

以上を踏まえて、CVSS v4.0 の評価基準の全体像を表したものが図 1-2 である。なお、オレンジ色で囲まれた箇所は CVSS v3.1 から変更があったものである。

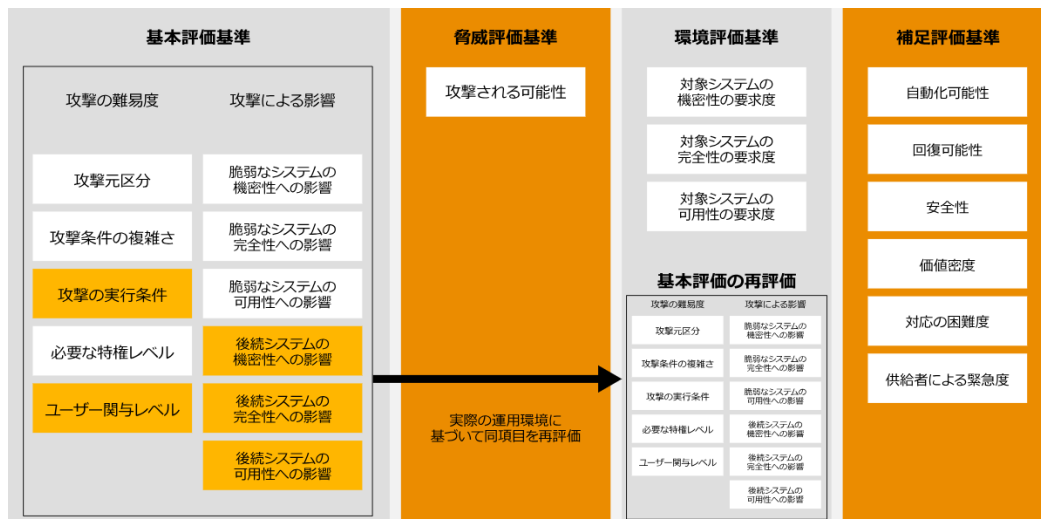


図 1-2 CVSS v4.0 の評価基準の全体像 [4]

CVSS v4.0 では、「基本評価基準 (B)」、「脅威評価基準 (T)」、「環境評価基準 (E)」の3つの評価基準が存在する。これらの組み合わせによって、算出されるスコアの名称が異なる。例として、基本評価基準 (B) × 脅威評価基準 (T) では「CVSS-BT」となる。図 1-3 では、組み合わせとその名称を表している。

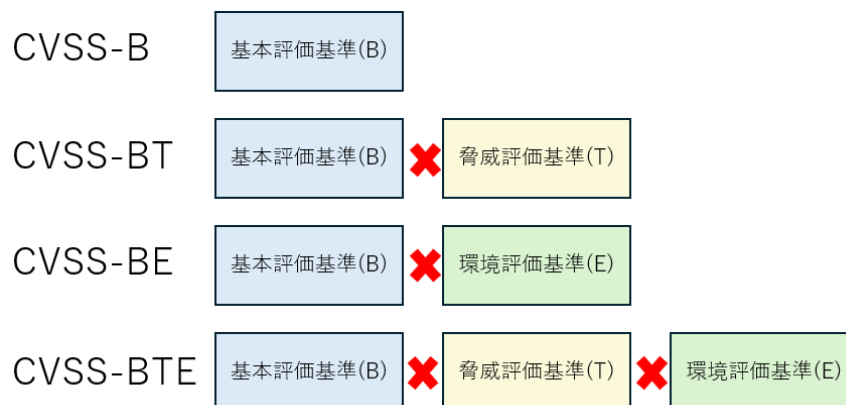


図 1-3 CVSS v4.0 での評価基準の名称

上記のいずれのケースでも全てのグループ (基本評価基準・脅威評価基準・環境評価基準) のメトリクスの値がスコア計算では利用される。算出していないメトリクスの値は既定値である「未定義」として計算される。例えば、CVSS-B を算出する場合、脅威評価基準と環境評価基準は「未定義」としてスコア計算に利用される。

そのため、どのメトリクスグループをスコアリングに利用したかを明確にするため、「CVSS-B:5.0」「CVSS-BE:8.2」といった表記が推奨されている。

CVSSv4.0の詳細については、Appendix B節を参照して頂きたい。

1.3.2 特徴

v4.0はv3.1の改良版であるため、CVSSに関する基本的な特徴は1.2.2節を参照いただきたい。ここではv4.0にフォーカスした特徴を述べる。

v4.0は2023年11月に公開されてまだ日が浅いということもあり、本書執筆時点では企業での運用例がまだ少なく、運用方法や活用方法の収集は容易ではない。とはいえ、ベースとなっているv3.1は広く用いられている評価指標であり、評価項目等の変更はあるものの利用方法はv3.1と大きく変えずに導入できるため、今後普及していくと考えられる。

v3.1でユーザ側での評価が難しいとされていた環境評価基準の「スコープ」や現状評価基準はv4.0では項目がより詳細に分解され、簡素化したことでユーザ側での評価がしやすくなるように工夫されている。また、v4.0ではICSへの活用も考慮されており、環境評価基準にある「後続システムへの完全性への影響」と「後続システムへの可用性への影響」に関して「安全性(Safety)」という選択項目が追加されており、本項目はICSが脆弱性を悪用された際に人身に被害を与える可能性がある場合に選択されるものとなっている。

新たに設定された補足評価基準は脆弱性の対応にフォーカスされた項目設定がされており、スコアの算出には使用されないが、組織がシステムの脆弱性に対処するにあたって有効となる補足的な情報が提供される。これにより脆弱性情報の利用者側で、補足評価基準で共有された情報を参考にリスク分析を強化するために利用できる。

1.4 SSVC v2.1

1.4.1 概要

SSVC (Stakeholder Specific Vulnerability Categorization) は、3 種類のステークホルダの観点から脆弱性に対するリスク評価を実施する指標である。^{[5][6]}ステークホルダごとに決定木が用意されており、この決定木を利用することで透明性があり説明可能なリスク評価が可能となっている。ステークホルダとしては、デプロイヤー・サプライヤー・コーディネーターが存在している。(表 1-1)

表 1-1 SSVC におけるステークホルダの分類

ステークホルダ	対象
デプロイヤー	脆弱性の対応としてパッチ適用を実施する組織
サプライヤー	製品開発ベンダとしてパッチを提供する組織
コーディネーター	脆弱性情報を統制する組織

また、SSVC では出力結果として脆弱性に対する対応優先度が算出されるので、出力結果がそのまま意思決定に直結する構造になっている。

本書では、SSVC のバージョン 2.1 (以下 SSVC v2.1) について取り扱い、ステークホルダとしてはデプロイヤーツリーに重点を置いて説明する。なお、SSVC の詳細については、Appendix C 節を参照頂きたい。

➤ デプロイヤーツリー

デプロイヤーの決定木では、条件分岐において Exploitation / Exposure / Automatable / HumanImpact の 4 種類が存在しており^[6]、それぞれの概要は以下の図 1-4 のとおりである。

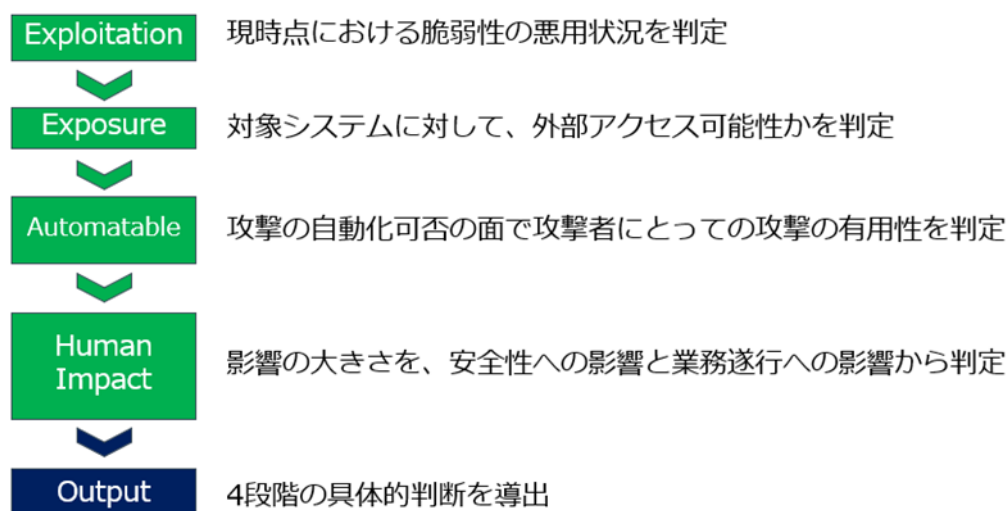


図 1-4 デプロイヤーツリーの概要図

Output では、意思決定に直結する判断結果が提供される。判断結果は表 1-2 のとおり、「Defer/Scheduled/Out-of-Cycle/Immediate」の 4 種類が存在する。

表 1-2 デプロイヤーツリーの Output

ステークホルダー	判断（決定木の出力）
デプロイヤー (パッチ適用側)	• Defer: 対応不要 • Scheduled: 定期メンテナンス時に対応 • Out-of-Cycle: 定期メンテナンス以外の早い時期に対応 • Immediate: 迅速な対応

1.4.2 特徴

SSVC では、ステークホルダごとに意思決定を取り扱う決定木が用意されており、評価者の立場に合わせてリスク評価が可能である。また、決定木に基づいた評価を実施するため、透明性があり説明可能なアプローチとなっている。これは各選定ポイントにおいてどのような判定を選択したか確認可能であり、必要であれば選定ポイントに遡り再評価も可能である。

デプロイヤーツリーにおいては、「Exploitation」での脅威情報を考慮する分岐点で状況に応じて判定を変更する必要がある。決定木では、このように状況に応じて変化するポイントに対して柔軟に評価を変更可能である。さらに、出力結果として具体的な判断・行動指針が導出されるため、脆弱性に対するリスク評価時の意思決定に有効なアプローチとなっている。

第1章 評価指標

一方で、実環境に沿って評価する項目においては、評価者側で十分に資産・構成管理情報を平時から管理・把握しておく必要がある。さらに、「Exploitation」の脅威情報を取得するには、セキュリティの専門的な知識を有する人材や脅威インテリジェンスサービスの利用が必要となる。一般に公開されている情報から脅威情報を取得することも可能ではあるが、情報の抜け漏れや過大評価されている情報等に惑わされ、適切にリスクを評価できない可能性がある。

1.5 EPSS

1.5.1 概要

EPSS (Exploit Prediction Scoring System) は、脆弱性対応の優先度を判断するための指標として FIRST によって開発されている仕組みで、今後 30 日以内に脆弱性が悪用される蓋然性を一定の計算式によって算出するものである^[7]。EPSS は、悪用された事実とその可能性を考慮する必要があるという思想のもと、脅威動向を取り入れた評価指標となっている。

EPSS モデルは 2021 年に公開されてから 2 度のアップデートを経ており、2024 年 6 月現在は EPSS モデルのバージョン 3 (以下 EPSS v3) が利用されている。今後も EPSS モデルはアップデートされる可能性があるが、本書では執筆時点で最新のバージョンであるバージョン 3 に関して言及する。EPSS の詳細については、Appendix D 節を参照頂きたい。

1.5.2 特徴

EPSS は、脆弱性情報と悪用情報から機械学習を用いて、30 日以内に悪用される可能性を確率として算出する指標である。脆弱性のリスク評価において脅威情報の取得は困難であるが、EPSS を利用することで脆弱性に対する脅威を簡易的に評価することが可能である。さらに、EPSS では日次で値が算出されるため、リアルタイムでの評価指標となる。また、脅威ベースでの評価指標となるので、各脆弱性に対して脅威を加味し、効率的な対応優先度を設定可能である。ただ、機械学習を活用するため、算出過程に透明性がなくブラックボックスとなっており、結果に対する説明が不明瞭となっている。また、結果に対する意思決定のためのガイドラインも存在しておらず、算出値に対する対応基準は評価者側で設定する必要がある。これに加えて、EPSS スコアは日々変動するため、運用面においてもどのタイミングで活用するか、どの程度信頼性があるかの検討も利用者側で考慮する必要がある。さらに、EPSS は米国機関が管理運営している指標となるため、日本製品に対しては脅威情報が不足し、算出される EPSS スコアが低くなってしまう懸念点が存在する。

最後に、本書では EPSS v3 について紹介しているが、年次でバージョンが更新されていることもあり、最新バージョンの動向を確認し利用する必要がある。

1.6 KEV

1.6.1 概要

KEV (Known Exploited Vulnerabilities) は、CISA(アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁)が公開している実際に悪用が確認された脆弱性を掲載したカタログである。

アメリカの政府機関においては、拘束力のある運用指令(BOD22-01)に基づいて期限付きの対応義務がある。民間企業に対しては義務はないものの、カタログに掲載される脆弱性を優先的に対応することでセキュリティを大幅に強化できるとして KEV の利用を強く推奨している。また、KEV に掲載される脆弱性は地域性を考慮しないものとなっているが、CISA が主導しているため基本的に米国目線となっており、日本だけで使われている製品の脆弱性や日本だけがターゲットの攻撃は KEV カタログに掲載されない恐れがあり、利用する際には注意が必要である。

下記の 3 要件を全て満たした脆弱性が KEV に記載される。

- ① CVE-ID が割り当てされている
- ② 悪用されていることを示す証拠がある、あるいは実際に攻撃が観測されている
- ③ 明確な修復措置がある

① CVE-ID が割り当てされている

CVE は個別製品中の脆弱性を対象として、米 MITRE 社が採番している脆弱性を一意に識別するための識別子である。JVN も CVE と連携しており、公表する脆弱性に CVE-ID を発番している。

② 悪用されていることを示す証拠がある、あるいは実際に攻撃が観測されている

ここでの悪用の証拠とは、ハニーポット上で脆弱性を突く攻撃を観測しているが、実環境への攻撃成功は観測されていない状態を表している。一方で、攻撃の観測は実環境への攻撃成功が観測されている状態を表している。

スキャンなどの攻撃準備段階を検知した場合や PoC コードの公開がされた場合も、それだけでは攻撃が観測されたとは判定されず、実際に攻撃が行われたという明確な事実が記載の根拠になる。

③ 明確な修復措置がある

メーカーやベンダから修正プログラムやパッチが公開されていることを示す。また、サポートが終了している製品の場合、緩和策や回避策が提示されていることを示す。（例えば、web管理画面に脆弱性があるので機能を無効化する等）

KEV は CISA の公式ホームページで確認することができる。他にも CSV/JSON 形式でも提供されている。それらの各項目と概要は表 1-3 のとおりとなっている。

表 1-3 KEV で公開される情報

項目	概要
CVE-ID	CVE-ID
Vendor Project	メーカー名
Product	対象製品
Vulnerability name	脆弱性の名前
Date added	KEV カタログへの追加日
Short description	事象の概要
Required action	必要な対応
Due date	対応期限（米国政府機関のみ対象）
Known ransomware campaign use	ランサムウェアキャンペーンで利用されたか
notes	参考リンク

1.6.1 特徴

KEV の最大の特徴は、CISA によって発行された、すでに悪用が確認された脆弱性をまとめたリストであるということである。

KEV はカタログであるため、利用者は参照する以外の作業が発生せず、利用時の運用負荷が少なく誰でも利用できるというのが大きなメリットとなる。ただし、KEV はあくまで CISA による維持管理がされておりアメリカの主観によるものであるため、日本特有の製品や日本でのみ悪用が進んでいる脆弱性についての情報は反映されない恐れがある点には注意が必要である。また、実際に悪用が確認された脆弱性の中の数パーセントしか KEV に掲載されていないといった情報もあり^[8]、網羅性は十分ではないこと、悪用から KEV への掲載にタイムラグがあることも利用時には注意が必要である。日本国内での攻撃状況や日本特有製品に特化した、悪用された脆弱性のカタログが存在すればより日本国内で利用しやすいが、残念ながら現在ではそういったものは日本の公的機関からは出されていない。

1.7 評価指標まとめ

ここまで評価指標として、CVSS v3.1 / CVSS v4.0 / SSVC / EPSS / KEV について解説してきた。これらを脆弱性の優先順位付けに利用するにあたり、それぞれの指標の役割を把握しておく必要がある。

本書ではこれら指標の役割をリスクの脅威・脆弱性・資産の3分類で図 1-5 に整理した。ここで、CVSS v3.1 および CVSS v4.0 について、特性は同様となるので、CVSS として取り扱う。なお、脅威・脆弱性・資産の定義は「1.1 リスク評価の考え方」にて解説した通りである。また、CVSS における各評価基準の名称を以下とする。

- CVSS 基：CVSS 基本値
- CVSS 現：CVSS 基本値 + CVSS 現状値/脅威値
- CVSS 環：CVSS 基本値 + CVSS 現状値/脅威値 + CVSS 環境値

リスク	脅威	脆弱性	資産
手法	悪用実績&攻撃コード公開	脆弱性自体の深刻度	自社環境を考慮
CVSS基		○	
EPSS	○		
CVSS現/脅	○	○	
CVSS環	○	○	○
SSVC	○	○	○
KEV	○		

図 1-5 各リスク評価指標の比較表

図 1-5 の各評価指標の比較表について説明する。CVSS 基は、脆弱性そのものの深刻度のみを指標している手法であるので、脆弱性のみ分類される。EPSS は、脆弱性そのものの深刻度を評価せず、今後 30 日以内に悪用される可能性、すなわち悪用実績を評価している手法であるので、脅威に分類される。CVSS 現は、リスク評価時の脅威情報に基づいて評価される手法となるので、脅威に分類される。また CVSS 現は、CVSS 基も含まれる評価になるので、脆弱性にも分類される。CVSS 環は、自社環境を考慮した評価がなされるので、資産に分類される。また CVSS 環は、CVSS 基と CVSS 現も含まれる評価になるので脆弱性と脅威の分類にも含まれている。ここで CVSS 現については、リスク評価時に含まれない(未評価となる)場合もあるが、その際には CVSS スコアが最大値となるように値が算出されるため、脅威情報も含まれるものとしている。SSVC は、決定木の各項目で脅威・脆弱性・資産を考慮しているため、3

つ全てに分類されている。最後に、KEVは悪用されていることを示す証拠がある、あるいは実際に攻撃が観測されていることが考慮されているため、脅威に分類される。

脆弱性対応業務において、各脆弱性のリスク評価を実施する際には、脅威・脆弱性・資産の3要素全てを含んだ評価することが望ましいと考えられる。図1-5からも分かる通り、CVSS基のみの評価では脆弱性に対する脅威や実環境を加味した評価を実施できていないため、十分なリスク評価を実施できていないといえない。また、脅威情報を加味しない評価では、本来は対応優先度が低い脆弱性に対しても対応を優先してしまう可能性があり、対応の効率性からも適切でないと言える。

これらを踏まえたうえで、2章では各評価指標の役割を考慮したリスク評価手法の例を示す。



第2章

各評価指標を活用したリスク評価

2 各評価指標を活用したリスク評価

2.1 各評価指標の活用検討

脆弱性対応業務におけるリスク評価では、1.7節で述べた通りリスクの3要素として脅威・脆弱性・資産を考慮した評価を実施する必要がある。しかしながら、日々公開される脆弱性情報の数は膨大であり、リスク評価が複雑な指標では運用リソースの負荷が大きくなることや専門的な知識を求められる等の問題から全てを評価するのは現実的ではない。そこで本書の活用方針では、1次評価と2次評価の2段階でリスク評価を実施する。リスク評価段階分けイメージを図2-1に示す。まず1次評価で運用リソースの負荷が少ない簡易的な評価を実施し、リスクが低い脆弱性情報を取り除き、その後、2次評価でリスクの3要素を加味した評価を実施することとする。

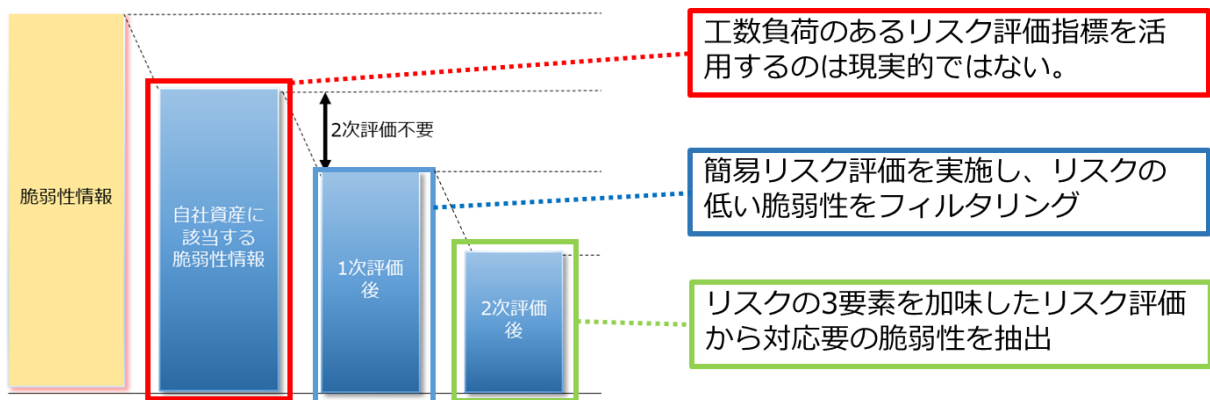


図 2-1 リスク評価段階分けイメージ

ここで、図2-2の各評価指標の役割表から1次評価および2次評価で活用する評価指標について説明する。まず、2次評価で利用される運用リソースの負荷が大きい評価指標として、緑で囲われている資産に分類されるCVSS環やSSVCが挙げられる。これらは、自社の環境を加味し、評価者側で評価を実施する必要があるためである。次に、黄土色で囲われている1次評価で利用される運用リソースの負荷が小さい指標としては、CVSS基、EPSSやKEV等が挙げられる。これらは、外部から提供されるデータとなり、利用者側で評価する必要がないためである。

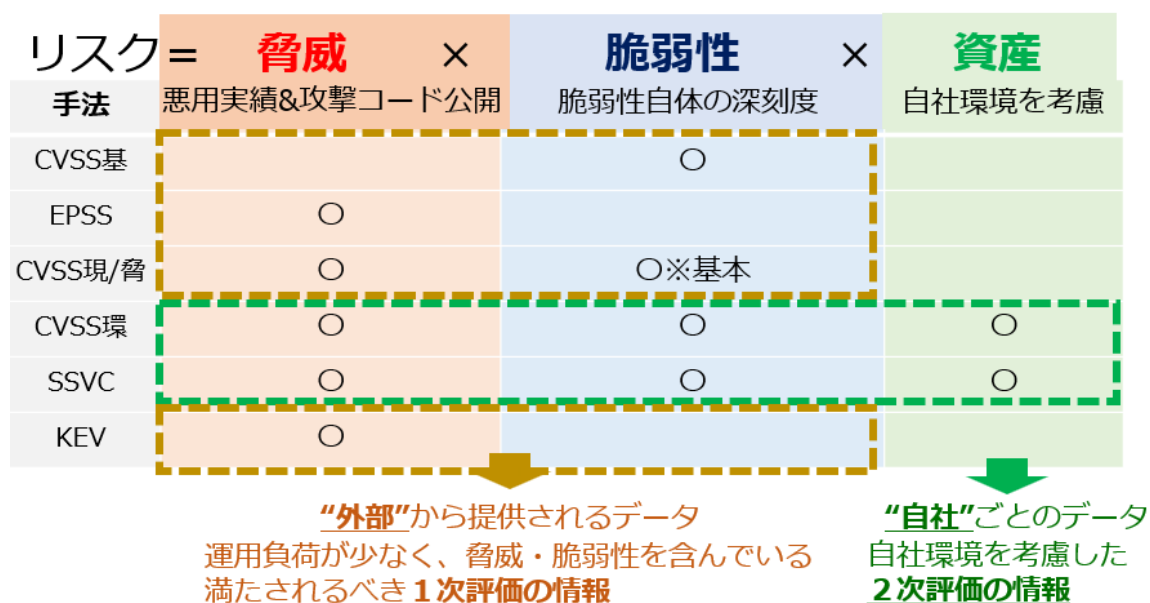


図 2-2 各評価指標の役割表

ここまでの内容を考慮したうえで、1次評価で利用されるのが好ましい指標について紹介する。1次評価の評価指標比較表は、表 2-1 のとおり。1次評価では運用リソースの負荷が小さいことが求められることから、外部組織が評価を提供している指標として CVSS 基と EPSS が該当する。KEV については、1.6.1 節で前述したように脆弱性のカタログであり、カタログに掲載の無い多くの脆弱性についての情報は得られないため、1次評価での利用からは除外する。また、CVSS 現については、外部組織にて評価されることもあるが、実際に評価されている場合は少ない。そのため、評価者側で評価を必要とされるため、運用リソースを中としている。これらより、1次評価では CVSS 基および EPSS の組み合わせ、またはそれぞれを単体で利用するケースが考えられる。

表 2-1 評価指標の比較表（1次評価）

指標	運用リソース	内容
CVSS 基	低	外部ベンダーや公的機関が評価値を算出
CVSS 現	中	基本的には外部組織から算出されるが、実際には値が提供される場合が少なく懸念が残る
CVSS 環	高	すべて自社での評価が必要。2次評価で活用
EPSS	低	FIRST が算出（ただし、スコアの変動あり）
SSVC	高	すべて自社での評価が必要。2次評価で活用
KEV	低	別枠で活用

次に2次評価で利用されるのが好ましい手法について紹介する。2次評価の評価指標比較表は、表2-2のとおり。2次評価ではリスクの3要素を加味した指標としてCVSS環とSSVCが該当する。活用方法については、CVSS環またはSSVCのどちらかを利用するケースが考えられる。

表 2-2 評価指標の比較表（2次評価）

指標	リスク3要素	内容
CVSS 基	なし	外部ベンダーや公的機関が評価値を算出
CVSS 現	なし	基本的には外部組織から算出されるが、実際には値が提供される場合が少なく懸念が残る
CVSS 環	あり	すべて自社での評価が必要。2次評価で活用。
EPSS	なし	FIRST が算出（ただし、スコアの変動あり）
SSVC	あり	すべて自社での評価が必要。2次評価で活用。
KEV	なし	別枠で活用

ここまでの方針を踏まえて、各評価指標の活用例を示す。まずは、これまで紹介した各評価指標を利用し、リスクの3要素を加味した評価例を2つ紹介する。ただし、資産の自社環境を考慮したリスク評価を実施するには、評価者側の運用リソースおよびセキュリティの専門的な知識を有する必要がある。そこで、資産重要度を加味し、限られた運用リソースで対応可能かつ属人的な解釈を取り除いた評価例も紹介する。

2.2 SSVC を活用したリスク評価例

2.2.1 SSVC 活用リスク評価の概要

これまでの説明では、リスク評価を1次評価・2次評価の段階に分けて説明した。ここに緊急対応の必要性が高い脆弱性を評価するための0次評価を追加する。SSVCを活用したリスク評価例の概要は、図2-3の通りである。0次評価では、JPCERT/CCの注意喚起並びにKEVに掲載されている脆弱性、すなわち深刻かつ影響範囲が広い、または悪用実績が確認されている脆弱性を抽出する。例として、Log4jの様な世間的に注目され、緊急性が高い脆弱性情報については、評価者側において即時対応と判断されるケースがある。

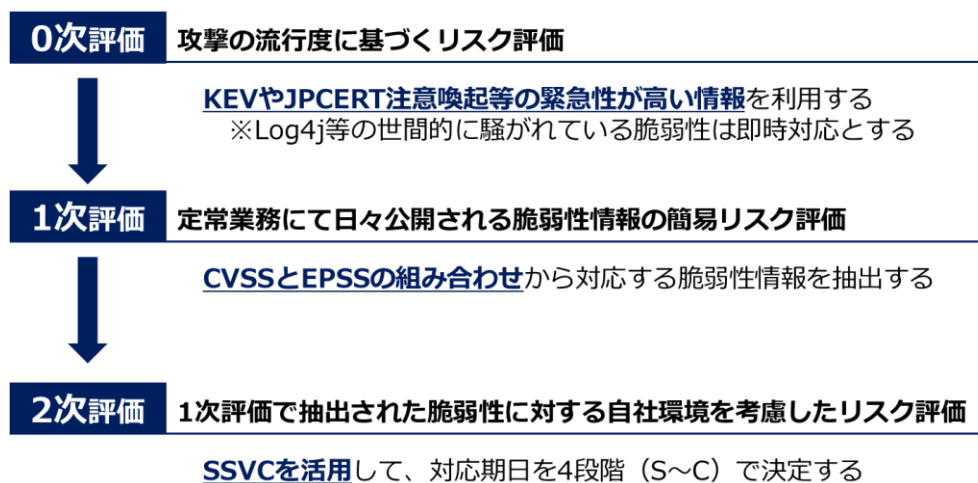


図 2-3 SSVC を活用したリスク評価の 0 次評価

次に、1次評価では日々公開される脆弱性情報の簡易リスク評価として、CVSS と EPSS を組み合わせた評価を実施し、2次評価の対象となる脆弱性情報を抽出する。

最後に、2次評価として SSVC を活用することで自社環境を考慮したリスク評価を実施し、S / A / B / C の4分類でランク付けを行う。各ランク付けを本書では、以下のとおり定義する。

S：即時対応が求められる緊急性の高い評価

A：緊急対応の必要性はないが優先的な対応が望ましい評価

B：緊急対応が不要であり将来的に対応が望ましい評価。

（費用対効果や資産状況に応じてリスク受容することも検討される評価でもある。）

C：リスク受容が妥当であり脆弱性の対処を実施しない評価

ここで各ランクに対する対応期日について、参考例として表 2-3 のとおりとしている。
ただし、これはあくまで目安であり、この期日まで対応しなくても問題がないということを示しているわけではない。また、この期日は各社の規定などに応じて変更することを推奨する。

表 2-3 対応ランクに対する対応期日例

	ランク			
	S	A	B	C
対応期日	即日~3 日以内	30 日以内	定期メンテナンス時	対応しない

2.2.2 0 次評価（攻撃の流行度評価）

0 次評価では、緊急性の高い即時対応を求められる S ランク相当の脆弱性情報を評価する。0 次評価の概要は、図 2-4 のとおり。まず、1 の「世間的に流行している脆弱性情報を取得」では、KEV や JPCERT/CC の注意喚起に掲載されている脆弱性情報を取得する。状況に応じてニュースメディアやソーシャルネットワーキングサービスの情報を活用することで攻撃の流行度を把握し、0 次評価の対象とする。次に 2 の「対象資産が公開・非公開領域かを判定」では、取得した脆弱性情報に該当するシステムが、ネットワーク公開領域か非公開領域で対応を分ける。これは、ネットワーク公開の有無によって攻撃の実行難易度や発生確率（狙われやすさ）が大きく変動するためである。ネットワーク非公開領域の場合には、即座に S ランク判定とするのではなく、2 次評価で自社環境を考慮したリスク評価を実施する。ネットワーク公開領域の場合には、社内のセキュリティ有識者で社内協議を実施し、S ランク判定相当かどうかを判定する。S ランク判定とならなかった場合には、2 次評価で自社環境を考慮したリスク評価を実施する。S ランク判定となった場合には、緊急性が高い脆弱性として、即時対応を実施する。ここで 3 の「公開領域の資産の場合は社内会議により対応判定」で、社内協議を実施する理由として、世間的には流行している脆弱性情報ではあるが、自社環境に照らし合わせた際、対策の必要性がない判断結果となり得る可能性があるためである。この社内協議は無駄な工数やコストをかけないためにも重要なポイントとなり得る。

0次評価

1. 世間的に流行している脆弱性情報を取得
2. 対象資産が公開・非公開領域かを判定
3. 公開領域の資産の場合は社内会議により対応判定

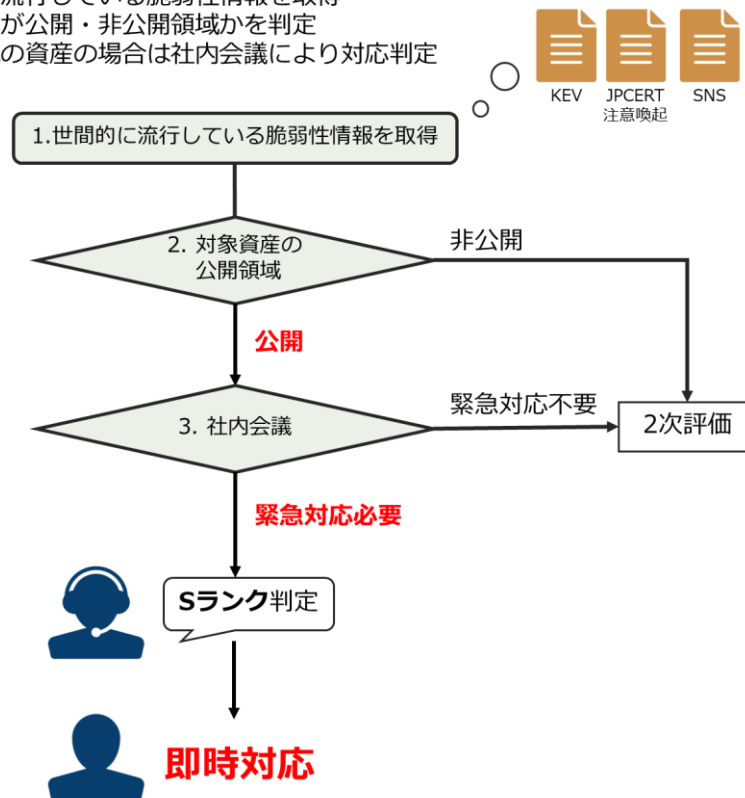


図 2-4 SSVC を活用したリスク評価の0次評価

2.2.3 1次評価（簡易リスク評価）

1次評価では、脅威と脆弱性の両方を加味した簡易リスク評価を実施する。1次評価の目的は、少ない運用リソースで対応不要な脆弱性をフィルタリングすることである。評価指標としてはEPSS+CVSS基を利用する。CVSS基で脆弱性そのものの深刻度を評価し、EPSSでは悪用実績やExploitコード/PoCコードの公開情報等から脅威度を評価する。

この評価例でCVSS基のみではなく、EPSSも組み合わせて活用する理由は、CVSS基のみでは取りこぼしてしまう恐れのある、脅威度の高い脆弱性を拾うためである。つまり、CVSS基本値が低い一方で、脅威度であるEPSSスコアが高い脆弱性に対しても、対応不要と判断せず自社環境と照らし合わせた2次評価を実施する。

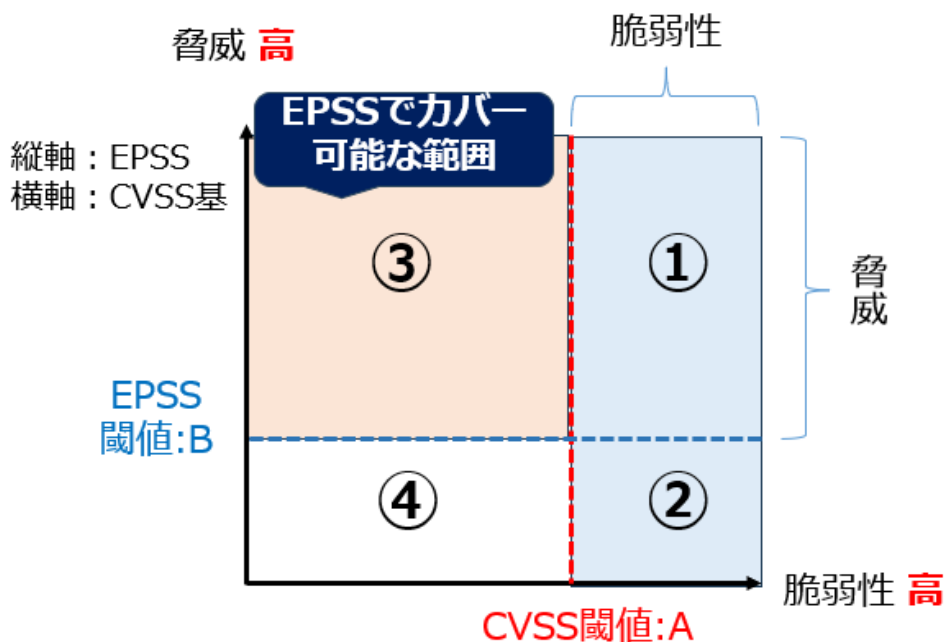


図 2-5 縦軸 EPSS・横軸 CVSS の 1 次評価のリスク分類図

図 2-5 は、一次評価で活用するリスクの分類図である。ここでは、CVSS 基の閾値 A と EPSS の閾値 B を設定し、各脆弱性を①～④の領域に分類する。そして分類した結果、①～③を 2 次評価の対象とし、④は C ランクとする。このようにして、1 次評価の目的である対応不要な脆弱性を少ないリソースで抽出することができる。

先に述べたように、CVSS 基のみの評価では脆弱性そのものの深刻度しか評価できず（①＋②が該当）、CVSS 基が閾値に及ばず実際に悪用されうる脆弱性を取りこぼす可能性がある。しかし、EPSS を活用することで取りこぼしを減らすことが可能となる（③が該当）。この結果、KEV や JPCERT/CC の注意喚起に掲載されない/されづらいが、脅威度が高い情報を包括可能となる。ただし、CVSS 基のみを利用する場合と比べて、対応が必要となる脆弱性の数は増加するため、より多くの運用リソースが必要となる。さらに、CVSS 基のみの評価において対応要となる脆弱性（①＋②が該当）において、EPSS スコアが高くより緊急度の高い脆弱性（①が該当）を抽出可能となり、2 次評価において対応ランクを高くする際の判断材料とすることができる。ここで、それぞれのリスク評価手法に対する閾値の設定が重要となってくるが、我々の検討結果としては、CVSS 基の閾値を 7.0、EPSS の閾値を 1 % とすることを推奨する。(2.5 節参照)

2.2.4 2次評価（SSVCを活用したリスク評価）

2次評価では、評価指標に SSVC を活用する。その理由としては 1.7 節でも説明したように、リスクの3要素を考慮したリスク評価が実施できるためである。脅威情報の更新があった際には、決定木の該当項目を再評価することで、評価時点でのリスク評価が可能である。さらには、SSVC は脆弱性対処の意思決定に直結する具体的なアクションが出力結果となっているため、ランク付けを実施するのに適している。

SSVC の具体的な出力結果とランクの対応としては、図 2-6 のとおりである。Immediate が S ランク、Out-of-cycle が A ランク、Scheduled が B ランク、Defer が C ランク判定となる。

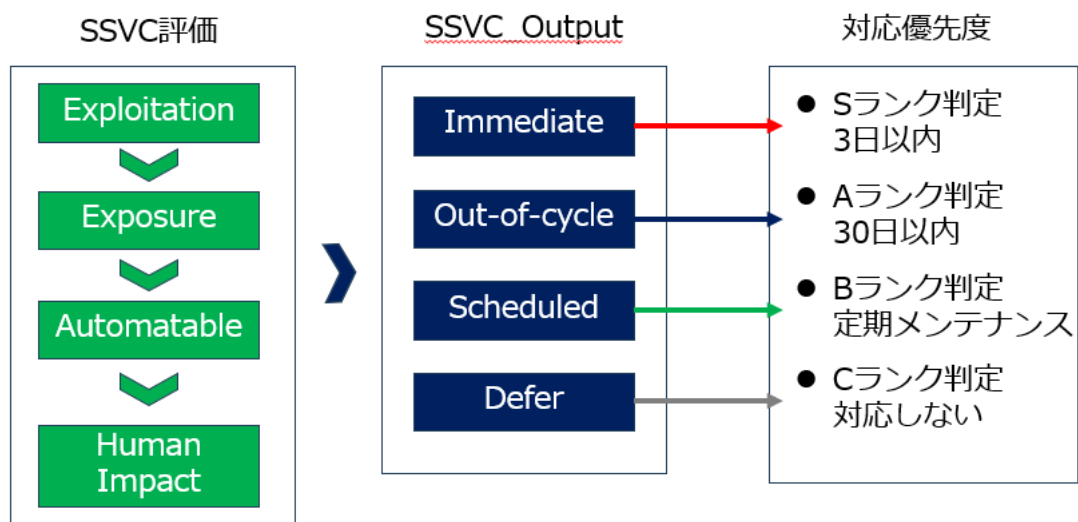


図 2-6 SSVC アウトプットと対応目安

2.2.5 まとめ

本リスク評価を実施することにより、リスクの3要素である脅威・脆弱性・資産の全てを考慮したリスク評価が可能である。SSVC でのリスク評価は、決定木の項目を4種類のみ選定していくだけでランク付けが可能であるため、次節の CVSS 環境値を活用する手法に比べて2次評価の運用リソースは小さくなると考えられる。しかし、SSVC における

「Exploitation」を選択する際には脅威情報が必要となり、この情報収集が困難となる可能性がある。また、「Exposure / Human Impact」を選択する際には、自社内の資産情報を十分に把握している必要がある。「Automatable」の選択については、セキュリティの専門的な知識を有する必要がある、評価が属人化してしまう恐れもある。

2.3 CVSS 環境値を活用したリスク評価例

2.3.1 CVSS 環境値を活用したリスク評価の概要

本活用例では、2次評価で CVSS 環境値を活用したリスク評価を実施する。1.4 節の SSVC を活用した例と同様に 0 次評価、1 次評価、2 次評価の順でリスク評価を実施していく。異なる点としては、0 次評価と 2 次評価である。SSVC を活用した例では、0 次評価においてネットワーク非公開領域の場合、2 次評価する。しかし、CVSS 環境値を活用した例の 2 次評価において 1 次評価の判定を利用するため、0 次評価のネットワーク非公開領域の場合には、1 次評価から実施する必要がある。この時の 1 次評価については、SSVC を活用した例と同様である。2 次評価については、利用する評価手法とランクの設定方法が異なる。2 次評価の評価方法が大きく異なるため、本節では 2 次評価のみを説明する。

2.3.2 2 次評価（CVSS 環境値を活用したリスク評価）

2 次評価では、評価指標に CVSS 環境値を活用する。その理由としては 1.7 節でも説明したように、リスクの 3 要素を考慮したリスク評価が実施できるためである。また、CVSS では評価基準が明確に公開されており、評価の透明性が確保されているのも理由の 1 つである。リスク評価の具体的な方法としては、表 2-4 のとおりである。1 次評価での優先度①～③と CVSS 環境値を組み合わせる最終的なランク（S～C）を選定する。

表 2-4 CVSS 環境値を活用した対応優先度表

	CVE 環境値			
	0 ～ 3.9	4.0 ～ 6.9	7.0 ～ 8.9	9.0 ～ 10.0
優先度①	C	B	A	S
優先度②	C	C	B	A
優先度③	C	B	A	S

ここで考え方のベースは、優先度①・③については EPSS スコアが閾値を超えており脅威度が高い脆弱性となり、②はその逆で脅威度が低い脆弱性となることである。CVSS 環境値は、CVSS の値ごとに深刻度レベルを、9.0～10.0 は Critical（緊急）、7.0～8.9 は High（重要）、4.0～6.9 は Medium（警告）、0～3.9 は Low（注意）の 4 分類にしている。これらの組み合わせとして、まず CVSS 環境値が Critical で、優先度①・③の場合は S ランク判定とし、優先度②の場合は A ランク判定としている。次に、CVSS 環境値が High の場合は、優先度①・③は A ランク判定とし、優先度②は B ランク判定としている。さらに、CVSS 環境

値が Medium で、優先度①・③の場合は B ランク判定とし、優先度②の場合は C ランク判定としている。最後に、CVSS 環境値が Low の場合は、自社環境への影響が少ない、もしくは無視できるものと判断し、優先度①・②・③において C ランク判定としている。

2.3.3 まとめ

本リスク評価を実施することで、リスクの3要素である脅威・脆弱性・資産の全てを考慮したリスク評価が実施可能である。CVSS 環境値を利用する手法では脅威度として CVSS 現状値を活用するので、外部機関が値を算出しており、脅威情報の収集が困難である点を解決可能である。ただし、CVSS 現状値は値が算出されている場合が少ないため、評価者側で情報収集する、もしくは選択項目を未評価として評価値の最大を取る、といった曖昧な評価となる懸念が存在する。また、CVSS 環境値は、「対象システムのセキュリティ要求度」および「環境条件を加味した基本評価の再評価」の多くの項目を評価するなど、評価項目が多く運用リソースが大きくなる。さらに、この評価にはセキュリティの専門的な知識を有することや自社内の資産状況を十分把握しておく必要があり、利用するにはハードルが高く、属人化してしまう恐れもある。

2.4 資産重要度を活用したリスク評価例

2.4.1 SSVC および CVSS 環境値を利用する場合の課題

2.2 節、2.3 節でリスクの3要素である脅威・脆弱性・資産を加味した SSVC および CVSS 環境値のどちらを利用する場合のリスク評価を説明した。しかしながら、これらのリスク評価を実施するには複数の懸念点が存在する。そこで、それら懸念点をリスクの3要素ごとに分けて説明する。

はじめに、脅威については SSVC を利用する際には脅威情報の取得が必要となるが、その取得が困難であり、実際の脅威と異なる評価がされてしまう、もしくは評価が実施できない可能性がある。CVSS 環境値を利用する場合には脅威として CVSS 現状値を利用するが、評価されている場合が少なく評価者側で評価が必要となり、SSVC を利用する場合と同様の課題が発生する。

次に、脆弱性については、SSVC を利用する際には脆弱性を評価する評価軸としては、「Automatable」で攻撃の自動化可否や「Human Impact」で業務影響を考慮した評価が存在しているが、評価項目が曖昧なため属人化してしまう恐れがある。

最後に、資産については、SSVC および CVSS 環境値のどちらを利用する場合でもリスク評価を実施する際の選択項目が担当者によって異なり、評価値がブレてしまう恐れがある。また、脆弱性と資産情報を随時照らし合わせながら評価を実施するため、運用リソースの負荷が大きくなる。

これらをまとめると、SSVC や CVSS 環境値を利用する場合には、リスク評価としては十分に適切な評価が実施可能である一方、運用リソースの増大や専門的知識の要求による属人化といった懸念点が存在することとなる。本節では、これらの課題を解決可能なリスク評価の一例について説明する。

2.4.2 資産重要度を活用したリスク評価の概要

本活用例では、資産重要度を活用したリスク評価を説明する。リスクの3要素を考慮しつつ、SSVC や CVSS 環境値を利用した際の課題を対処する内容となる。

まず、脅威に対しては、EPSS のみを活用することで脆弱性の脅威度を評価する。これにより、EPSS を脅威情報とみなすことで、利用者側で困難であった脅威情報の取得対応を排除することが可能となる。次に、脆弱性に対しては、CVSS 基本値のみを活用することで脆弱性そのものの深刻度を評価する。最後に、資産に対しては、評価者側で資産の CIA（機密性・完全性・可用性）の要求度およびネットワーク公開領域か非公開領域を事前に設定・調査しておくことで自社環境を考慮した評価が可能となる。これらより、運用リソースの最小

化、かつ評価の属人化防止といった効率的な対応が可能となることが期待できる。

リスク評価の流れとしては、図 2-7 のとおりである。SSVC や CVSS 環境値を利用した際と同様に 0 次評価～2 次評価を実施する。ただし、本書における評価を実施するには事前準備が不可欠となる。事前準備とは、各資産に対して CIA の要求度を評価し、そこから資産の重要度を定義することである。0 次評価・1 次評価は CVSS 環境値を活用したリスク評価と同様である。そのため、本節では 2 次評価のみを説明する。

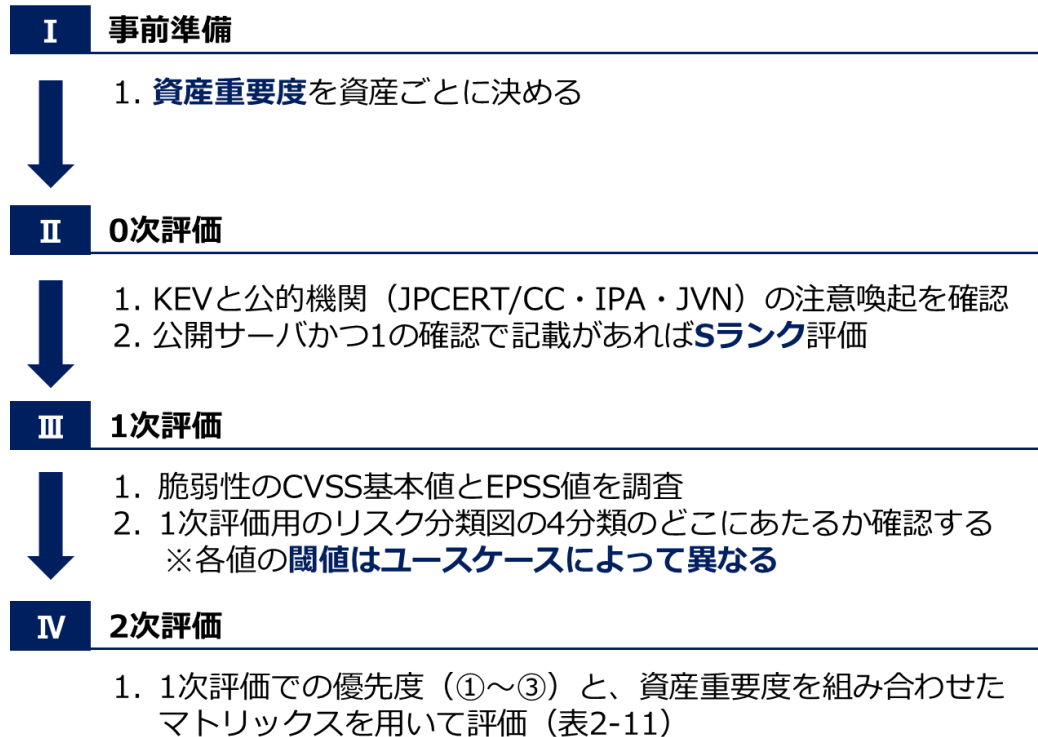


図 2-7 評価の全体の流れ

2.4.3 事前準備（資産重要度の設定）

前節で述べたように、自社環境を考慮した評価を SSVC や CVSS 環境値を利用せずに評価するためには、事前準備として資産重要度をあらかじめ設定する必要がある。資産重要度は機密性の要求度・完全性の要求度・可用性の要求度を低・中・高の3段階で評価し、各々の評価に定められた点数の合計点により決定される。

資産重要度の評価は、CVSS 環境値の評価項目を参考に定義している。機密性・完全性・可用性の要求度の評価は、評価者側でシステムに対して低・中・高を設定し、それぞれ1点・2点・3点の点数を付与する（表 2-5）。これら3項目の合計点から資産重要度が決定される。この合計点が、3~4 なら低、5~7 なら中、8~9 なら高となる（表 2-6）。なお、本資産重要度の設定値はあくまで参考であり、自社にて設定を算出・評価し意思決定する必要がある。

表 2-5 資産重要度の判定表

	評価		
	低	中	高
機密性の要求度	1	2	3
完全性の要求度	1	2	3
可用性の要求度	1	2	3

表 2-6 判定合計値と資産重要度の紐づけ表

	合計点数		
	3 ~ 4	5 ~ 7	8 ~ 9
資産重要度	低	中	高

参考：機密性・完全性・可用性の評価基準例

表 2-5 にて各資産に対して機密性・完全性・可用性の評価を低・中・高の3段階で実施することを示したが、その各評価の基準の例を以下に掲載する。ただし、これはあくまで一例であり、自社の規定やガイドラインに応じて変更することを推奨する。

表 2-7 機密性の評価基準例

点数	評価	説明
3	高	特定の関係者または部署のみに開示・提供できる情報を保持
2	中	組織内で開示・提供できる情報を保持
1	低	第三者に開示・提供できる情報を保持

表 2-8 完全性の評価基準例

点数	評価	説明
3	高	情報の内容を改ざんされた場合、ビジネス影響は深刻かつ重大
2	中	情報の内容が改ざんされた場合、ビジネスへの影響は大きい
1	低	情報の内容が改ざんされた場合、ビジネスへの影響は小さい

表 2-9 可用性の評価基準例

点数	評価	説明
3	高	・ 24/365 のうち 99.9%以上利用できることを保証 ・ 1 分以上のシステム停止が許容されない
2	中	・ 業務時間内もしくはサービス利用時間の利用は保証 ・ 1 時間のシステム停止が許容される
1	低	1 日の情報システム停止が許容される

2.4.4 2次評価（資産重要度を活用したリスク評価）

2次評価では、資産重要度を活用したリスク評価を実施する。事前準備で設定した資産重要度と1次評価でCVSS基本値とEPSSを活用した優先度①～③の評価を掛け合わせてリスク評価する。ただし、使用する2次評価のマトリクスは、該当資産のインターネット公開の有無によって異なるものを使用する。これは公開の有無によって、脆弱性を突いた攻撃の難易度や悪用可能性が左右され、リスクが異なるためである。

2次評価のマトリクスでは、資産重要度が高いほど攻撃を受けた際の影響が大きいことから、対応ランクは資産重要度に沿って高く設定している。また、公開サーバと非公開サーバでは、公開サーバの方が前述の通りリスクが大きくなるため、対応ランクが非公開サーバに比べて一部では高くなるように設定している。

表 2-10 2次評価マトリクス（公開サーバ）

	資産重要度		
	低	中	高
優先度①	B	A	S
優先度②	C	B	A
優先度③	C	B	B

表 2-11 2次評価マトリクス（非公開サーバ）

	資産重要度		
	低	中	高
優先度①	B	A	A
優先度②	C	B	B
優先度③	C	C	B

まず、表 2-10 の公開サーバのマトリクスについて説明する。優先度①については、脅威と脆弱性のスコアが両方とも高い水準にあり、その中で資産重要度が高の場合には S ランク判定、中の場合には A ランク判定、低の場合には B ランク判定としている。次に優先度②については、脅威のスコアが低く脆弱性のスコアが高い水準にあり、その中で資産重要度が高の場合には A ランク判定、中の場合には B ランク判定、低の場合には C ランク判定としている。最後に優先度③については、脅威のスコアが高く脆弱性のスコアが低い水準にあり、その中で資産重要度が高・中の場合には B ランク判定、低の場合には C ランク判定としている。

次に、表 2-11 の非公開サーバについて説明する。非公開サーバにおいては、外部ネットワークにさらされておらず、公開サーバに比べてリスクが小さいため、対応ランクは公開サ

サーバよりも低くなるように設定している。非公開サーバにおいては、公開サーバに比べ攻撃者が脆弱性を突いた攻撃を実施する難易度や攻撃に要する時間が大きく異なることから、緊急対応が必須となる脆弱性は基本的にはないとの考えのもと、対応ランクの判定を最大で A ランクとなるようにしている。よって、非公開サーバの脆弱性については、基本的に対応ランクが B ランク判定となるようにし、特にリスクの高い脆弱性についてのみ A ランク判定となるようにしている。まず優先度①については、脅威と脆弱性のスコアが両方とも高い水準にあり、その中で資産重要度が高・中の場合には A ランク判定、低の場合には B ランク判定としている。次に優先度②については、脅威のスコアが低く脆弱性のスコアが高い水準にあり、その中で資産重要度が高・中の場合には B ランク判定、低の場合には C ランク判定としている。最後に優先度③については、脅威のスコアが高く脆弱性のスコアが低い水準にあり、その中で資産重要度が高い場合には B ランク判定、中・低の場合には C ランク判定としている。

2.4.5 まとめ

本リスク評価を実施することにより、リスクの3要素を加味したリスク評価をしつつ、SSVC や CVSS 環境値を利用する際の課題としている運用リソース増大やリスク評価の属人化を解決することが可能である。ただし、脅威については EPSS のみの活用であり、EPSS の特徴でも前述しているとおり、日本製品については正確な値が算出されない懸念が残る。また資産について、CVSS 環境値の評価項目を簡易化して事前に設定する方法になるので、CVSS 環境値ほど正確に自社環境を考慮した評価にはなりえないことには留意すべきである。本リスク評価手法においては、評価に対してリソースの最小化と属人化防止を目的としており、また機械的に評価することが可能である。そのため、膨大な工数を求められる脆弱性対応業務において、自動化も視野にいれることのできる評価となっている。

2.5 1次評価の閾値

2.2.3「1次評価（簡易リスク評価）」では、評価時に利用する各閾値について、CVSS 基本値を 7.0、EPSS スコアを 1%と設定することを推奨した。ここでは、我々が設定した各閾値の根拠について説明する。なお、本閾値はあくまで我々が検討した結果の一例であり、実際に 1 次評価を実施する際には各企業で検討の上、適切な閾値を設定することを強く推奨する。

2.5.1 閾値の必要性

閾値を設定することにより、属人的な判断に委ねることなく、明確な基準をもってリスク評価を実施することができる。さらには、経営層やシステム担当者に対応理由を述べる際の重要な情報の 1 つともなるだろう。

しかしながら、閾値は明確な根拠をもって決定することが難しい。そこには、主に自社の脆弱性対応へのニーズや、各評価指標の特性等への理解不足といった背景があるためと考えられる。また、CVSS 基本値や EPSS の説明などは世にあるものの、閾値を設定するための明確な情報が存在していないためでもある。

そこで、本節ではそれらの背景を踏まえて、どのようにして各評価指標に対する閾値を決定すべきか、我々が推奨する閾値を導き出したプロセスと併せて説明する。

2.5.2 閾値の考え方

先に述べたように閾値を決める際には、脆弱性対応に関する各企業のニーズが大きな指標となり得る。ここでの脆弱性対応に関する各企業のニーズとは、「対応人員のリソースや対応コスト及び、自社の社会的立場等を鑑みて、どの程度のリスクの脆弱性を優先して対応するか、またどの程度のリスクの脆弱性はリスク受容するか」といった考えを指している。このニーズを踏まえて、閾値決めをする際に考慮すべき事項となるのが以下に挙げた「効率性」と「網羅性」である。効率性と網羅性のイメージと算出方法は、図 2-8 のとおり。

◇ 効率性

対応する脆弱性のなかに、実際に悪用されている脆弱性がどれだけ含まれているかの割合を指す。つまり、効率性が高いことは、本来対応を必要としない脆弱性（＝悪用実績がない、もしくは悪用される可能性の低い脆弱性）への無駄な対応を最小限に抑えることができ、効果的な脆弱性対応を少ないリソースで実施できていることを意味する。

◇ 網羅性

対応する脆弱性が、実際に悪用されている脆弱性をどれだけ包括しているかの割合を指す。つまり、網羅性が高いことは、本来対応すべき脆弱性(＝実際に悪用されている、もしくは悪用される可能性の高い脆弱性)の取りこぼしが少ないことを意味する。

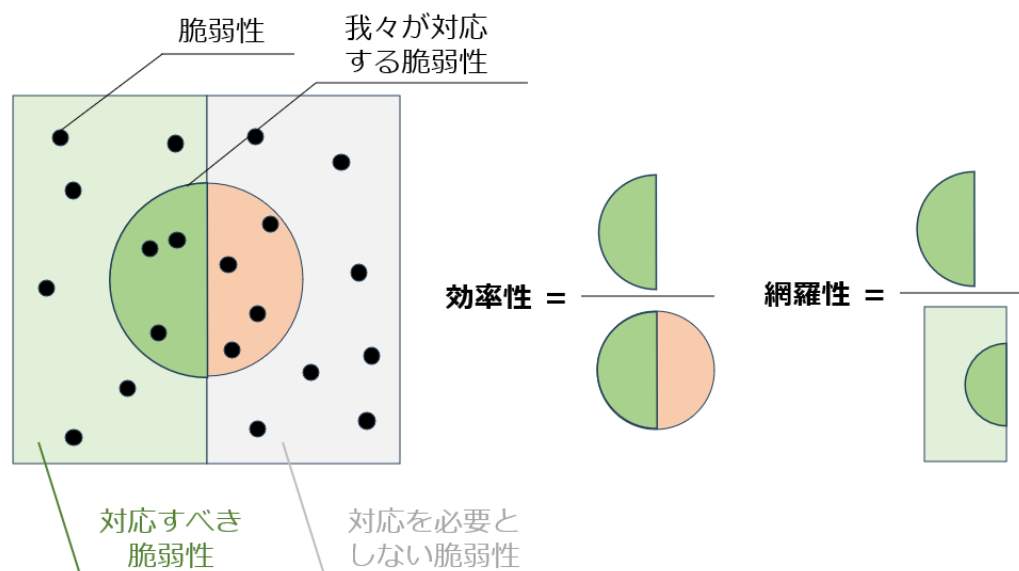


図 2-8 効率性と網羅性の算出^[9]

この2つが共に高い数値となる閾値を設定するのが理想だが、実際にそのような閾値を設定することは不可能に近い。表 2-7 は、RSA Conference 2019 で、Cyenta Institute の Jay Jacobs 氏と Kenna Security の Michael Roytman 氏（英語記事）が、『The Etiology of Vulnerability Exploitation（脆弱性悪用の病因学）』と題した研究にて掲載した、各 CVSS 基本値を閾値として対応した場合の効率性と網羅性を示したものである。

表 2-7 各 CVSS 基本値での効率性と網羅性^[9]

CVSS 基本値	効率性 [%]	網羅性 [%]
10	23.1	7
9	23.2	14.5
8	23.1	14.9
7	31.5	53.2
6	29.2	65.9
5	26.1	80.8

表 2-7 を見ると、CVSS 基本値が 7.0 までは効率性・網羅性共に向上することが確認できるが、それより低いスコアになると網羅性は向上が見られる一方、効率性は低下する。つま

り、自社環境をセキュアにすることを重視して網羅性を求めれば、それだけ効率性が下がり、必要となる人的・金銭的リソースが増えることとなる。
このことから、これらの関係は相反する関係であり、自社の企業ニーズに合わせて最もバランスの取れた閾値を決めることが求められると言える。

ニーズの例1) 自社のリソースが非常に限られており、リスクの高いものに絞って効果的に対応したい

- リソースが限られていることから、網羅性を犠牲にして効率性を重視し、CVSS 基本値の閾値を 9.0 にする。

ニーズの例2) 自社のリソースが十分にあるため、脆弱性の対応漏れを可能な限りなくすことを重視したい

- リソースが十分にあることから、効率性の低下はある程度許容できる。一方で、対応漏れを減らすために網羅性を重視する。このことから、CVSS 基本値の閾値を 6 にする。

以上を踏まえ、本節では閾値の一例として、どちらかを重視するのではなく両性質のバランスが最もとれる CVSS スコア、EPSS スコアの閾値を調査・検討し、その結果を示す。

2.5.3 CVSS 基本値の閾値決め

はじめに、CVSS 基本値の閾値を検討する。網羅性と効率性のバランスを求めるため、どちらかが大幅に欠けることは避けたい。

そこで、まずは先に掲載した表 2-8 を再度確認する。この表より、CVSS 基本値が 7 の時に網羅性が CVSS 基本値が 8 に比べ大幅に向上し、また効率性も併せて向上していることが分かる。一方で、7 よりも基本値を低いものにした場合、網羅性は向上するが、効率性は低下してしまう。このことから、CVSS 基本値 7 が最も両性質のバランスの取れたものであると考えられる。

表 2-8 各 CVSS 基本値での効率性と網羅性（再掲）

CVSS 基本値	効率性 [%]	網羅性 [%]
10	23.1	7.0
9	23.2	14.5
8	23.1	14.9
7	31.5	53.2
6	29.2	65.9
5	26.1	80.8

さらに、我々は KEV に掲載されている各脆弱性の CVSS 基本値の分布を調査した。その結果を図 2-9 に示す。

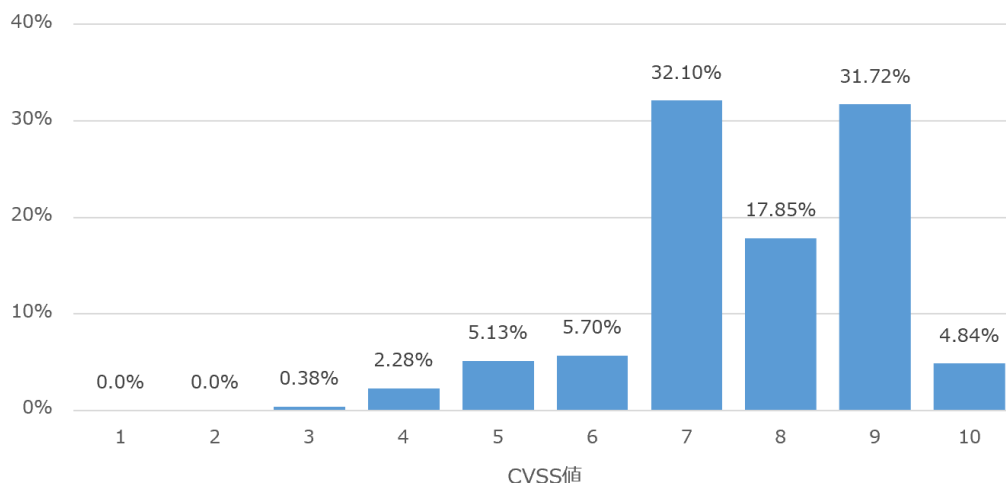


図 2-9 KEV に掲載された脆弱性の CVSS 基本値の分布

図 2-9 の横軸は各脆弱性が該当する CVSS 基本値を、縦軸はその値に属する脆弱性が全体の何割を占めているかの割合を示したものである。この分布より、CVSS 基本値が 7 以上で 6 に比べて急激に脆弱性の数が増えること、そして全体に占める割合の実に 85%以上が 7 以上であることがわかる。すなわち、悪用実績が確認されているとされる KEV に掲載される脆弱性の 8 割以上が、CVSS 基本値が 7 以上の閾値で包括することができるといえる。このことから、CVSS スコア 7 は閾値として適していると考えられる。

また、これは多くの企業が閾値を 7 にすることの根拠としている指標と考えられるが、FIRST では各 CVSS スコアごとの深刻度の分類を表 2-9 のように定義している。

表 2-9 スコアごとの深刻度

深刻度	スコア
緊急	9.0 ~ 10.0
重要	7.0 ~ 8.9
警告	4.0 ~ 6.9
注意	0.1 ~ 3.9
なし	0

CVSS スコア 7.0 は深刻度が「重要」となる閾値でもあるため、これを 1 つの根拠とすることも考えられるだろう。

2.5.4 EPSS の閾値決め

次に、EPSS スコアの閾値を検討する。閾値を検討する前に、まずは1次評価に EPSS を用いる目的を振り返る。それは 2.2.3 節で述べたように、CVSS 基本値のみでは評価できない脅威度を評価し、以下2つの脆弱性を洗い出すことである。

- (ア) 脆弱性の深刻度と脅威度が共に高く、緊急対応を要するもの
- (イ) 脆弱性の深刻度は低い一方で、脅威度が高く、悪用可能性が高いもの

これはすなわち、(ア) では CVSS 基本値が高い脆弱性の中で、さらに対応優先度付けをすることが目的である。CVSS はスコアが 7.0 以上に集中してしまうという特性があるため、その中で対応優先度を CVSS 基本値とは別の指標で判断できることは非常に有益となる。また、(イ) では CVSS 基本値が低い脆弱性の中で、脅威度が高い脆弱性を抽出することが目的である。これら (ア) と (イ) の脆弱性を抽出するための EPSS スコアの設定を検討する。

閾値を設定するために、2023 年 4 月 1 日～2023 年 12 月 30 日の間に CVE-ID が発番された脆弱性に対して、各 EPSS スコアの初期値（各脆弱性に CVE-ID が発番されてから最初に算出された EPSS スコア）を取得した。初期値を用いる主な理由としては、新規脆弱性を評価するのは主にその脆弱性が世に公表されて間もないタイミングであり、そこでの EPSS スコアは概ね初期値に近い値となるからである。なお、脆弱性スキャンツール等を用いて発見された既知の脆弱性に対して1次評価を実施する場合には、後述する 3.5 節で示す閾値を参考いただきたい。これは、既知の脆弱性を評価するタイミングでの EPSS スコアは初期値とは乖離がある可能性が高いためである。

取得した各 EPSS スコアの初期値を用いて、1次評価を実施した際の分布図を図 2-10 に示す。なお、図 2-10 では EPSS 閾値を 0.1%,1%,10%の3パターンで評価を行い、比較のため横並びで示している。

※EPSS はスコア算出のためのモデルの定期的なアップデートが実施されている。モデルの最新版のバージョンアップが 2023 年 3 月 7 日に実施され、それ以前と以降では EPSS スコアに大きな変化が生じる。そのため、本調査では 2023 年 4 月 1 日以降に付番された脆弱性を対象としている。

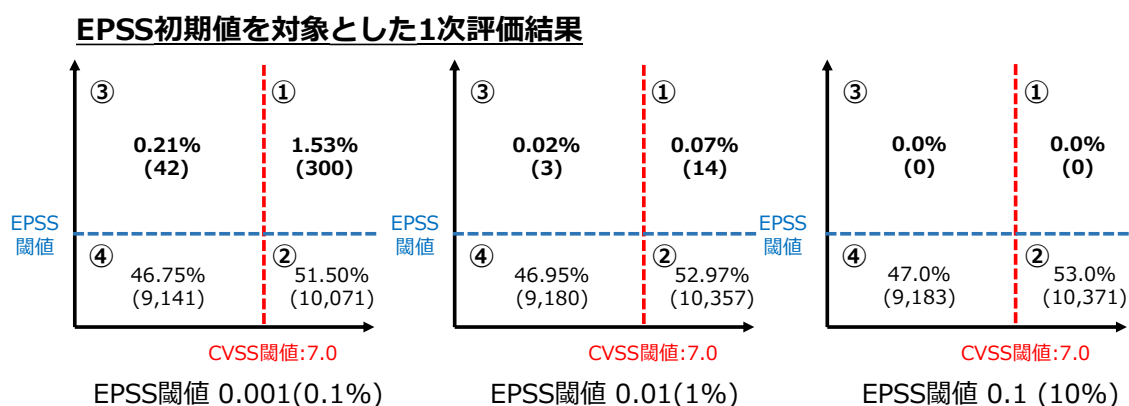


図 2-10 EPSS 分析データ (初期値)

図 2-10 のそれぞれの分布図において、1 次評価結果の優先度① ((ア)の脆弱性に該当) と優先度③ ((ウ)の脆弱性に該当) がどの程度抽出されているかを確認する。

まず、EPSS 閾値が 0.1%の場合、優先度①の脆弱性数が 300 件で全体の 1.53%の数であり、優先度③の脆弱性数が 42 件で全体の 0.21%の数である。次に、EPSS 閾値が 1%の場合、優先度①の脆弱性数が 14 件で全体の 0.07%の数であり、優先度③の脆弱性数が 3 件で全体の 0.02%の数である。最後に、EPSS 閾値が 10%の場合、優先度①・③のともに脆弱性数が 0 件である。これらの分布図から閾値が 10%の時は、優先度①・③の脆弱性を抽出できていないことが分かる。

ここで、閾値が 0.1%と 1%の比較を考える。閾値が 0.1%の場合、優先度①の脆弱性が 300 件あり、これは約 33.3 件/月の計算となる。閾値が 1%の場合、優先度①の脆弱性が 14 件となり、これは約 1.5 件/月の計算となる。

これらより、優先度①の脆弱性について、閾値を 0.1%に設定すると (ア)に該当する脆弱性が閾値を 1%に設定した場合に比べて、運用リソースの負荷が大きくなる。緊急性の高い脆弱性を抽出することは重要な要素ではあるが、月に数十件の緊急対応を実施するのは現実的ではない。以上の結果より、EPSS スコア 0.01(=1%)を閾値に設定することが 1つの案として考えられる。

続いて、設定した閾値(1%)の妥当性を確認するため、実際に 1 次評価を実施した際の結果について、KEV・JPCERT/CC 注意喚起に掲載されている脆弱性を用いて説明する。この理由は、KEV・JPCERT/CC 注意喚起に掲載される脆弱性は脅威度が高い傾向があることから、設定した閾値 (1%)で脅威度が高い脆弱性を抽出できているかある程度確認することが可能なためである。図 2-11 は、2023 年 4 月 1 日～2023 年 12 月 30 日の間に CVE-ID が発番された脆弱性に対して、各 EPSS スコアの初期値を用い、1 次評価を実施した際の分布図である。

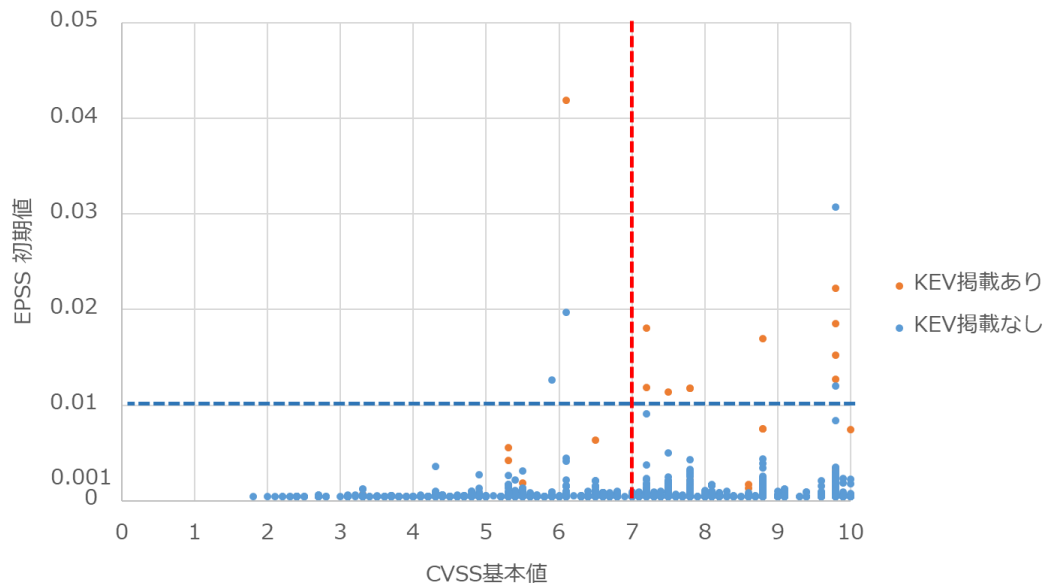


図 2-11 EPSS 初期値を利用した 1 次評価結果

図 2-11 より、EPSS の閾値を 1%に設定した場合、KEV に掲載されている脆弱性のある程度抽出可能であることが分かる。この分布図からわかる通り、CVSS 基本値が 7 以上の中で脅威度の高い脆弱性を抽出するために EPSS を利用するのは有効な 1 つの手段である。

ただし、EPSS スコアの初期値が 1%未満かつ KEV に掲載されている脆弱性も存在する。これは EPSS スコアの初期値が低くなりやすい特性を持つためである。ここで、EPSS スコアの特性を確認するために、JPCERT/CC の注意喚起情報や KEV に掲載されるような脆弱性に対する EPSS スコアの初期値を取得した。実際に以下 2 つの条件でそれぞれの EPSS スコアを取得し、その値を示した分布図を図 2-12、図 2-13 に示す。

- [1] JPCERT/CC の注意喚起情報に掲載された脆弱性の内、CVE-ID が 2023 年 4 月～2023 年 12 月※までに付番された脆弱性
- [2] KEV に掲載された脆弱性の内、CVE-ID が 2023 年 4 月～ 2023 年 12 月※までに付番された脆弱性

※EPSS はスコア算出のためのモデルの定期的なアップデートが実施されている。モデルの最新版のバージョンアップが 2023 年 3 月 7 日に実施され、それ以前と以降では EPSS スコアに大きな変化が生じる。そのため、本調査では 2023 年 4 月 1 日以降に付番された脆弱性を対象としている。

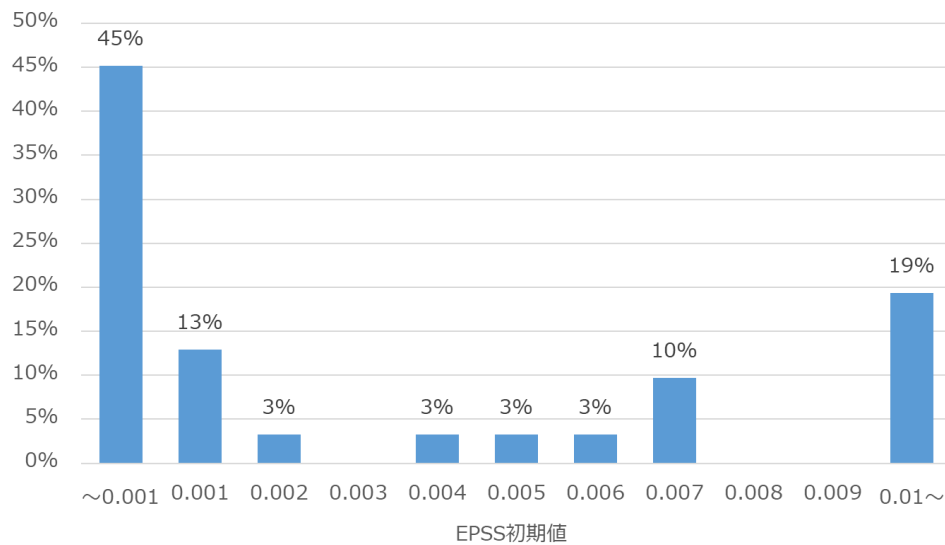


図 2-12 JPCERT/CC 注意喚起情報に掲載された脆弱性の EPSS 初期値の割合

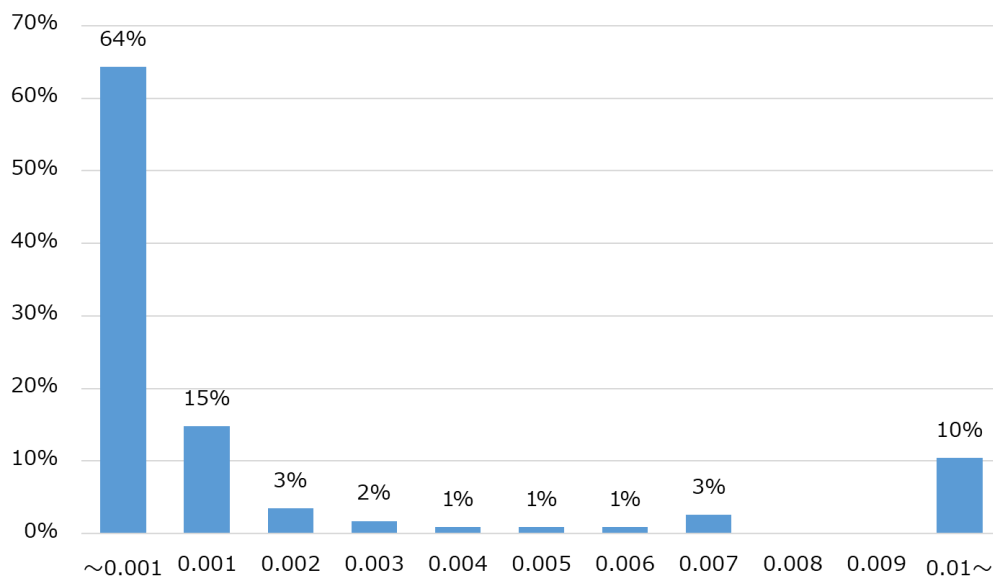


図 2-13 KEV に掲載されている脆弱性の EPSS 初期値の割合

図 2-12 を見ると、EPSS 初期値が 0.001 (=0.1%) 未満の脆弱性の割合が最も多く、EPSS 初期値が 0.01(=1%)以上の脆弱性の割合は全体の 2 割ほどである。図 2-13 についても同様な特徴を示しており、EPSS 初期値が 0.001 (=0.1%) 未満の脆弱性の割合が最も多く、EPSS 初期値が 0.01(=1%)以上の脆弱性の割合は全体の 1 割ほどである。これらのデータより、KEV や JPCERT/CC に掲載されている脆弱性であっても EPSS スコアの初期値は、低くなる傾向であることが分かる。

ここまで EPSS の閾値を 1%に設定する理由を説明したが、自社の各種ニーズによっては網羅性を高めたいといった要望もあるかと考えられるため、そういった場合には閾値をより

低くする（例：0.001(=0.1%)とする）ことも考えられるだろう。ただし、網羅性を求めるあまり閾値を下げすぎた場合、1次評価で(ア)に該当する脆弱性が多くなり、「緊急」の意味が薄れて対応の温度感が下がる恐れもある等の点については注意が必要である。

また、EPSS スコアが 0.01 という非常に低い値に感じるが、実際にはそうではない。EPSS スコアを取得する際に、併せてその値が全体の EPSS スコアの上位何%に位置するのかが示すパーセンタイル (percentile) という値を取得することができる。ここで、EPSS スコアが 0.01 に近い 0.0104 の脆弱性のパーセンタイルを取得したところ、その値は 0.8396（2024/6/2 時点）であった。つまり、EPSS スコアが 0.0104 でも、全体の上位約 84%に位置するスコアであるということである。このことから EPSS スコア 0.01 が十分に高い数値である、ということが分かる。

以上が 1 次評価で利用する EPSS の閾値を 0.01(=1%)とした場合の 1 次評価結果の確認結果である。なお、本節冒頭でも述べた通り本閾値はあくまで我々が検討した結果の一例であるという点に注意が必要がある。実際に 1 次評価を実施する際には、各企業のニーズ等にあわせた検討の上、適切な閾値を設定することを強く推奨する



第3章

運用編

3 運用編

3.1 資産重要度を活用したリスク評価における運用例の概要

2章では、各評価指標を活用したリスク評価の活用例について示した。本章では、2.4節で紹介した資産重要度を活用したリスク評価例について、運用する際に有益なツールや運用上での懸念点について説明する。なお、本章では CVE-ID が発番され、新規に公開された脆弱性に対する運用例を紹介する。

新規の脆弱性に対する対応フローは、図 3-1 のとおりとなる。まず、①公開された脆弱性情報を取得し、自社の資産に関係のある情報かを判断する（3.2 節 脆弱性情報収集）。次に、②資産重要度を活用したリスク評価を実施する。ここで、S ランク判定ならば即時対応となり、A～C ランク判定ならば各判定の期限に沿って逐次対応をしていくことになる（3.3 節 資産重要度を活用したリスク評価）。③即時対応となる S ランク判定以外の A～C ランク判定については、脆弱性に対する緊急度が上昇する可能性があり、一定期間モニタリングしておく必要がある。これは、リスクの3要素の1つ脅威が時間の経過につれ変化すると考えられるためである。このモニタリング期間内で脅威度が上昇した場合には、該当の脆弱性に対する緊急度が上昇したと考えられ、再度リスク評価を実施する（3.4 節 脆弱性情報のモニタリング）。

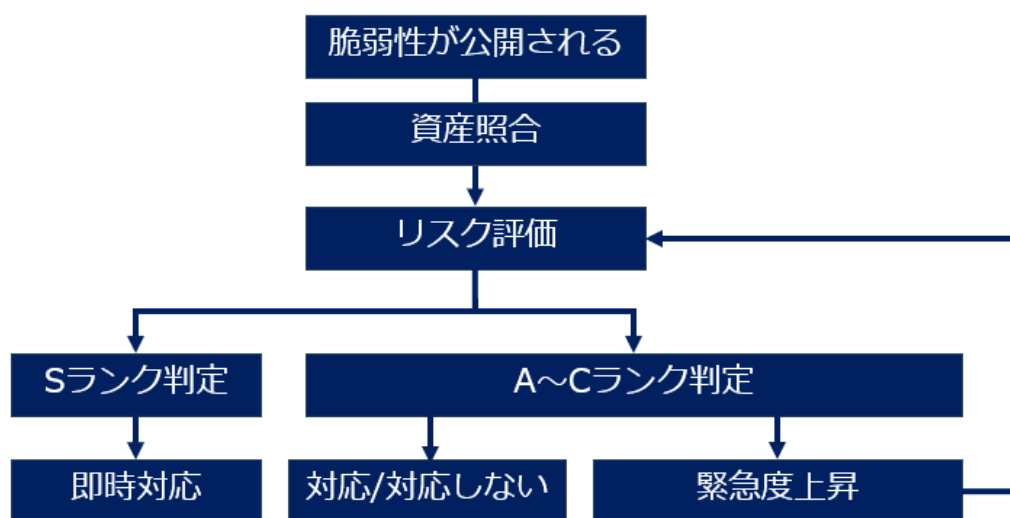


図 3-1 新規の脆弱性に対するリスク評価フロー

3.2 脆弱性情報の収集

脆弱性情報の収集では、脆弱性情報、資産情報と脅威情報を取り扱う。脆弱性対応業務における情報収集は、図 3-2 のとおりである。まず脆弱性情報では、NVD や JVN といった公的機関の脆弱性情報データベースや企業で契約しているベンダから脆弱性情報を収集する。次に自組織の資産情報を活用し、自社資産に照らし合わせて必要な情報のみを収集する。最後に、後工程のリスク評価をスムーズにするために、脆弱性情報を収集する段階で、脅威情報を取得しておく。この脅威情報は、本章の資産重要度を活用したリスク評価では0次評価のみで活用されるが、SSVC や CVSS 環境値を活用する場合には2次評価でも活用される。脅威情報は、脆弱性のリスク評価を実施する際には重要な情報となるため、併せて収集することを推奨する。

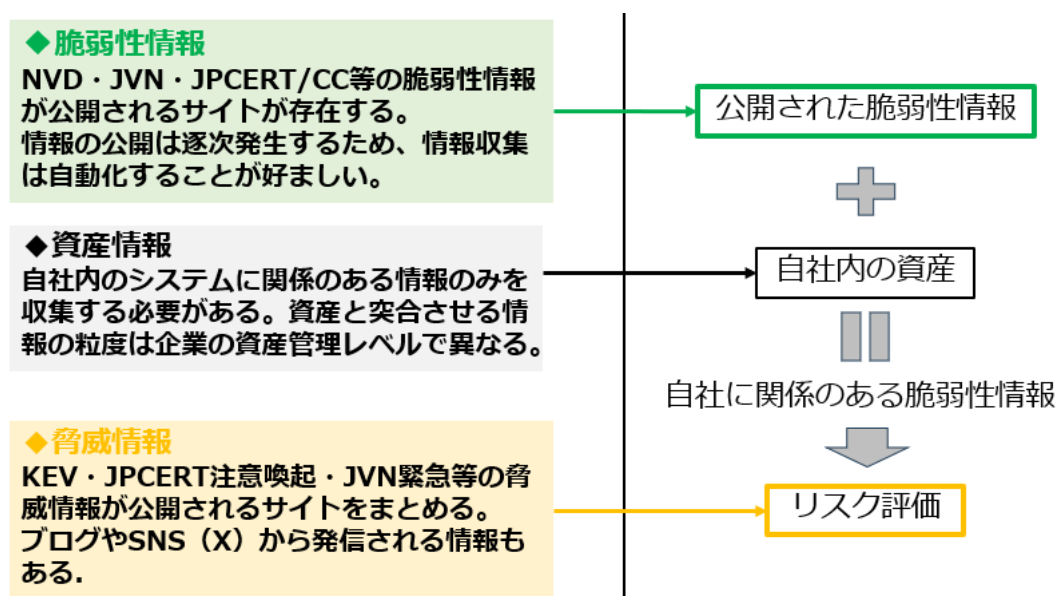


図 3-2 脆弱性対応業務における情報収集

脆弱性情報を収集する際の、収集先のサイトについて紹介する。まず、脆弱性情報を公開しているサイトとして、公的機関・非営利の民間団体として IPA・NVD (NIST)・JVN・JPCERT/CC 等が存在する。これとは別に、各企業が取引先ベンダーと保守契約を結んでいる場合には、ベンダーから脆弱性情報を得られる場合もある。ただ、ソフトウェアのライブラリやオープンソースの脆弱性情報については、ベンダー側から提供されない可能性もあるので、公開サイトから日々脆弱性情報を収集すべきである。また、ソーシャルメディアからも情報収集も可能ではあるが、情報投稿者の投稿頻度がまばらであったり正確な情報であるかの精査が必要なため、活用するには十分な注意が必要である。主要な脆弱性情報収集サイトは、表 3-1 のとおりである。

表 3-1 主要な脆弱性情報収集サイト一覧

サイト名	概要	備考
IPA (https://www.ipa.go.jp/security/security-alert/index.html)	IPA による緊急度が高い注意警戒情報として掲載される脆弱性情報	緊急度が高い脆弱性情報のみが掲載されるので全ての脆弱性情報が掲載されない。
JPCERT/CC (WeeklyReport) (https://www.jpcert.or.jp/wr/)	JPCERT/CC による 1 週間分の重要度が高いとして掲載される脆弱性情報	重要度が高い脆弱性情報のみが掲載されるので全ての脆弱性情報が掲載されない。
JPCERT/CC (注意喚起) (https://www.jpcert.or.jp/at/)	JPCERT/CC による深刻且つ影響範囲の広い脆弱性などに関する情報として掲載される脆弱性情報	緊急度が高い脆弱性情報のみが掲載されるので全ての脆弱性情報が掲載されない。
NVD (https://nvd.nist.gov/vuln)	米国立標準技術研究所 (NIST) が運営する脆弱性情報が管理されているデータベース	CVE-ID が発番された脆弱性情報が基本的に掲載される。脆弱性情報に加えて、CVSS 基本値や KEV の情報も掲載される。API で情報の自動収集が可能。
JVN (https://jvn.jp/)	JPCERT/CC と IPA が共同で運営している国内の脆弱性対策情報ポータルサイト	NVD から公開された脆弱性情報が掲載される。JVN iPedia の脆弱性情報データベースが用意されており、API で情報の自動収集が可能。

次に、脆弱性情報を収集した際、自社資産に関係があるか確認する必要がある。この作業は運用リソースが大きいため、自動で情報を抽出するかベンダーから情報を直接提供されることが好ましい。自動で情報を抽出する場合には、企業の資産管理レベルによるが、以下の3パターンが考えられる。

① ベンダー名で情報を企業内資産と突合させる

企業内で利用している製品のベンダー名単位で脆弱性情報を収集する。この場合、資産管理レベルが高くなくても、ある程度の脆弱性情報を自社資産と照らし合わせることが可能である。ただ、粒度が大きいため、企業の資産とは関係のない情報まで収集してしまう場合が発生する。

② 製品名で情報を企業内資産と突合させる

企業内で利用している製品単位で脆弱性情報を収集する。この場合、製品単位で脆弱性情報を収集するので、ベンダー名で情報を収集する場合よりも収集する脆弱性情報を削減することが可能である。

③ CPE (Common Platform Enumeration) で情報を企業内資産と突合させる

製品を識別するためのフォーマットには CPE 以外にも SWID (Software Identification) 等が存在するが、ここでは普及率の高い CPE を取り上げることとする。なお、NVD は現在 SWID の採用を推進しており、今後 SWID の活用も視野に入れることが推奨される。

企業内で利用している CPE 単位で脆弱性情報を収集する。この場合、ソフトウェアのバージョンまで脆弱性情報と突合させるため、ほぼ必要な脆弱性情報のみを収集可能である。ただ、企業内資産が CPE 単位で管理されている必要があり、非常に高い資産管理レベルが求められる。また脆弱性情報サイト側でも CPE 単位で情報展開されている必要があるため、実運用するまでのハードルは非常に高い。

参考：CPE の概要

共通プラットフォーム一覧：CPE（Common Platform Enumeration）は、情報システムを構成する、ハードウェア、ソフトウェアなどを識別するための共通の名称基準を目指したものである^[10]。CPE の活用により、脆弱性が影響を与える製品の識別が容易になることが期待できる。

以下に CPE 名の基本構成について簡単に説明する。

■ CPE 名の基本構成

cpe：/{種別}:{ベンダ名}:{製品名}:{バージョン}:{アップデート}:{エディション}:{言語}

※大文字と小文字の区別はない

※基本構成のそれぞれの箇所が空白の場合、「全て」を意味します。例えばバージョンが空白の場合、全てのバージョンを意味する

1. 種別

製品種別（ハードウェア,OS,アプリケーション）を判別する情報として,h=ハードウェア,o=OS,a=アプリケーションを記述する。

2. ベンダ名

ドメイン名を利用してベンダ名を作成し、記述する。

3. 製品名

製品名を記述する。複数の単語で構成されている製品名の場合、スペースをアンダースコア(_)に置き換えた名前を記述する。

4. バージョン

製品のバージョン情報を記述する。

5. アップデート

製品のアップデートやサービスパックの情報を記述する。バージョンとアップデートの違いは、ベンダや製品が出す情報に依存する。

6. エディション

製品のエディションを記述する。エディションとはソフトウェア等の提供方法等（例：プロフェッショナル版、無償版）を示す。

7. 言語

製品で使用している言語を特定したい場合に記述する。この項目の表記には、言語識別のための IETF RFC 4646(*7)のタグを利用する。

その他の詳細な記述例については、参考文献[10]IPA のサイトを参照いただきたい。

3.3 資産重要度を活用したリスク評価

本書では、リスク評価として資産重要度を活用したリスク評価例を紹介した。リスク評価の実施方法については、2.4 節のとおりである。ここでは、資産重要度の設定基準例と各評価指標の値を取得する方法およびツールについて紹介する。

3.3.1 資産重要度の設定基準例

2.4.3 節で説明したようにリスク評価を実施する事前準備として、あらかじめ資産重要度設定を実施する必要がある。しかし、全ての資産に対して一斉に資産重要度を設定することは、運用負荷が高いため現実的ではない。そこで、狙われやすく重要資産となる可能性が高い、アタックサーフェスの近くから資産重要度を設定することを推奨する。また、セキュリティ関連部門で資産重要度を設定することが困難である場合には、関連部署と連携して設定することを推奨する。資産重要度を設定する際の基準例は表 2-7、表 2-8、表 2-9 のとおり。

3.3.2 各評価指標の活用例

資産重要度を活用したリスク評価手法では、評価指標として CVSS 基本値と EPSS を活用する。本節では、CVSS 基本値と EPSS スコアを取得する方法を紹介する。各評価指標は 1 次評価で活用されるため、可能な限り運用リソースを割かずに値を取得することが望ましい。そこで、自動化を意識した値取得方法について説明する。なお、値を取得する際の脆弱性の例として、CVE-2021-44228（Apache Log4j の脆弱性）を利用する。

➤ CVSS 基本値

CVSS 基本値は、公的機関やベンダーにて値が算出される。本書では、NVD を活用して CVSS 基本値を取得する方法について説明する。まず、手動で CVSS 基本値を確認する方法として、NVD の脆弱性 DB のサイト (<https://nvd.nist.gov/vuln/search>) から、過去 3 か月以内の選択項目を選択し、新規の脆弱性情報を確認する。図 3-3 は NVD の脆弱性 DB 検索サイトの画面である。この中の「Search Type」を「Last 3 Months」を選択し、「Search」を押下する。

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions. Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

図 3-3 NVD の脆弱性 DB 検索サイト

図 3-4 は、脆弱性 DB 検索サイトで検索された脆弱性情報の画面である。ページ内の Severity に CVSS 基本値の値が表示されている。今回の例では、CVSS 基本値は 10.0 であることが分かる。

図 3-4 NVD の CVSS 基本値

次に、API を活用して自動で CVSS 基本値を取得する場合について説明する。NVD の API 活用方法は、API の解説サイト (<https://nvd.nist.gov/developers/vulnerabilities>) にも説明があるように多岐にわたる。

脆弱性情報収集時に取得した CVE-ID を API パラメータとして活用することで、該当する CVE-ID の脆弱性情報が取得可能である。CVE-2021-44228 に対する API の例は、図 3-5 のとおりである。

```
https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2021-44228
```

図 3-5 NVD の API 例

API 出力結果は図 3-6 のようになり、CVSS v3.1 基本値を取得することが可能である。この表示結果内の"baseScore"が CVSS 基本値であり、今回の例では CVSS 基本値は 10.0 であることが分かる。

```
{
  "source": "nvd@nist.gov",
  "type": "Primary",
  "cvssData": {
    "version": "3.1",
    "vectorString":
"CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
    "attackVector": "NETWORK",
    "attackComplexity": "LOW",
    "privilegesRequired": "NONE",
    "userInteraction": "NONE",
    "scope": "CHANGED",
    "confidentialityImpact": "HIGH",
    "integrityImpact": "HIGH",
    "availabilityImpact": "HIGH",
    "baseScore": 10,
    "baseSeverity": "CRITICAL"
  },
  "exploitabilityScore": 3.9,
  "impactScore": 6
}
```

図 3-6 NVD の API 出力結果（一部抜粋）

➤ EPSS スコア

EPSS は FIRST が運営しており、EPSS のサイトから API を活用することで EPSS スコアを取得可能である。EPSS スコアは日ごとに変動するスコアとなるが、本例では取得したタイミングのスコアを活用するものとする。EPSS の API 活用方法は、EPSS サイト (<https://www.first.org/epss/api>) に記載がある。このサイトに従って、脆弱性情報収集で取得した CVE-ID に対する EPSS スコアを取得する。図 3-7 は、CVE-2021-44228 の EPSS スコアを取得する際の API の例である。

```
https://api.first.org/data/v1/epss?cve= CVE-2021-44228
```

図 3-7 EPSS の API 例

EPSS の API 出力結果は、図 3-8 とおりである。"epss": "0.975600000"が EPSS スコアであり、この場合は EPSS スコアは 97.56%となる。また、"percentile": "0.999980000"は EPSS のパーセンタイルであり、この場合は EPSS に登録されている脆弱性の上位 99.998%に位置す

ることになる。これより CVE-2021-44228 は、脆弱性の中でも脅威度が非常に高いものであることが分かる。

```
{
  "status": "OK",
  "status-code": 200,
  "version": "1.0",
  "access": "public",
  "total": 1,
  "offset": 0,
  "limit": 100,
  "data": [
    {
      "cve": "CVE-2021-44228",
      "epss": "0.975600000",
      "percentile": "0.999980000",
      "date": "2024-05-22"
    }
  ]
}
```

図 3-8 EPSS の API 出力結果

➤ CVSS 基本値+EPSS スコア

ここでは、脆弱性のリスク評価において有益な情報を自動取得可能なツールである CVE_Prioritizer (https://github.com/TURROKS/CVE_Prioritizer) について紹介する。このツールでは脆弱性情報収集時に取得した CVE 番号に対して、EPSS スコア・CVSS 基本値・KEV 等に関する情報を取得可能である。また、リスク評価例の 1 次評価と同様に EPSS スコアと CVSS 基本値の設定した閾値から脆弱性の優先度を自動で分類することも可能である。これらの閾値はコマンド上で指定でき、組織で設定した閾値ごとに優先度を出力できる。

CVE_Prioritizer の出力例は図 3-9 のとおり。この例では、`-c` コマンドで CVE 番号と、`-v` コマンドを入力することによって EPSS スコア、CVSS 基本値、KEV、優先度に関する詳細情報が出力される。`-v` コマンドを入力してない場合は、該当 CVE に対する優先度のみが出力される。

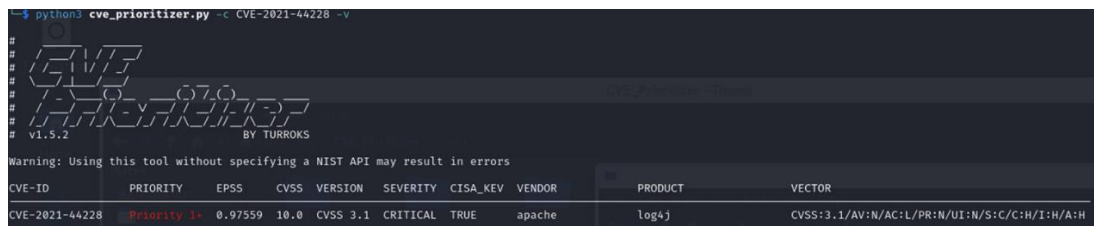


図 3-9 CVE_Prioritizer の活用例

これらのツール等を活用し、CVSS 基本値と EPSS スコアを取得して 1 次評価を実施する。その後、資産重要度との組み合わせより対応ランクの判定を実施する。各脆弱性に対する対応ランクの判定は S~C となる。この各対応ランクに対する対応期限例は、表 3-2 のとおりである。対応期限としては、暫定対処期限と本格対処期限でそれぞれ期限を設定している。暫定対処は、恒久的な対策であるパッチ適用等を実施するのが困難な場合において、アクセス制限や該当機能の無効化等の暫定的な緩和策や回避策を実施することを意味している。本格対処としては、該当ソフトウェアのアップデートやパッチ適用を実施し、脆弱性そのものを排除する恒久的な対策を実施することを意味している。

表 3-2 対応優先度ごとの対処期限目安の例

評価	説明	暫定対処期限	本格対処期限
S	脆弱性の深刻度、悪用可能性の両方が高く、緊急の対応を要する脆弱性。	即日~3 日以内	7 日以内
A	悪用可能性が低い、攻撃難易度が高い等の理由から緊急対応の必要性はないが、悪用された際の影響が大きいため優先的に対応が望ましい脆弱性。	30 日以内	45 日以内
B	緊急の対応は不要であるが、将来的には対応が望ましい脆弱性。ただし、費用対効果や資産状況に応じてリスク受容することも考えられる。	定期メンテナンス実施時	定期メンテナンス実施時
C	脆弱性の深刻度、悪用可能性の両方が低く、リスク受容が妥当と思われる脆弱性。	対処しない	対処しない

3.4 脆弱性情報のモニタリング

本節では、リスク評価され各脆弱性に対する対応ランクが定まった後の継続モニタリングに関する説明をする。ここでSランク判定の脆弱性については、即時対応となるため継続モニタリングは必要がない。A～Cランク判定の脆弱性については、対応を実施するまでに脅威が変動する可能性があるため、継続モニタリングする必要がある。ここで、継続モニタリングする必要がある情報は、リスクの3要素の内の脅威に対する情報である。これはリスクの3要素の中で、時間で変化するのは、基本的には脅威に関する情報のみだからである。つまり、リスク評価はあくまでも評価したタイミングのみのリスクを評価していることになり、リスク評価したタイミングではリスクは小さいと判断されたが、リスク評価した後に悪用実績や攻撃コードが公開された場合にはリスクが大きくなる可能性が高いといえる。このように脅威が上昇した脆弱性に対しては再度リスク評価を実施する必要がある。

脅威情報をモニタリングする方法の例として、①KEV や JPCERT/CC の注意喚起情報を確認 ②EPSS スコア上昇を把握 ③ニュースメディアやソーシャルメディアの確認 ④脅威インテリジェンスサービスの活用 の4種類が挙げられる。これらの方法を活用し、時間的に変化する脅威情報をリアルタイムで取得する必要がある。ここで、①と②については専門知識を有さない方法となり、③と④については専門知識を有する方法と分類可能である。それぞれの対応方法について説明する。

➤ 専門知識を有さない対応方法

KEV や JPCERT/CC 注意喚起情報の確認および EPSS スコア上昇を把握では、企業内で基準を定めておけば、対応が一意に定まる属人化しない対応方法である。

① KEV や JPCERT/CC 注意喚起情報の確認

- KEV の情報取得

KEV ではカタログに掲載されている情報を CSV または json 形式で出力可能である。この情報を定期的に取得することで、脅威度を確認することが可能である。また、サブスクライブを登録しておくことで、KEV 情報が公開された際に通知を受け取ることが可能である。

(https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?topic_id=USDHSCISA_136)

- JPCERT/CC の注意喚起情報の取得

JPCERT/CC の注意喚起のサイトは、緊急度が高い警戒情報情報を提供している。このサイトは RSS (Rich Site Summary) があるため、サイト更新時に情報を自動収集可能である。

② EPSS スコア上昇を把握

EPSS スコアを監視しておくことで、脆弱性の脅威度が上昇したかを把握可能となる。これは、EPSS スコアが設定した閾値を超えたかどうかを確認する。(Appendix D 節参照) 例として、4 週間程度の期間を脆弱性情報が公開されてから観測しておく。また、観測期間を過ぎた脆弱性情報については、CVEdetails (Appendix A 節参照) を活用することで EPSS スコアが上昇した脆弱性を確認することが可能である。

➤ 専門知識を有する対応方法

ニュースメディアやソーシャルメディアの確認や脅威インテリジェンスサービスの活用では、セキュリティ専門知識が必要となるため属人化しやすい対応方法となる。本書では、専門知識を有する対応方法についての詳細は、脆弱性や企業の業界によって対応が異なるため説明は省く。脅威インテリジェンスサービスの活用方法については、ICSCoE7 期の別プロジェクトである「脅威インテリジェンス導入・運用ガイドライン作成」を確認する。

3.5 EPSS スコアのモニタリング及び既知脆弱性評価時の EPSS 閾値

本節では EPSS スコアをモニタリングし、スコアの変化に応じて 1 次評価を繰り返し実施（モニタリング）することの重要性と、モニタリング 及び 既知脆弱性の評価時に利用する EPSS の閾値について説明する。

3.5.1 モニタリングの必要性

モニタリングの必要性は本編の 3.4 節で説明した通り、リスクの 3 要素の内、脅威に関する情報が時間と共に変化するためである。リスク評価はあくまでも評価したタイミングのみのリスクを評価していることになり、リスク評価を行ったタイミングではリスクは小さいと判断されたが、リスク評価した後に悪用実績や攻撃コードが公開された場合にはリスクが大きくなる可能性が高いといえる。このように脅威が上昇した脆弱性に対しては再度リスク評価を実施する必要がある。

本書の 1 次評価手法では脅威レベルを EPSS スコアを利用して評価している。2.5 節で説明した通り、新規の脆弱性に対する 1 次評価では EPSS スコアの初期値を利用しているが、EPSS スコアは一般に初期値を最小値として、時間変化による脅威レベルの更新により上昇していく傾向がある。よって、EPSS スコアの時間変化をモニタリングすることで、変化する脆弱性の脅威に対応したリスク評価が可能となる。

3.5.2 既知脆弱性の評価

本書における各リスク評価手法は、主に日々公開される新規の脆弱性に着目して検討・調査したものを記載したが、これらのリスク評価手法は脆弱性スキャンツール等を用いて発見された既知脆弱性に対しても活用することできる。ただし、各手法における 1 次評価で用いる EPSS の閾値については、新規脆弱性対応時のものとは別の値を利用することを推奨する。それは、既知脆弱性は CVE-ID が付番、つまり世に公表されてから一定程度の時間が経過しており、EPSS のスコアが初期値よりも上昇している可能性が高いからである。

3.5.3 モニタリング 及び 既知脆弱性用の EPSS スコアの閾値

前述した通り、モニタリング 及び 既知脆弱性の対処時では EPSS スコアの上昇を考慮した評価が必要である。よって、閾値の検討には、EPSS スコアの初期値ではなく時点（2024/4/30 時点）での最大値を利用することとする。

次に、EPSS スコアの閾値を検討する。閾値の検討プロセスについては、2.5.4 節と同様、CVSS 基本値と EPSS スコアの分布図を利用する。閾値を検討する前に、まずは 1 次評価に EPSS を用いる目的を振り返る。それは 2.2.3 節で述べたように、CVSS 基本値のみでは評価できない脅威度を評価し、以下 2 つの脆弱性を洗い出すことである。

(ア) 脆弱性の深刻度と脅威度が共に高く、緊急対応を要するもの

(イ) 脆弱性の深刻度は低い一方で、脅威度が高く、悪用可能性が高いもの

これは要するに、(ア) では CVSS 基本値が高い脆弱性の中で、対応優先度付けをすることが目的である。CVSS はスコアが 7.0 以上に集中してしまうという特性があるため、その中で対応優先度を CVSS 基本値とは別の指標で判断できるのは非常に有益となる。また、(イ) では CVSS 基本値が低い脆弱性の中で、脅威度が高い脆弱性を抽出することが目的である。これら (ア) と (イ) の脆弱性を抽出するための EPSS スコアの設定を検討する。

閾値を設定するために、2023 年 4 月 1 日～2023 年 12 月 30 日の間に CVE-ID が発番された脆弱性に対して、各 EPSS スコアの最大値（各脆弱性に CVE-ID が発番されてから 2024 年 4 月 30 日までの EPSS スコアの中での最大値）を取得した。各 EPSS スコアの最大値を用いて、1 次評価を実施した際の分布図を図 3-10 に示す。図 3-10 は、取得したデータに対して EPSS 閾値を 1%,10%,20%とした際の分布図である。

図 3-10 のそれぞれの分布図において、1 次評価結果の優先度①（(ア)の脆弱性に該当）と優先度③（(ウ)の脆弱性に該当）を上手く抽出されているか確認する。

まず、EPSS 閾値が 1%の場合、優先度①の脆弱性数が 467 件で全体の 2.4%の数であり、優先度③の脆弱性数が 66 件で全体の 0.3%の数である。次に、EPSS 閾値が 10%の場合、優先度①の脆弱性数が 194 件で全体の 1.0%の数であり、優先度③の脆弱性数が 17 件で全体の 0.1%の数である。最後に、EPSS 閾値が 20%の場合、優先度①の脆弱性の数が 162 件で全体の 0.8%の数であり、優先度③の脆弱性数が 12 件で全体の 0.1%の数である。

これらの分布図から、初期値を用いた 1 次評価での EPSS 閾値（0.01(=1%)）以上のどの閾値を設定しても優先度①・③の脆弱性を抽出できるということが分かる。ここで、優先度①の脆弱性の数に着目する。閾値が 1%の場合、優先度①の脆弱性は 467 件であり、これは 51 件/月の計算となる。次に、閾値が 10%の場合、優先度①の脆弱性は 197 件であり、これは 21 件/月の計算となる。最後に、閾値が 20%の場合、優先度①の脆弱性数は 162 件であり、これは 18 件/月の計算となる。この結果から、閾値が 10%を下回ると、月の運用リソースの負荷が著しく増加する傾向があることが分かる。また、閾値が 1%の場合の対応件数は 51 件/月であり 10%未満の閾値を採用することは運用リソースの負荷の観点から現実的ではない。続いて、閾値 10%と 20%の場合数を比較すると①・③の数の変化は小さいことが分かる。EPSS の最大値は初期値と比べて脅威度を正しく反映することができるため、月数件の運用負荷の差しかないのであれば、より網羅的に①・③の脆弱性を抽出することが望ましい。よってこの場合、EPSS10%が EPSS 閾値の 1 つの案として考えられる。

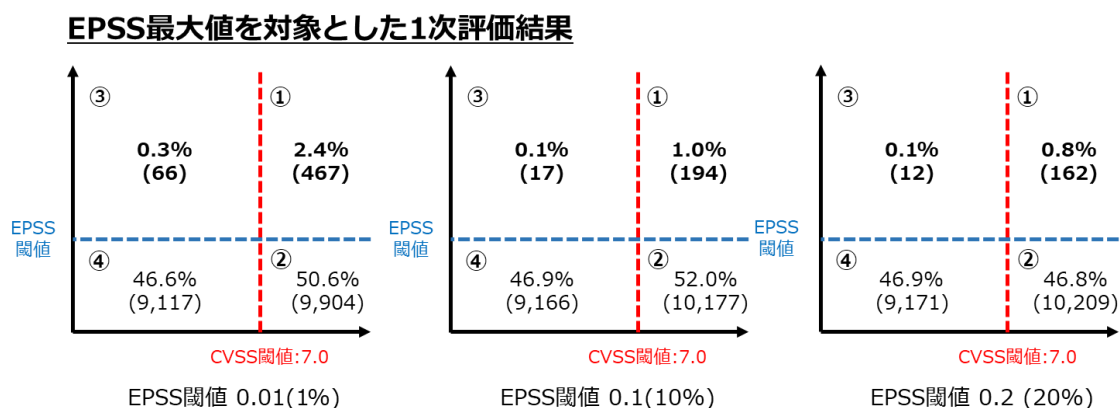


図 3-10 EPSS 分析データ（最大値）

続いて、設定した閾値(10%)の妥当性を確認するため、1次評価を実施した際の結果について、KVE に掲載されている脆弱性を用いて説明する。この理由は、KEV・JPCERT/CC 注意喚起に掲載される脆弱性は脅威度が高い傾向があることから、設定した閾値（10%）で脅威度が高い脆弱性を抽出できているかある程度確認することが可能なためである。図 3-11 は、2023 年 4 月 1 日～2023 年 12 月 30 日の間に CVE-ID が発番された脆弱性に対して、各 EPSS スコアの最大値を用い、1 次評価を実施した際の分布図である。

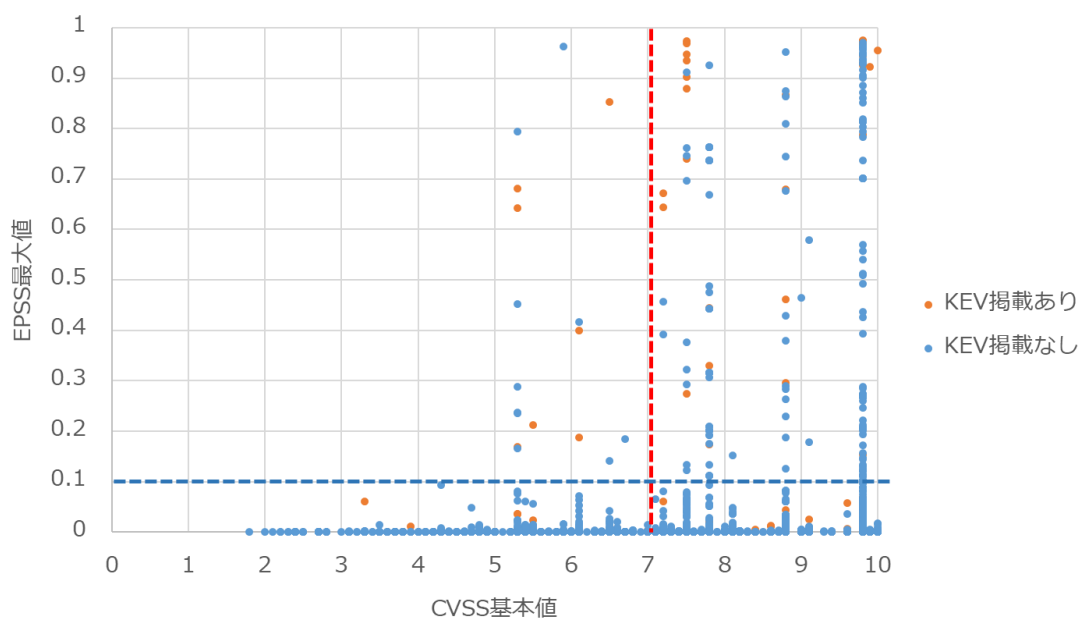


図 3-11 EPSS 最大値を利用した 1 次評価結果

図 3-11 より、EPSS の閾値を 10%に設定した場合、KEV に掲載されている脆弱性がある程度抽出可能であることが分かる。この分布図からわかる通り、CVSS 基本値が 7 以上の中で脅威度の高い脆弱性を抽出するために EPSS を利用するのは有効な 1 つの手段である。た

だ、EPSS スコアの初期値が 10%未満で KEV に掲載されている脆弱性も存在する。これは、悪用が確認された脆弱性の EPSS が必ず高くなるわけではないという EPSS の特徴に起因するものであると考えられる。ここで、EPSS スコアの特性を確認するために、JPCERT/CC の注意喚起情報や KEV に掲載されるような脆弱性に対する EPSS スコアの最大値を取得した。実際に以下 2 つの条件でそれぞれの EPSS スコアを取得し、その値を示した分布図を図 3-12、図 3-13 に示す。

[1] JPCERT/CC の注意喚起情報に掲載された脆弱性の内、CVE-ID が 2023 年 4 月～2023 年 12 月※までに付番された脆弱性

[2] KEV に掲載された脆弱性の内、CVE-ID が 2023 年 4 月～2023 年 12 月※までに付番された脆弱性

※EPSS はスコア算出のためのモデルの定期的なアップデートが実施されている。モデルの最新版のバージョンアップが 2023 年 3 月 7 日に実施され、それ以前と以降では EPSS スコアに大きな変化が生じる。そのため、本調査では 2023 年 4 月 1 日以降に付番された脆弱性を対象としている。

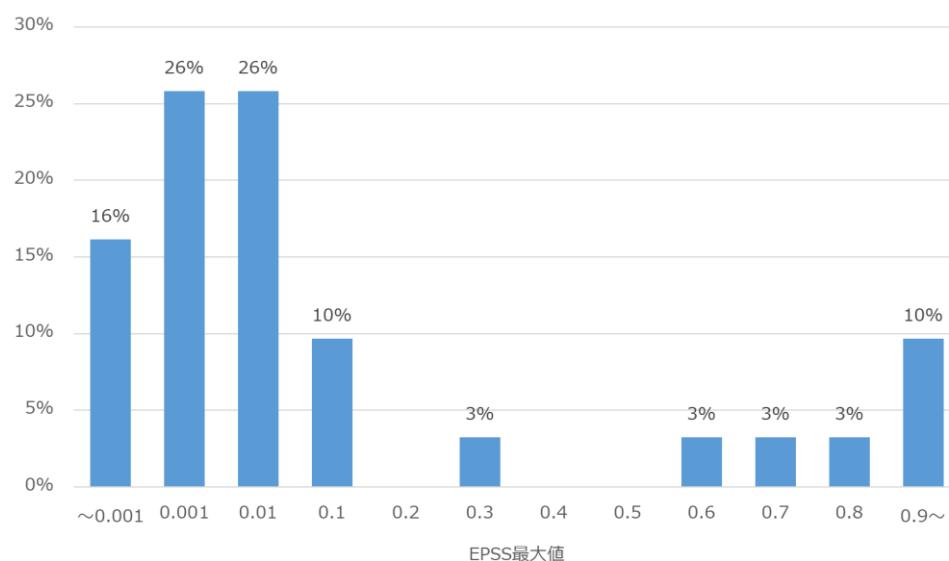


図 3-12 JPCERT/CC 注意喚起情報に掲載された脆弱性の EPSS 最大値の割合

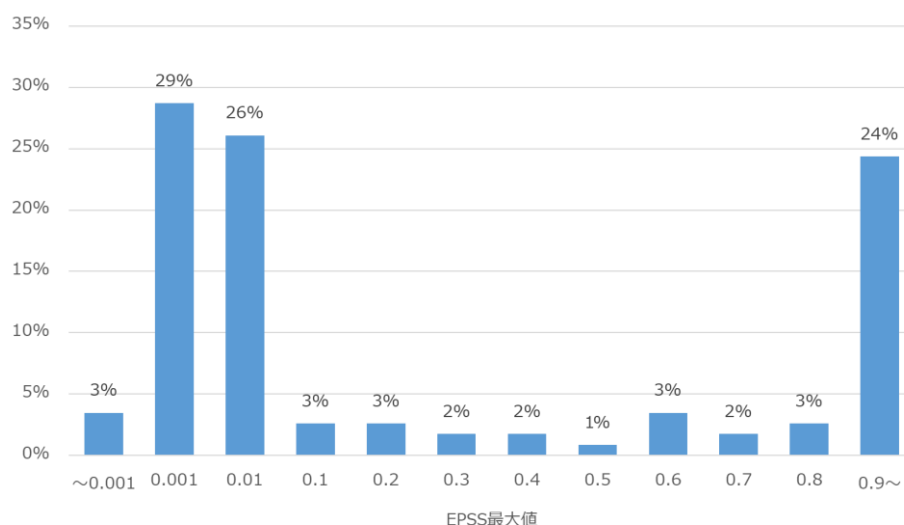


図 3-13 KEV に掲載された脆弱性の EPSS 最大値の割合

図 3-12 を見ると、EPSS 最大値が 0.1 (=10%) 未満の脆弱性の割合が約 7 割を占めており、EPSS 最大値が 0.1(=10%)以上の脆弱性の割合は全体の 3 割ほどである。図 3-13 についても同様な特徴を示しており、EPSS 最大値が 0.1 (=10%) 未満の脆弱性の割合が最も多く、EPSS 最大値が 0.1(=10%)以上の脆弱性の割合は全体の 4 割ほどである。これらのデータより、KEV や JPCERT/CC に掲載されている脆弱性であっても EPSS スコアの最大値は、必ずしも高くなることはないということが分かる。

ここまで、EPSS の閾値を 10%に設定する理由を説明したが、自社の各種ニーズによっては網羅性を高めたいといった要望もあるかと考えられるため、そういった場合には閾値をより低くする（例：0.01(=1%)とする）ことも考えられるだろう。ただし、網羅性を求めるあまり閾値を下げすぎた場合、1 次評価で(ア)に該当する脆弱性が多くなり、「緊急」の意味が薄れて対応の温度感が下がる恐れもある等の点については注意が必要である。

以上が、脆弱性のモニタリングで 1 次評価を利用することを想定した際に、EPSS 閾値を 0.1(=10%)とした場合の 1 次評価の確認結果である。なお、本節冒頭でも述べた通り本閾値はあくまで我々が検討した結果の一例であるという点に注意が必要がある。実際に脆弱性のモニタリング及び既知の脆弱性の評価のために 1 次評価を実施する際には、各企業のニーズ等にあわせた検討の上、適切な閾値を設定することを強く推奨する。

3.6 運用上の懸念点

ここまで脆弱性対応の運用例について紹介した。本節ではこの運用時の各懸念点について説明する。

まず、脆弱性のリスク評価においては、資産管理が適切にされていることが前提となる点である。リスク評価例で紹介したとおり、自社環境に照らし合わせた適切なリスク評価を実施するには資産管理が十分である必要がある。本来は全ての資産に対して適切に資産管理されているのが好ましいが、最低限として攻撃される可能性が高いアタックサーフェスの近くの資産に対する資産管理のみでも実施しておくべきである。本書の内容を理解することで、脆弱性対応のためには資産管理としてどのような情報が必要か、今一度認識されれば幸いである。次に、膨大な脆弱性情報を手動で管理するのが困難である点である。日々公開される脆弱性情報に対するリスク評価での判断結果や対応状況を把握することは、情報量が多く管理が乱雑になる。これに対して、脆弱性管理ツールを活用することで、これらを素早く把握することが出来るようになる。このように膨大な脆弱性情報に対して、手動管理することは運用負荷が高いため、チケット管理ツールを活用することを推奨する。最後に、脅威情報の収集が困難な点である。EPSS や KEV は属人化せずに脅威情報を取得可能であるが、十分な脅威情報を取得できない。EPSS は閾値の設定に対する明確なガイドラインが存在しておらず、各組織での閾値設定が困難である。また、KEV は全ての脆弱性の悪用実績が掲載されるわけではなく、脅威情報としては取りこぼしが発生する恐れがある。脅威インテリジェンスサービスを活用する方法も存在するが、導入後の活用方法のハードルが高く、組織として高いセキュリティ成熟度が求められる



第4章

まとめ

4 まとめ

本書では、一般的に広く利用されている CVSS v3.1 基本値とこれ以外の各評価指標について紹介した。また、これらの評価指標を活用したリスク評価の例やリスク評価の運用例について解説した。

年々公開される脆弱性情報の数は増加傾向にあり、これらの脆弱性情報に対して効率的かつ適切にリスク評価を実施することが必要不可欠となっている。現状、一般的に広く活用されている評価指標の CVSS v3.1 基本値では、脆弱性に対する脅威動向や自社の環境に照らし合わせたリスク評価が実施できない。これらの評価しきれていないリスクに対して、CVSS v3.1 基本値以外の評価指標の特性・役割を理解することで、適切なリスク評価が可能となる。

また、リスクを脅威・脆弱性・資産の3要素に分類し、各評価指標がどの要素を評価可能であるかを確認した。この3要素を考慮することで、各脆弱性に対して適切にリスク評価が可能となる。

各リスク評価の例では、SSVC、CVSS 環境値、資産重要度を活用した3種類の評価指標の活用例を紹介した。リスク評価において、リスクの高い脆弱性を発見することが目的の1つではあるが、これとは別に対応する必要がない脆弱性を発見することも目的としている。これは膨大な脆弱性情報に対して、対応する脆弱性の取捨選択をするのもリスク評価の目的であるためである。

これに対して、リスク評価を1次・2次評価に分類し、1次評価においてはリスクの脅威と脆弱性に対しての簡易評価を実施した。これにより、対応する必要がない脆弱性を洗い出すことが可能である。

また、2次評価においては、自社環境に照らし合わせた評価を実施することで自社にとってリスクの高い脆弱性を洗い出している。SSVC、CVSS 環境値を活用したリスク評価では、リスクの3要素を加味したリスク評価が実施可能であることを説明した。ただし、脅威情報の取集といった専門的知識を必要とすることによる属人化であったり、運用リソースが大きくなるといった課題もあり、セキュリティ業務に余裕のある企業のみが運用可能なリスク評価手法となっている。資産重要度を活用したリスク評価においては、SSVC、CVSS 環境値を活用したリスク評価の課題である、属人化および運用リソース増大を解決している。しかし、資産重要度を企業内の全ての資産に対して実施することは困難であるため、実際にはアタックサーフェスの近くの資産から資産重要度を設定し、それ以外の資産については従来通り CVSS 基本値や EPSS を活用したリスク評価を実施していくのが現実的である。

最後に、本書が自組織の脆弱性情報に対するリスク評価の助けになれば幸いである。



Generated by DALL·E 2, an OpenAI service

Appendix

Appendix

A) CVSS v3.1 の詳細説明

本節では、CVSS v3.1 の評価の基準について説明する。CVSS v3.1 では脆弱性の深刻度レベルを「緊急」/「重要」/「警告」/「注意」の4つに分類している。これはあくまで深刻度の段階を表すものであり、意思決定のための情報を提供するものではないことを留意すべきである。つまりは、CVSS v3.1 を利用する意思決定者は、各レベルに対して自ら方針を策定する必要がある。各深刻度に対する CVSS の値は表 A-1 のとおり。

表 A-1 CVSS の値に対する重大性

重大性	評価値
緊急 Critical	9.0 ~ 10.0
重要 High	7.0 ~ 8.9
警告 Medium	4.0 ~ 6.9
注意 Low	0.1 ~ 3.9
なし	None (0)

➤ 基本評価基準(Base Metrics)

基本評価基準では、脆弱性そのものの特性を評価する基準で、8種類の項目を評価し、CVSS 基本値を算出する。8種類の評価項目は表 A-2 のとおりである。

表 A-2 CVSS v3.1 における基本評価基準の評価項目^[3]

評価項目	内容
攻撃元区分 (AV : Attack Vector)	脆弱性のあるコンポーネント※9をどこから攻撃可能であるかの評価を示す。
攻撃条件の複雑さ (AC : Attack Complexity)	脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さの評価を示す。
必要な特権レベル (PR : Privileges Required)	脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルの評価を示す。
ユーザ関与レベル (UI : User Interaction)	脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルの評価を示す。
スコープ (S : Scope)	脆弱性のあるコンポーネントへの攻撃による影響範囲の評価を示す。
機密性への影響(情報漏洩の可能性) (C : Confidentiality Impact)	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が漏えいする可能性の評価を示す。
完全性への影響 (情報改ざんの可能性) (I : Integrity Impact)	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が改ざんされる可能性の評価を示す。
可用性への影響 (業務停止の可能性) (A : Availability Impact)	脆弱性を攻撃された際に、対象とする影響想定範囲の業務が遅延・停止する可能性の評価を示す。

これらの各評価項目に対して、脆弱性ごとに適切な項目を選択していき深刻度を算出する。それぞれの評価項目に対する選択項目とその説明をまとめたものが、表 A-3 である。

表 A-3 CVSS v3.1 における基本評価基準の選択項目^[3]

評価項目	選択項目	説明
攻撃元区分 (AV : Attack Vector)	N (ネットワーク)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。例えば、インターネットからの攻撃など
	A (隣接)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。例えば、ローカル IP サブネット、ブルートゥース、IEEE 802.11 ^{※10} 等
	L (ローカル)	対象コンポーネントをローカル環境から攻撃する必要がある。例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など
	P (物理)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。例えば、IEEE 1394 ^{※11} 、USB 経由で攻撃が必要など
攻撃条件の複雑さ (AC : Attack Complexity)	L (低)	特別な攻撃条件を必要とせず、対象コンポーネントを常に攻撃可能である。
	H (高)	攻撃者以外に依存する攻撃条件が存在する。例えば、次のいずれかの条件に合致する場合などが該当する。攻撃者は、設定情報、セッション番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。攻撃者は、中間者攻撃のため環境が必要となる。
必要な特権レベル (PR:Privileges Required)	N (不要)	特別な権限を有する必要はない。
	L (低)	コンポーネントに対する基本的な権限を有していれば良い。
	H (高)	コンポーネントに対する管理者権限相当を有する必要がある。
ユーザ関与レベル (UI : User Interaction)	N (不要)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。

	R (要)	リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。
スコープ (S : Scope)	U (変更なし)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープ※12に留まる。
	C (変更有り)	影響範囲が脆弱性のあるコンポーネントの帰属するオーソリゼーションスコープ以外にも広がる可能性がある。例えば、クロスサイトスクリプティング、リフレクター攻撃に悪用される可能性のある脆弱性など
機密性への影響 (情報漏洩の可能性) (C : Confidentiality)	H (高)	機密情報や重要なシステムファイルが参照可能であり、その問題による影響が全体に及ぶ。
	L (低)	情報漏えいやアクセス制限の回避などが発生はするが、その問題による影響が限定的である。
	なし (N)	機密性への影響はない
完全性への影響 (情報改ざんの可能性) (I : Integrity Impact)	H (高)	機密情報や重要なシステムファイルの改ざんが可能で、その問題による影響が全体に及ぶ。
	L (低)	情報の改ざんが可能ではあるが、機密情報や重要なシステムファイルの改ざんはできないために、その問題による影響が限定的である。
	なし (N)	完全性への影響はない
可用性への影響 (業務停止の可能性) (A : Availability Impact)	H (高)	リソース(ネットワーク帯域、プロセッサ処理、ディスクスペースなど)を完全に枯渇させたり、完全に停止させることが可能である。
	L (低)	リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能である。
	なし (N)	可用性への影響はない

➤ 現状評価基準(Temporal Metrics)

脆弱性の現在の深刻度を評価する基準で、3種類の評価項目から CVSS 現状値を算出する。Exploit コード/PoC コードの出現有無や対策情報が利用可能であるかといった基準で評価する。この基準による評価結果は、脆弱性への対応状況に応じ、時間が経過すると変動する。

3種類の評価項目は表 A-4 のとおりである。

表 A-4 CVSS v3.1 における現状評価基準の評価項目^[3]

評価項目	内容
攻撃される可能性 (E : Exploit Code Maturity)	攻撃コードや攻撃手法が実際に利用可能であるかを評価する。
利用可能な対策のレベル (RL : Remediation Level)	脆弱性の対策がどの程度利用可能であるかを評価する。
脆弱性情報の信頼性 (RC : Report Confidence)	脆弱性に関する情報の信頼性を評価する。

これらの評価項目に対して、脆弱性ごとに項目を選択していき脅威度を算出する。それぞれの評価項目に対する選択項目と説明をまとめたものが、表 A-5 である。

表 A-5 CVSS v3.1 現状評価基準の選択項目^[3]

評価項目	選択項目	説明
攻撃される可能性 (E : Exploit Code Maturity)	X (未評価)	この項目を評価しない。
	H (容易に攻撃可能)	攻撃コードがいかなる状況でも利用可能である。攻撃コードを必要とせず、攻撃可能である。
	F (攻撃可能)	攻撃コードが存在し、ほとんどの状況で使用可能である。
	P (実証可能)	実証コードが存在している。 完成度の低い攻撃コードが存在している。
	U (未実証)	実証コードや攻撃コードが利用可能でない。 攻撃手法が理論上のみで存在している。
利用可能な対策レベル (RL : Remediation Level)	X (未評価)	この項目を評価しない。
	U (なし)	利用可能な対策がない。 対策を適用できない。

	W (非公式)	製品開発者以外からの非公式な対策が利用可能である。
	T (暫定)	製品開発者からの暫定対策が利用可能である。
	O (正式)	製品開発者からの正式対策が利用可能である。
脆弱性情報の信頼性 (RC : Report Confidence)	X (未評価)	この項目を評価しない。
	C (確認済)	製品開発者が脆弱性情報を確認している。 ソースコードレベルで脆弱性の存在を確認されている。 脆弱性情報が実証コードや攻撃コードなどにより広範囲に確認されている。
	R (未確認)	セキュリティベンダや調査団体から、複数の非公式情報が存在している。 ソースコードレベルで脆弱性の存在が確認できていない。 脆弱性の原因や検証が十分ではない。
	U (未確認)	未確認の情報のみ存在している。 いくつかの相反する情報が存在している。

なお、現状評価基準において未評価項目を選択した場合、「最も危険度が高い」（容易、ない、確認済み）と同等の評価になる。

➤ 環境評価基準(Environmental Metrics)

ユーザ利用環境も含め、最終的な脆弱性の深刻度を評価する基準で、「対象システムのセキュリティ要求度」と「環境条件を加味した基本評価の再評価」の2つの評価軸から CVSS 環境評価値を算出する。(表 A-6)

表 A-6 CVSS v3.1 における環境評価基準の評価項目^[3]

評価項目	内容
対象システムのセキュリティ要求度 (CR、IR、AR : Security Requirements)	要求されるセキュリティ特性に関して、その該当項目(『機密性(C)』、『完全性(I)』、『可用性(A)』)を重視する場合、その該当項目を高く評価する。 該当項目毎に、『機密性の要求度(Confidentiality Requirement : CR)』、『完全性の要求度(Integrity Requirement : IR)』、『可用性の要求度(Availability Requirement : AR)』を評価する。
環境条件を加味した基本評価の再評価 (Modified Base Metrics)	攻撃の難易度を評価する項目、攻撃による影響を評価する項目を実状に合わせて再評価する。実状に合わせた再評価は、現時点での利用環境に対して再評価したり、緩和策や対策後の利用環境に対して再評価したりすることになる。

「対象システムのセキュリティ要求度」に対して項目を選択し、「環境条件を加味した基本評価の再評価」については、基本評価基準と同様の項目を自社の環境に照らし合わせて再度選択する。

「対象システムのセキュリティ要求度」に対して選択項目とその説明をまとめたものが、表 A-7 である。

表 A-7 CVSS v3.1 の環境評価基準の選択項目^[3]

評価項目	選択項目	説明
対象システムのセキュリティ の要求度 (CR/IR/AR : Security Requirements)	未評価(X)	この項目を評価しない。
	低(L)	該当項目を失われても、一部の影響にとどまる。
	中(M)	該当項目を失われると、深刻な影響がある。
	高(H)	該当項目を失われると、壊滅的な影響がある。

なお、未評価項目を選択した場合、「中」と同じ評価になる。また、環境条件を加味した基本評価の再評価において、未評価項目を選択した場合、基本評価基準と同じ評価になる。

B) CVSS v4.0 の詳細説明

本節では、CVSS v4.0 の各評価指標についてまとめる。CVSS v4.0 では v3.1 同様、脆弱性の深刻度レベルを 4 段階に分類している。詳細は Appendix A 節を参照いただきたい。

➤ 基本評価基準(Base Metrics)

基本評価基準では 11 種類の項目を評価し、CVSS 基本値を算出する。11 種類の評価項目は表 B-1 のとおりである。

表 B-1 CVSS v4.0 における基本評価基準の評価項目^{[3][11]}

評価項目	内容
攻撃元区分 (AV : Attack Vector)	脆弱性のあるコンポーネントをどこから攻撃可能であるかの評価を示す。
攻撃条件の複雑さ (AC : Attack Complexity)	脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さの評価を示す。
攻撃の実行条件 (AT : Attack Requirements)	脆弱性のあるコンポーネントを攻撃する際に必要な前提条件の有無の評価を示す。
必要な特権レベル (PR : Privileges Required)	脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルの評価を示す。
ユーザ関与レベル (UI : User Interaction)	脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルの評価を示す。
脆弱なシステムの機密性への影響 (VC : Confidentiality Impact to the Vulnerable System)	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が漏えいする可能性の評価を示す。
脆弱なシステムの完全性への影響 (VI : Integrity Impact to the Vulnerable System)	脆弱性を攻撃された際に、対象とする影響想定範囲の情報が改ざんされる可能性の評価を示す。
脆弱なシステムの可用性への影響 (VA : Availability Impact to the Vulnerable System)	脆弱性を攻撃された際に、対象とする影響想定範囲の業務が遅延・停止する可能性の評価を示す。
後続システムの機密性への影響 (SC : Confidentiality Impact to the Subsequent System)	脆弱性を攻撃された際に、脆弱なシステムに関連する他のシステムの情報が漏えいする可能性の評価を示す。
後続システムの完全性への影響 (SI : Integrity Impact to the Subsequent System)	脆弱性を攻撃された際に、脆弱なシステムに関連する他のシステムの情報が改ざんされる可能性の評価を示す。

後続システムの可用性への影響 (SA : Availability Impact to the Subsequent System)	脆弱性を攻撃された際に、脆弱なシステムに関連する他のシステムの業務が遅延・停止する可能性の評価を示す。
---	---

これらの項目について、v3.1 との差分に触れながら説明していく。

はじめに、「攻撃の難易度」に分類される表 B-1 の上から 5 項目について触れていく。v3.1 になかった項目としては、「攻撃の実行条件」が追加されており、ここでは攻撃を成功させるために特定の前提条件を必要とするか否かの判定がされている。

次に「攻撃時による影響」(Impact Metrics) について触れていく。v3.1 から存在した脆弱なシステムへの「機密性への影響」「完全性への影響」「可用性への影響」の評価に加えて、後続システムへのそれぞれの影響を評価する項目を追加している。これにより、v3.1 に存在した脆弱性悪用時の影響の広がり具合を表す「スコープ」が廃止されている。これらの項目が追加されることで、攻撃されたシステム以外への影響を考慮できるようになっている。

以上を踏まえ、それぞれの評価項目に対する選択項目とその説明をまとめたのを表 B-2 に示す。

表 B-2 CVSS v4.0 の基本評価基準の選択項目^{[3][11]}

評価項目	選択項目		内容
	v4	v3.1	
攻撃元区分 (AV : Attack Vector)	N (ネットワーク)	N (ネットワーク)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。例えば、インターネットからの攻撃など
	A (隣接)	A (隣接)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。例えば、ローカル IP サブネット、ブルートゥース、IEEE 802.11 など
	L (ローカル)	L (ローカル)	対象コンポーネントをローカル環境から攻撃する必要がある。例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など
	P (物理)	P (物理)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。例えば、IEEE 1394、USB 経由で攻撃が必要など
攻撃条件の複雑さ	L (低)	L (低)	特別な攻撃条件を必要とせず、対象コンポーネントを常に攻撃可能である。

(AC : Attack Complexity)	H (高)	H (高)	攻撃者以外に依存する攻撃条件が存在する。 例えば、次のいずれかの条件に合致する場合などが該当する。攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。攻撃者は、中間者攻撃のため環境が必要となる。
攻撃の実行条件 (AT : Attack Requirements)	N (なし)	—	攻撃を成功させるために、特定の条件は存在しない。
	P (あり)	—	攻撃を成功させるために、特定の条件が存在する。例えば、攻撃者は、攻撃を成功させるために、競合が発生する条件を明らかにする必要がある、中間者攻撃のため環境が必要となるなど。
必要な特権レベル (PR : Privileges Required)	N (不要)	N (不要)	特別な権限を有する必要はない。
	L (低)	L (低)	コンポーネントに対する基本的な権限を有していれば良い。 例えば、秘密情報以外にアクセスできるなど
	H (高)	H (高)	コンポーネントに対する管理者権限相当を有する必要がある。 例えば、秘密情報にアクセスできるなど
ユーザ関与レベル (UI:User Interaction)	N (不要)	N (不要)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。
	P (受動的)	R (要)	v3:リンクのクリック、ファイル閲覧、設定の変更など、ユーザ動作が必要である。 v4 : 関与は必要だが、意識的な関与は不要
	A (能動的)	—	v4 : 関与は必要で、意識的な関与が必要
脆弱なシステムの機密性への影響 (VC : Confidentiality)	H (高)	H (高)	機密性が完全に失われ、脆弱なシステムのすべての情報が漏えいし、その問題による影響が全体に及ぶ。

Impact to the Vulnerable System)	L (低)	L (低)	機密性が部分的に失われ、脆弱なシステムにおいて情報漏えいなどが発生はするが、その問題による影響は限定的である。
	なし (N)	なし (N)	脆弱なシステムに機密性への影響はない。
脆弱なシステムの完全性への影響 (VI : Integrity Impact to the Vulnerable System)	H (高)	H (高)	完全性が完全に失われ、脆弱なシステムのすべての情報の改ざんが可能で、その問題による影響が全体に及ぶ。
	L(低)	L(低)	完全性が部分的に失われ、脆弱なシステムにおいて情報の改ざんが可能となるが、その問題による影響は限定的である。
	なし (N)	なし (N)	脆弱なシステムに完全性への影響はない。
脆弱なシステムの可用性への影響 (VA : Availability Impact to the Vulnerable System)	H (高)	H (高)	可用性が完全に失われ、脆弱なシステムにおいて、リソースを完全に枯渇させる、完全に停止させることが可能であり、その問題による影響が全体に及ぶ。
	L (低)	L (低)	可用性が部分的に失われ、脆弱なシステムにおいて、リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能であるが、その問題による影響は限定的である。
	なし (N)	なし (N)	脆弱なシステムに可用性への影響はない。
後続システムの機密性への影響 (SC : Confidentiality Impact to the Subsequent System)	H (高)	—	機密性が完全に失われ、脆弱なシステムに関連する他のシステムにおいても、すべての情報が漏えいし、その問題による影響が全体に及ぶ。
	L (低)	—	機密性が部分的に失われ、脆弱なシステムに関連する他のシステムにおいても、情報漏えいなどが発生はするが、その問題による影響は限定的である。
	なし (N)	—	脆弱なシステムに関連する他のシステムに機密性への影響はない。
後続システムの完全性への影響 (SI : Integrity Impact	H (高)	—	完全性が完全に失われ、脆弱なシステムに関連する他のシステムにおいても、すべての情報の改ざんが可能で、その問題による影響が全体に及ぶ。

to the Subsequent System)	L (低)	—	完全性が部分的に失われ、脆弱なシステムに関連する他のシステムにおいても、情報の改ざんが可能となるが、その問題による影響は限定的である。
	なし (N)	—	脆弱なシステムに関連する他のシステムに完全性への影響はない。
後続システムの可用性への影響 (SA : Availability Impact to the Subsequent System)	H (高)	—	可用性が完全に失われ、脆弱なシステムに関連する他のシステムにおいても、リソースを完全に枯渇させる、完全に停止させることが可能であり、その問題による影響が全体に及ぶ。
	L (低)	—	可用性が部分的に失われ、脆弱なシステムに関連する他のシステムにおいても、リソースを一時的に枯渇させたり、業務の遅延や一時中断が可能であるが、その問題による影響は限定的である。
	なし (N)	—	脆弱なシステムに関連する他のシステムに可用性への影響はない。

ここからは各項目の選択項目について、v3.1 と v4.0 を比較し、変更点を説明していく。

- 「攻撃元区分」
変更がなかった。
- 「攻撃情報の複雑さ」
変更がなかった。
- 「攻撃の実行条件」
今回新たに追加された項目であり、脆弱性を突く攻撃を成功させるための対象システムの前提条件の有無が評価される。
- 「ユーザ関与レベル」
CVSS v4.0 では評価が N・R（要・不要）の 2 段階評価から N・P・A（不要・パッシブ・アクティブ）の 3 段階になった。
- 「スコープ」
CVSS v4.0 から廃止となった。
- 「機密性への影響」「完全性への影響」「可用性への影響」
変更はなかった。
- 「後続システムへの機密性の影響」「後続システムへの完全性への影響」「後続システムへの可用性の影響」

CVSS v4.0 で新たに設定された項目で、攻撃を受けた脆弱なシステムに関連している他のシステムへの影響度を3段階で評価する内容となっている。

➤ **脅威評価基準 (Threat Metrics)**

脅威評価基準における CVSS v3.1 から CVSS v4.0 への変更点を図 B-4 に示す。CVSS v3.1 では、「現状評価基準」として「攻撃される可能性」「利用可能な対策レベル」「脆弱性情報の信頼性」の3つのメトリクスから構成されていたが、CVSS v4.0 では「脅威評価基準」と改名され、含まれるメトリクスも「攻撃される可能性」の1つに見直されている。

□ CVSS v3.1

評価項目	意味
攻撃される可能性 (E : Exploit Code Maturity)	攻撃コードや攻撃手法が実際に利用可能であるかを評価する。
利用可能な対策のレベル (RL : Remediation Level)	脆弱性の対策がどの程度利用可能であるかを評価する。
脆弱性情報の信頼性 (RC : Report Confidence)	脆弱性に関する情報の信頼性を評価する。



□ CVSS v4.0

評価項目	意味
攻撃される可能性 (E : Exploit Maturity)	攻撃コードや攻撃手法が実際に利用可能であるかを評価する。

図 B-1 CVSS v3.1⇒CVSS v4.0 脅威評価基準の変更点

脅威評価基準の唯一の評価項目となっている「攻撃される可能性」の評価は CVSS v3.1 では5段階だったが、CVSS v4.0 では4段階になっている。また、それぞれの評価項目の内容にも変化が生じている (表 B-3)。

表 B-3 CVSS v4.0 の脅威評価基準の選択項目^{[3][11]}

評価項目	選択項目		内容
	v4	v3.1	
攻撃される可能性 (E : Exploit Maturity)	X (未定義)	X (未評価)	この項目を評価しない。
	—	H (容易に攻撃可能)	攻撃コードがいかなる状況でも利用可能である。攻撃コードを必要とせず、攻撃可能である。
	A (攻撃確認)	F (攻撃可能)	v3.1 : 攻撃コードが存在し、ほとんどの状況で使用可能である。

			v4：攻撃活動は報告されている、あるいは、脆弱性を攻撃できる状態にある。
	P (概念実証)	P (実証可能)	v3.1：実証コードが存在している。完成度の低い攻撃コードが存在している。 v4：実証コードは存在しているが、悪用される段階に達していない。
	U (未報告)	U (未実証)	v3.1：実証コードや攻撃コードが利用可能でない。 攻撃手法が理論上のみで存在している。 v4：実証コードや攻撃活動などは報告されていない。

➤ 環境評価基準(Environmental Metrics)

環境評価基準の評価項目は v3.1 と同様であるため、表 A-6 を参照いただきたい。

評価項目の「対象システムのセキュリティ要求度」の内容については、CVSS v3.1 からの変更はないため、表 A-7 を参照いただきたい。

「環境条件を加味した基本評価の再評価」については、「後続システムの完全性・可用性への影響」を除く各項目は基本評価基準で使用している値で再評価する（図 B-2）。

- 攻撃元区分 (MAV: Modified Attack Vector)
- 攻撃条件の複雑さ (MAC: Modified Attack Complexity)
- 攻撃の実行条件 (MAT: Modified Attack Requirements)
- 必要な特権レベル (MPR: Modified Privileges Required)
- ユーザ関与レベル (MUI: Modified User Interaction)
- 脆弱なシステムの機密性への影響 (MVC: Modified Vulnerable System Confidentiality)
- 脆弱なシステムの完全性への影響 (MVI: Modified Vulnerable System Integrity)
- 脆弱なシステムの可用性への影響 (MVA: Modified Vulnerable System Availability)
- 後続システムの機密性への影響 (MSC : Modified Subsequent System Confidentiality)

➤ 未評価 (X:Not Defined)：この項目を評価しない

➤ 未評価以外については、各項目が基本評価基準で使用している値を選択

図 B-2 CVSS v4.0 の再評価項目（基本評価基準と同じ項目での評価のもの）

「後続システムの完全性への影響」と「後続システムの可用性への影響」に関して、v4.0 では環境評価基準においては安全性に関する選択項目が追加された。本項目は ICS が脆弱性

を悪用された際に人身に被害を与える可能性がある場合に選択される。これにより、v3.1では考慮されていなかった ICS の評価が可能になった（表 B-4）。

表 B-4 CVSSv4.0 後続システムの完全性/可用性への影響^[1]

評価項目	選択項目		内容（環境評価における）
	環境評価	基本評価	
後続システムの完全性/可用性への影響 (MSI : Modified Subsequent System Integrity) (MSA : Modified Subsequent System Availability)	X (未評価)	-	この項目を評価しない。
	H (高)	H (高)	完全性/可用性が完全に失われる。
	L (低)	L (低)	完全性/可用性が部分的に失われる。
	N (軽微)	N (なし)	完全性/可用性への影響は軽微である。
	S (安全性)	-	脆弱性が悪用された場合に、人が怪我をするなどの安全性に関する影響がある場合に使用する。IEC 61508 ^{*13} による危害の程度が中程度、重大、致命的に該当する場合に、高(H)/低(L)/なし(N)以外に、安全性(S)を選択できる。

➤ **補足評価基準 (Supplemental Metric Group)**

v4.0 では、新しく補足評価基準が追加され、該当の脆弱性の特性を追加で表現し、評価者へ伝えられるようになった。補足評価基準は、以下の6つのメトリクスで構成される。

- 安全性 (S : Safety)
- 自動化可能性 (AU : Automatable)
- 供給者による緊急度 (U : Provider Urgency)
- 回復可能性 (R : Recovery)
- 価値密度 (V : Value Density)
- 対応の困難度 (RE : Vulnerability Response Effort)

なお、これらのメトリクスは最終的なリスク評価スコアには影響を与えない。一方で、脆弱性の対応判断に影響を与える可能性がある情報を得ることができる。

6つのメトリクスの各項目について以下に掲載する。

- 「安全性」

システムの使用目的や用途に安全性が含まれる場合には、そのシステムの脆弱性を悪用されたときに安全性への影響があるかどうかを明示できる基準となっている。本メトリクスの評価は任意であり、未評価であることは「安全性に関するインパクトがないこと」を意味しない点に留意が必要である（表 B-5）。

表 B-5 補足評価基準（安全性）^[11]

評価項目	選択項目	内容
安全性 (Safety)	X (未評価)	この項目を評価しない。
	N (軽微)	IEC 61508 による危害の程度が軽微である。
	P (影響あり)	IEC 61508 による危害の程度が中程度、重大、致命的に該当する。

- 「自動化可能性」

複数のシステムに対して、脆弱性を悪用した攻撃の自動化が可能かを評価する。自動化の対象範囲は、サイバーキルチェーンのステップである 1.偵察(Reconnaissance)、2.武器化(Weaponization)、3.配送(Delivery)、4.攻撃(Exploitation)、5.インストール(Installation)、6.遠隔制御(Command and Control)、7.実行(Actions on Objectives)のうち、ステップ 1～4(偵察、武器化、配送、攻撃)である。

表 B-6 補足評価基準（自動化可能性）^[11]

評価項目	選択項目	内容
自動化可能性 (Automatable)	X (未評価)	この項目を評価しない。
	N (なし)	ステップ 1～4(偵察、武器化、配送、攻撃)を自動化することはできない。
	Y (あり)	ステップ 1～4(偵察、武器化、配送、攻撃)を確実に自動化できる。

- 「供給者による緊急度」

製品ベンダ、販売代理店などが、利用者に対して、脆弱性情報の緊急度を伝達するための評価基準となっている。（表 B-7）

表 B-7 補足評価基準（供給者による緊急度）^[1]

評価項目	選択項目	内容
供給者による緊急度 (Provider Urgency)	X (未評価)	この項目を評価しない。
	Red	脆弱性の影響の緊急度は高い
	Amber	脆弱性の影響の緊急度は中程度
	Green	脆弱性の影響の緊急度は低い
	Clear	脆弱性の影響に緊急性はない

- 「回復可能性」

脆弱性が攻撃された際に、性能と可用性の観点からサービスを回復するためのコンポーネント/システムの回復力を示す評価基準となっている（表 B-8）。

表 B-8 補足評価基準（回復可能性）^[1]

評価項目	選択項目	内容
回復可能性 (Recovery)	X (未評価)	この項目を評価しない。
	A (自動)	サービスは自動的に回復する。
	U (手動)	サービスを回復するためにはユーザによる手動の介入を必要とする。
	I (回復不能)	ユーザが介入しても回復できない。

- 「価値密度」

攻撃者が1回の攻撃活動の結果、利用可能となる資源の状況の評価する基準である。(表B-9)

表 B-9 補足評価基準（価値密度）^[1]

評価項目	選択項目	内容
価値密度 (Value Density)	X (未評価)	この項目を評価しない。
	D (少ない)	脆弱性のあるコンポーネントを含むシステムは資源に限りがある。攻撃者が単一の攻撃で利用できる資源は比較的少ない。
	C (豊富)	脆弱性のあるコンポーネントを含むシステムは資源が豊富である。

- 「対応の困難度」

製品とサービスの脆弱性に対処するために必要な労力を示す評価基準となっている。(表B-10)。

表 B-10 補足評価基準（対応の困難度）^[1]

評価項目	選択項目	意味
対応の困難度 (Vulnerability Response Effort)	X (未評価)	この項目を評価しない。
	L (低)	脆弱性に対処するために必要な労力は小さい。例えば、アップグレード、ファイアウォールによるアクセス制御など
	M (中)	脆弱性に対処するためには、ある程度の作業が必要となる。例えば、サブシステムの無効化、ドライバー更新など
	H (高)	脆弱性に対処するために必要な労力はとても大きく、サービスへの影響が持続する可能性がある。例えば、物理的な交換が必要、ハードウェアなどの修復不可能な障害など

C) SSVc v2.1 の詳細説明

SSVC ではステークホルダごとの決定木を利用し、各脆弱性に対する意思決定のための結果を出力をしている。本節では各ステークホルダの決定木の説明をする。決定木ごとの出力結果は、決定木ごとに異なっている。各ステークホルダに合わせた対応判断が用意されている。(表 C-1)

表 C-1 ステークホルダごとの決定木の出力

ステークホルダ	判断 (決定木の出力)
サプライヤー (パッチ提供側)	- Defer: 対応不要 - Scheduled: 定期メンテナンス時に対応
デプロイヤー (パッチ利用側)	- Out-of-Cycle: 定期メンテナンス以外の早い時期に対応 - Immediate: 迅速な対応
コーディネーター 1 (調整役、トリアージ)	- Decline: 対応不要 - Track: 観測を継続 - Coordinate: 対応する
コーディネーター 2 (調整役、情報公開)	- Don't publish: 公開しない - Publish: 公開する
CISA (参考 ^[12])	- Track: 観測を継続 - Track*: 定期メンテナンス時に対応 - Attend: 定期メンテナンス以外の早い時期に対応 - Act: 迅速な対応

➤ デプロイヤーツリー

デプロイヤーの決定木では、条件分岐において Exploitation / Exposure / Automatable / HumanImpact の 4 種類が存在しており^[6]、各概要は以下の図 C-1 のとおりである。

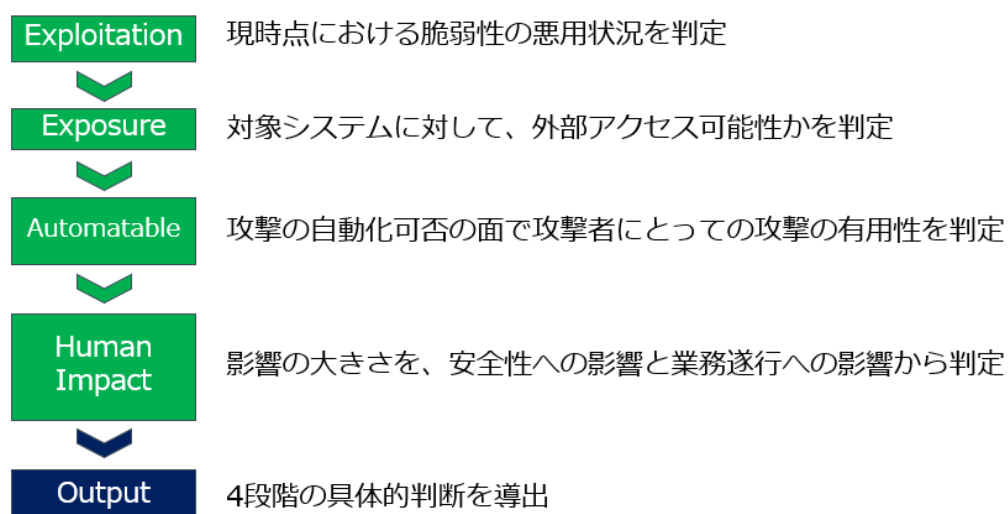


図 C-1 デプロイヤーツリーの概要図

• 「Exploitation」

現時点における脆弱性の悪用状況を判定している。決定木の選択項目としては、「None / PoC / Active」の 3 種類がある。脆弱性に対する悪用状況を確認し、項目を選択する。(表 C-2)

表 C-2 Exploitation の選択項目^[13]

選択項目	内容
None	実際に悪用されている証拠がなく、かつ攻撃検証コードが公開されていない。
PoC	ダークウェブ ^{※14} 、ディープウェブ ^{※15} などのアンダーグラウンドで攻撃検証コードが売買されている、攻撃検証コードがインターネット上の脆弱性データベースやソースコードリポジトリで公開されている、または攻撃の再現手法が公知となっている。
Active	公的機関、セキュリティベンダ、ソーシャルメディアなどで脆弱性を悪用した攻撃の発生が確認、報告されている。

• 「Exposure」

影響を受けるシステムの外部露出の程度を判定している。決定木の選択項目としては、「Small / Controlled / Open」の 3 種類がある。脆弱性を持つ該当システムに対して、資産情報及びネットワーク構成情報を加味し項目を選択する。(表 C-3)

表 C-3 Exposure の選択項目^[13]

選択項目	内容
Small	ネットワークに接続されていないサービスやプログラムまたはファイアウォールなどで厳格にアクセスが制御されたネットワーク
Controlled	らかのアクセス制限や緩和措置が施されているネットワーク
Open	アクセス制限を十分に実施できないインターネット、または広くアクセス可能なネットワーク（DNS サーバー、ウェブサーバー、VOIP サーバー、メールサーバーなどが該当する）

- 「Automatable」

攻撃者が脆弱性を悪用した攻撃を自動化できるかどうかを評価する。決定木の選択項目としては、「No / Yes」の2種類が存在する。ここではサイバーキルチェーンのステップ1~4（偵察・武器化・配送・攻撃）を自動化可能かどうかで判断する。（表 C-4）

表 C-4 Automatable の選択項目^[13]

選択項目	内容
No	サイバーキルチェーンのステップ1~4（偵察・武器化・配送・攻撃）の自動化が困難。自動化が困難な理由としては、以下のような理由が挙げられる： ・ネットワーク経由での脆弱性の検出・列挙が不可能 ・武器化にあたり人間による個別の関与が必要 ・配信にあたり広く普及しているネットワークセキュリティ対策の回避が必要 ・ASLR 等の規定で適用される脆弱性攻撃緩和策によりエクスプロイトの信頼性が低い
Yes	偵察からエクスプロイトの自動化が可能。または、外部からのコードインジェクション、コマンドインジェクションなど、任意コード実行が可能

- 「HumanImpact」

影響の大きさとして、安全性の影響と業務遂行への影響の両面から評価する。安全性の影響としては、「None / Minor / Major / Hazardous / Catastrophic」の五段階で評価する（表 C-5）。業務遂行への影響としては、「None / Degraded / Crippled / MEF Failure / Mission Failure」の五段階で評価する（表 C-6）。最終的に、「HumanImpact」は安全性の影響と業務遂行への影響の評価を組み合わせ、決定木の選択項目として「Low / Medium / High / Very High」の4種類から評価される（表 C-7）。

表 C-5 安全性の影響の選択項目^[13]

選択項目	内容	
None	影響が「Minor」以下（影響が全くないわけではなく、「Minor」の閾値以下）	
Minor	以下のいずれかに該当する場合	
	Physical Harm	システム利用者の不快感
		軽微な労働安全衛生上の危険
		物理的なシステムの安全マージンの減少
	Enviroment	軽微な物的損害や環境的な損害
	Finacial	複数の人に対する金銭的な損失
	Psycological	複数の人に対する精神的、または心理的な損害
Major	以下のいずれかに該当する場合	
	Physical Harm	システム利用者の身体的苦痛、負傷
		重大な労働安全上の危険
		物理的なシステムの障害
	Enviroment	大きな物理的損害や環境的損害
	Finacial	複数の人に対する破産に繋がるような大きな金銭的な損失
	Psycological	集団に対する精神的、または心理的な損害
Hazardous	以下のいずれかに該当する場合	
	Physical Harm	重傷、または致命傷につながる危険
		安全な運用を支援するサイバーフィジカルシステムの一部故障
	Enviroment	生命への脅威、広範囲の環境破壊、公衆衛生リスクの可能性など
	Finacial	選挙や金融などの社会を支えるシステムが不安定化や安全ではない状態に陥る
	Psycological	N/A
Catastrophic	以下のいずれかに該当する場合	
	Physical Harm	多数の死者の発生
	Environment	公衆衛生への脅威、小規模な生態系の破壊につながる環境破壊など
	Financial	選挙や金融などの社会を支えるシステムの崩壊
	Psycological	N/A

表 C-6 業務遂行の影響の選択項目^[13]

選択項目	Mission Impact
None	ミッション達成に必要な機能にはほとんど影響がない。
Degraded	ミッション達成に必要な機能に影響がある。
Crippled	ミッション達成を直接的に支える活動が機能不全となるが、ミッション達成に必要な機能は一時的に継続する。
MEF Failure	ミッション達成に不可欠な機能のいずれかにおいて、許容範囲を超えて長期間にわたり障害が発生する。
Mission Failure	ミッション達成に不可欠な機能の複数または全てに障害が発生し、回復能力が低下する。回復能力の低下により組織のミッションが果たせなくなる。

表 C-7 安全性の影響と業務遂行の影響の組み合わせに対する HumanImpact の出力結果^[13]

Situated Safety Impact	Mission Impact	Human Impact
None/Minor	None/Degraded/Crippled	Low
None/Minor	MEF Failure	Medium
None/Minor	Mission Failure	Very High
Major	None/Degraded/Crippled	Medium
Major	MEF Failure	High
Major	Mission Failure	Very High
Hazardous	None/Degraded/Crippled	High
Hazardous	MEF Failure	High
Hazardous	Mission Failure	Very High
Catastrophic	None/Degraded/Crippled	Very High
Catastrophic	MEF Failure	Very High
Catastrophic	Mission Failure	Very High

- 「Output」

意思決定に直結する判断結果が提供される。判断結果として、「Defer/Scheduled/Out-of-Cycle/Immediate」の4種類が存在する（表 C-8）。

表 C-8 デプロイヤーツリーの Output

ステークホルダー	判断（決定木の出力）
デプロイヤー （パッチ適用側）	● Defer: 対応不要 ● Scheduled: 定期メンテナンス時に対応 ● Out-of-Cycle: 定期メンテナンス以外の早い時期に対応 ● Immediate: 迅速な対応

➤ サプライヤーツリー

サプライヤーツリーの決定木では、条件分岐として、Exploitation / Utility / TechnicalImpact / PublicSafetyImpact の4種類が存在しており^[6]、それぞれの概要は以下の図 C-2 のとおりである。

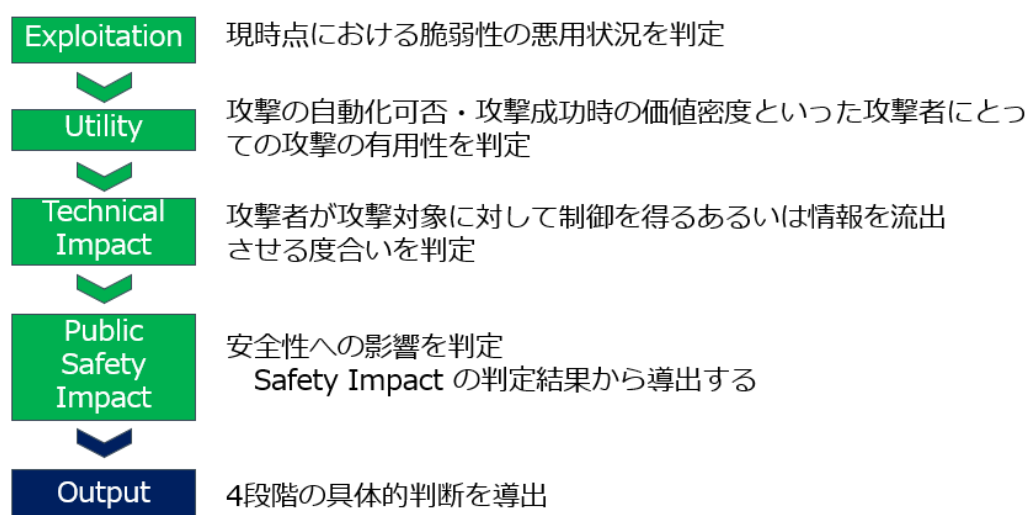


図 C-2 サプライヤーツリーの概要図

- 「Exploitation」

デプロイヤーツリーと同様である。表 C-2 を参照のこと。

- 「Utility」

攻撃の自動化可否・攻撃成功時に得られるリソース量（価値密度）の項目から攻撃者視点で有用性を評価する。Automatable(攻撃の自動化可否)と Value Density(価値密度)の両面から評価する。攻撃の自動化可否については、「No / Yes」の2段階で評価され

る（表 C-9）。価値密度については、「Diffuse / Concentrated」の2種類で評価される（表 C-10）。

最終的に、「Utility」は攻撃の自動化可否と価値密度の評価を組み合わせ、決定木の選択項目として、「Laborious/Efficient/Super Effective」の3種類から評価される（表 C-11）。

表 C-9 Automatable の選択項目^[13]

選択項目	内容
No	自動化が困難な理由としては以下のような理由が挙げられる。 • ネットワーク経由での脆弱性の検出・列挙が不可能 • 武器化にあたり人間による個別の関与が必要 • 配信にあたり広く普及しているネットワークセキュリティ対策の回避が必要 • ASLR 等の規定で適用される脆弱性攻撃緩和策によりエクスプロイトの信頼性が低い
Yes	偵察からエクスプロイトの自動化が可能。または、外部からのコードインジェクション、コマンドインジェクションなど、任意コード実行が可能

表 C-10 Value Density の選択項目^[13]

選択項目	内容
Diffuse	攻撃成功時に攻撃者が得られるリソースやコントロールが限定的。システム管理者ではない一般ユーザのアカウント、端末など。
Concentrated	攻撃成功時により高いリソースやコントロールを奪取することが可能。データベース、認証サーバ、ログイン機能を提供するウェブサーバ、クラウドサービスプロバイダー、秘匿性の高いデータなど。

表 C-11 Automatable と Value Dnsity の組み合わせに対する Utility の出力結果^[13]

	Automatable	Value Density
Laborious	No	Diffuse
Efficient	No	Concentrated
	Yes	Diffuse
Super Effective	Yes	Concentrated

- 「Technical Impact」

攻撃を受けた場合の技術的影響を判定する。選択項目としては、「Partial / Total」の2種類がある。この評価を実施するにあたり、脆弱性が存在するコンポーネントが、システムの中でどのような役割を持つか理解しておく必要がある。(表 C-12)

表 C-12 Technical Impact の選択項目^[13]

選択項目	内容
Partial	攻撃成功時に攻撃者は、限定的なコントロールの奪取・情報の窃取を行うことが可能。または実現性が非常に低い前提の下、完全なコントロールを奪取することが可能。
Total	攻撃成功時に攻撃者は、脆弱性が存在するシステムの完全なコントロールの奪取・情報の窃取を行うことが可能。

- 「Public Safety Impact」

脆弱性による安全性に対する影響度を判定する。選択項目としては、「Minimal / Significant」の2種類がある。(表 C-13)

表 C-13 Public Safety Impact の選択項目^[13]

選択項目	内容
Minimal	Safety Impact の判定結果が None または Minor
Significant	Safety Impact の判定結果が Major、Hazardous、Catastrophic

- 「Output」

意思決定に直結する判断結果が提供される。判断結果はデプロイヤーツリーと同様で、「Defer/Scheduled/Out-of-Cycle/Immediate」の4種類が存在する。表 C-8 を参照のこと。

➤ コーディネーターツリー

コーディネーターツリーでは、トリアージツリーと情報公開ツリーの2種類のツリーが存在する。トリアージツリーでは、公開された脆弱性情報に対する情報展開するかの対応要否を判定する。情報公開ツリーでは、脆弱性情報を公開するかどうかの判定をする。

[1] トリアージツリーの条件分岐

「Public / Contacted / Credible / Cardinality / Engagement / Utility / PublicSafetyImpact」の7種類が存在しており^[6]、それぞれの概要は以下の図 C-3 のとおりである。

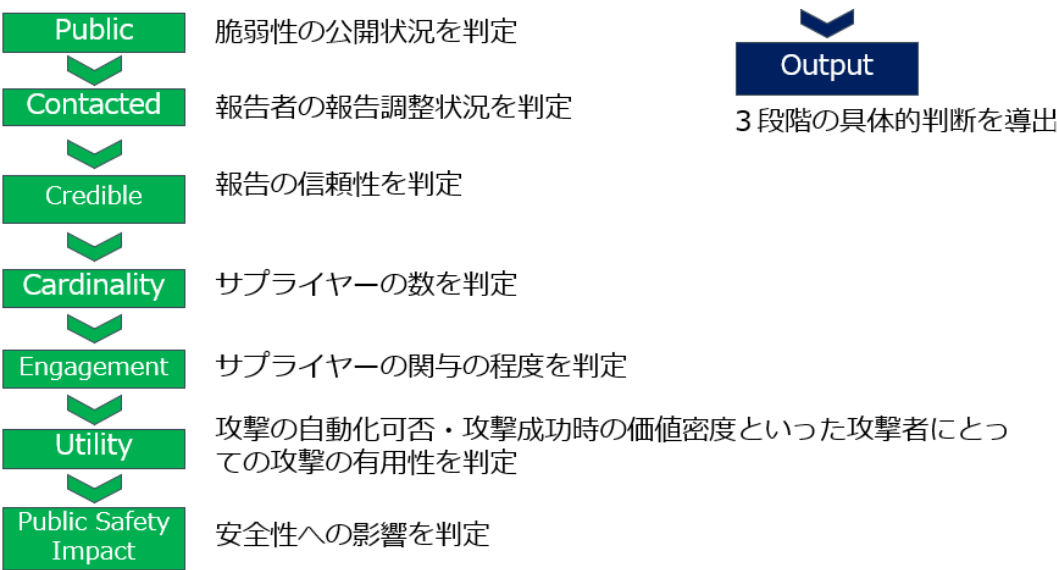


図 C-3 トリアージツリーの概要図

• 「Public」

脆弱性情報の公開の程度を判定する。

決定木の選択項目としては「Yes / No」の2種類がある。(表 C-14)

表 C-14 Public の選択項目^[6]

選択項目	内容
No	脆弱性の詳細に関するレポートが既に公開されている
Yes	脆弱性の詳細に関するレポートがまだ公開されていない

- 「Contracted」

サプライヤーとの報告調整状況を判定する。決定木の選択項目としては、「Yes / No」の2種類が存在する。質の高い連絡方法としては、一般に公表されている良好な電子メールアドレスや、ベンダのウェブサイト上の公開ポータル等がある。(表 C-15)

表 C-15 Contacted の選択項目^[6]

選択項目	内容
No	質の高い連絡方法を用いて、脆弱なコンポーネントを供給したサプライヤーに対して誠実に連絡する努力をした
Yes	質の高い連絡方法を用いて、脆弱なコンポーネントを供給したサプライヤーに対して誠実に連絡する努力をしていない

- 「Credible」

公開された報告書の信頼性を判定する。決定木の選択項目としては、「Credible/Not Credible」の2種類が存在する。(表 C-16)

表 C-16 Credible の選択項目^[6]

選択項目	内容
Credible	報告書は信頼できる
Not credible	報告書は信頼できない

- 「Cardinality」

サプライヤの数を判定する。決定木の選択項目としては、「One / Multiple」の2種類が存在する。(表 C-17)

表 C-17 Cardinality の選択項目^[6]

選択項目	内容
One	脆弱なコンポーネントとその修復・緩和計画に責任を負うサプライヤは1社である
Multiple	脆弱なコンポーネントとその修復・緩和計画に責任を負うサプライヤは複数社である

- 「Engagement」
サプライヤの関与について判定する。決定木の選択項目としては、「Active / Unresponsive」の2種類が存在する。(表 C-18)

表 C-18 Engagement の選択項目^[6]

選択項目	内容
Active	サプライヤはレポーターの連絡に答え、調整作業に積極的に参加している
Unresponsive	サプライヤはレポーターの連絡に答えない、または調整作業に積極的に参加していない

- 「Utility」
サプライヤーツリーと同様。表 C-11 を参照のこと。
- 「Public Safety Impact」
サプライヤーツリーと同様。表 C-13 を参照のこと。
- 「Output」
意思決定に直結する判断結果が提供される。判断結果として、「Decline / Track / Coordinate」の3種類が存在する。(表 C-19)

表 C-19 コーディネーター 1 の Output

ステークホルダー	判断（決定木の出力）
コーディネーター 1 (調整役、トリアージ)	• Decline: 対応不要 • Track: 観測を継続 • Coordinate: 対応する

[2] 情報公開ツリー

情報公開ツリーの決定木では、条件分岐として、Supplier involvement / Exploitation / Value added の3種類が存在しており^[6]、それぞれの概要は以下の図 C-4 のとおりである。

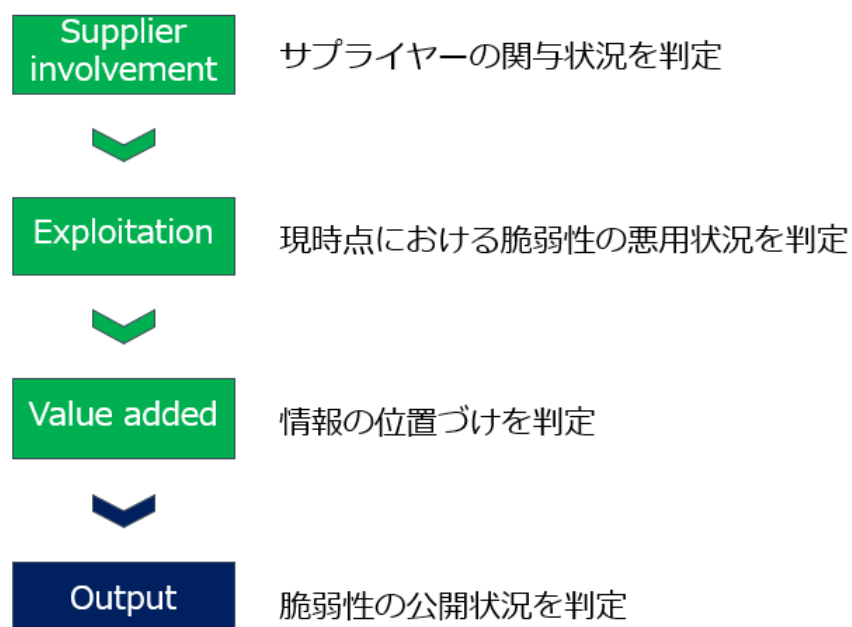


図 C-4 情報公開ツリーの概要図

- 「Supplier involvement」
サプライヤーの脆弱性対応に取り組んでいる関与状況を判定する。決定木の選択項目としては、「Fix ready / Cooperative / Uncooperative」の3種類がある。(表 C-20)

表 C-20 Supplier involvement の選択項目^[6]

選択項目	内容
Fix Ready	サプライヤーがパッチまたは修正プログラムを提供している
Cooperative	サプライヤーはパッチや修正プログラムを積極的に作成している。
Uncooperative/ Unresponsive	サプライヤーが応答しない、修正の生成を拒否する、あるいはサプライヤーがすでに存在しない。

- 「Exploitation」
デプロイヤーツリーと同様。表 C-2 を参照のこと。

- 「Value Added」

公開情報の位置づけを判定する。決定木の選択項目としては、「Precedence / Ampliative / Limited」の3種類がある。(表 C-21)

表 C-21 Value Added の選択項目^[6]

選択項目	内容
Precedence	公開する情報が世の中で最初に公開される情報であるか、最初に公開される情報と同時期の公開である。
Ampliative	既存の情報の追加的な情報や、他の公開情報の修正、追加的な注意喚起など、既存の情報
Limited	既存の情報の質が高く、複数の情報源で提供されているため、既存の公開情報に付加される価値が限定的である。

- 「Output」

意思決定に直結する判断結果が提供される。判断結果として、「Don't publish / Publish」の2種類が存在する。(表 C-22)

表 C-22 コーディネーター2の Output

ステークホルダー	判断 (決定木の出力)
コーディネーター2 (調整役、情報公開)	• Don't publish: 公開しない • Publish: 公開する

D) EPSS の詳細説明

EPSS は以下の 5 つのステップで 30 日以内に悪用される可能性を算出している。EPSS の概要を図 D-1 に示す。

ステップ 1：脆弱性情報の収集では、公開された脆弱性情報そのものに対する情報を収集する。

ステップ 2：悪用活用の証拠を収集では、脆弱性の悪用が試みられたことを示す証拠を収集する。

ステップ 3：脆弱性情報と悪用活動の関係を発見・学習（EPSS モデリング）では、機械学習を活用してステップ 1・2 で収集した情報間のパターンと関係を特定する。

ステップ 4：パフォーマンスを測定・調整してモデルを最適化（EPSS パフォーマンス）では、EPSS モデリングのアップデートが実施される。

ステップ 5：今後 30 日間の悪用確率の日時推定値を生成（悪用確率の生成）では、今後 30 日間に悪用活動が観察される確率とパーセンタイルが出力される。

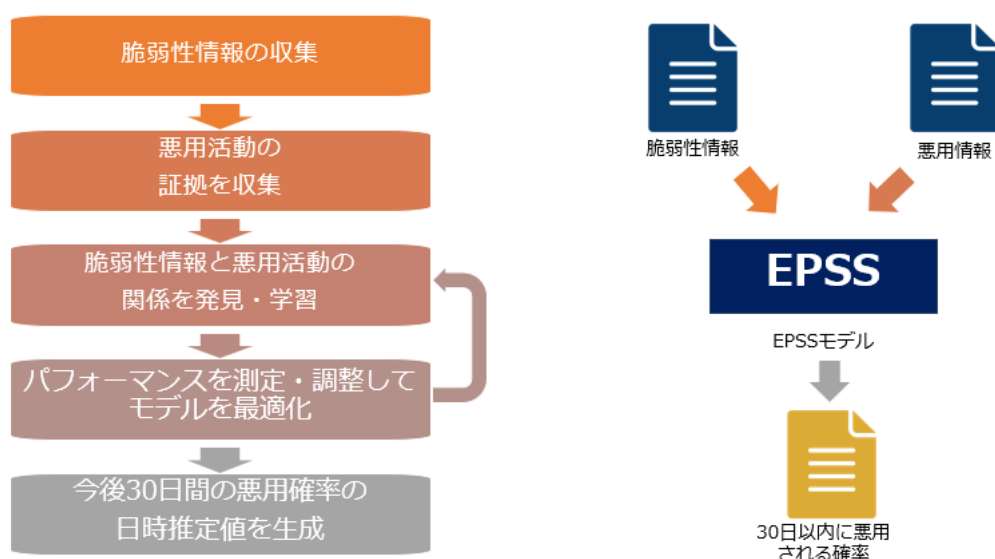


図 D-1 EPSS の概要図

ステップ 2 で収集する悪用活動の証拠は、脆弱性の悪用が試みられたことを示すものであり、脆弱なターゲットに対して攻撃が成功したことを示すものではない。悪用活動の証拠の情報元となるデータは、FIRST のデータ提供パートナーのフィードバックから収集したデータであり、ハニーポット^{※16}/IPS センサー/ホストベースの検出のような情報を活用している。ここで注意する点として、KEV（1.6 節参照）のような情報は悪用活動としてではなく、ステップ 1 の脆弱性情報の収集で利用されていることである。EPSS では、30 日以内に悪用される確率を算出するために、悪用されたタイミングを正確に知り、現在も継続して悪

用されているかどうかを知ることを重要視している。

各脆弱性に対する EPSS の値については、FIRST の公式ページから取得することが可能である。また、API が公開されており、JSON 形式で EPSS スコアを取得することも可能である。EPSS の API から取得可能なデータは表 D-1 のとおりである。

表 D-1 EPSS の API から取得可能なデータ

項目	意味	値(例)	備考
Status	レスポンスの状態を示す。	OK	OK = 正常な値
Status-code	レスポンスの HTTP ステータスコードを示す	200	200 = 成功
Version	使用されている EPSS API のバージョンを示す	1.0	今回の場合 1.0
Access	データにアクセスするための権限を示す	Public	一般公開
Total	レスポンスに含まれるデータの総数を示す	1	データの総数
Offset	レスポンス内のデータの開始位置を示す	0	データの開始位置
limit	1 回のリクエストで取得できるデータの最大数を示す	100	-
data	実際のデータが含まれる部分	Cve ~ Date 迄	実際のデータが含まれる部分
Cve	CVE 識別子を示す	CVE-2011-2523	CVE 識別子を示す
EPSS	EPSS スコアを示す	"0.123000000"	EPSS スコア
Percentile	EPSS スコアのパーセンタイルを示す。	"0.951040000",	EPSS スコアのパーセンタイル
Date	脆弱性の報告日付を示す	"2022-09-01"	-

E) CVEdetails.com

● 概要

CVEdetails.com (<https://www.cvedetails.com/>) は SecurityScorecard 社が提供している無料の脆弱性情報提供サイトで、NVD を含む複数サイトを参照し、CVE に紐づく情報をまとめているサイトである。サブスクリプションに登録することで、RSS カスタムフィールドや API 利用のような機能も一部存在する。

ホーム画面にはダッシュボード画面があり、新規/更新された CVE 情報、過去 10 年間の CVE スコア、過去 10 年間の CVE 推移グラフが確認可能である。新規/更新された CVE 情報では、数日間の CVE や EPSS の変化を視覚的に表示してくれる。図 E-1 のグラフでは、昨日以降・7 日以内・30 日以内の期間で以下条件に当てはまる CVE と、EPSS スコアが 5%以上・10%以上・50%以上変動したものをカウントし表示されている。

- ・新規発番もしくは更新された CVE
- ・KEV に新規掲載された CVE
- ・EPSS スコアが変動した CVE

青文字の部分はクリックすると条件に該当する CVE 一覧が表示され、各 CVE の詳細ページにも移動できる。

New/Updated CVEs



67 CVEs created, **79** CVEs updated since yesterday

1013 CVEs created, **1240** CVEs updated in the last 7 days

4891 CVEs created, **10235** CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday

0

Last 7 days

1

Last 30 days

11

Recent EPSS score changes

>5%

10

>10%

2

>50%

0

図 E-1 新規/更新された CVE 情報

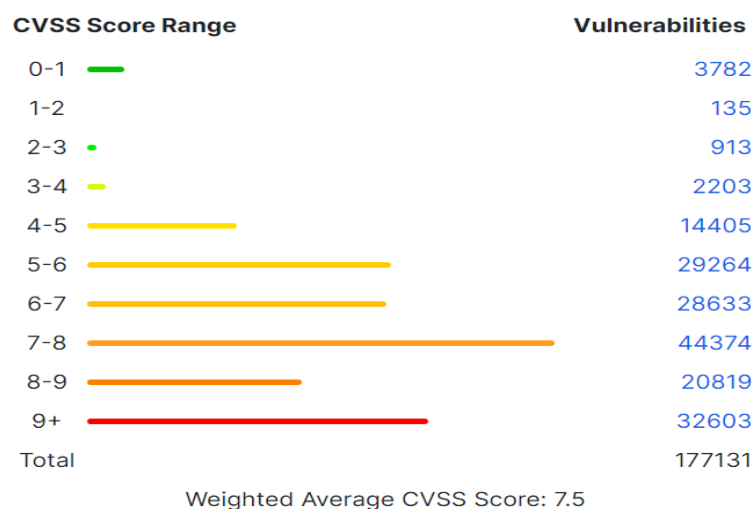
CVE 詳細ページでは各 CVE に紐づく情報を一元的に確認可能である。CVE 詳細ページの記載内容は、表 E-1 のとおり。

表 E-1 CVE に対する情報一覧

項目	内容
脆弱性の説明	脆弱性の詳細説明が記載されている。また、エクスプロイトが存在することやランサムウェア攻撃への利用がタグ付けされている。
複数ソースの CVSS スコアと CVSS ベクトル	CVSS スコアが NIST や Microsoft など複数で算出されている場合、それぞれ掲載される。
KEV 掲載有無	KEV に掲載されているかが記載されている。
Metasploit モジュール	Metasploit モジュールの実装情報が記載されている。
EPSS スコア	現在の EPSS スコアが記載されている。また、過去の EPSS スコアも確認可能であり、推移グラフも表示される。
CWE ID	関係する CWE が記載されている。
影響を受ける製品	影響を受ける製品・バージョン等が記載されている。

過去 10 年間の CVE スコアでは、以下の図 E-2 のように、過去 10 年間で発番された CVE をスコアごとにカウントされた情報として確認可能である。

Distribution of vulnerabilities by CVSS scores



* For CVEs published in the last 10 years

図 E-2 過去 10 年間の CVE スコア分布

過去 10 年間の CVE 推移グラフでは、以下の図 E-3 のように過去 10 年間の各年で発番された CVE の数の推移が表示されている。最多の 2023 年は 29,065 件となっており、発番される CVE の数が年々増加していることがわかる。

Vulnerabilities by type & year

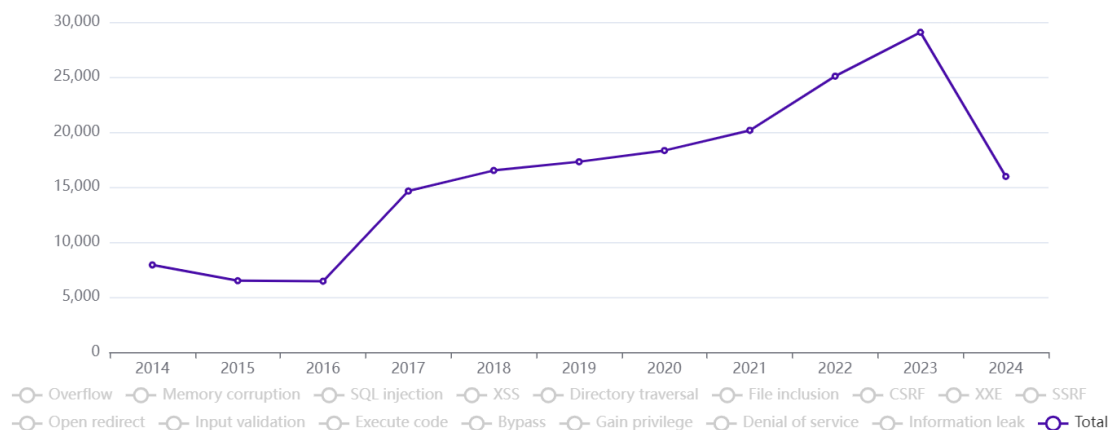


図 E-3 過去 10 年間の CVE 推移グラフ

● EPSS の情報

ここからは、EPSS スコアに変動があった CVE をピックアップする機能について説明する。図 E-4 では、EPSS スコアの変動が 10%以上あった場合の CVE 一覧である。この一覧より確認可能な情報は以下のとおりである。

- ・ EPSS スコア変動日
- ・ CVE
- ・ 変動前の EPSS スコア
- ・ 変動後の EPSS スコア
- ・ 変動値

また、EPSS スコアの変動は以下から選択することができる。ただし、利用者側で自由に値を設定することはできない。

- ・ ±1%
- ・ ±5%
- ・ ±10%
- ・ ±50%
- ・ +5%
- ・ +10%
- ・ +50%
- ・ ALL

EPSS score history - Score changes > +10%

Show score changes (delta) greater than: [±1%](#) [±5%](#) [±10%](#) [±50%](#) [+5%](#) [+10%](#) [+50%](#) [All](#)

Page: 1



変動値

#	Date	CVE	Old EPSS Score	New EPSS Score	Delta (New - Old)
1	2024-05-20	CVE-2021-3378	55.13%	68.55%	+13.43
2	2024-05-20	CVE-2015-2117	24.91%	38.84%	+13.93
3	2024-05-20	CVE-2014-1770	46.66%	68.20%	+21.54
4	2024-05-20	CVE-2007-4620	11.89%	22.04%	+10.16
5	2024-05-19	CVE-2023-46574	7.04%	20.19%	+13.15
6	2024-05-19	CVE-2014-3806	8.33%	18.46%	+10.13
7	2024-05-19	CVE-2007-3799	14.71%	41.23%	+26.52
8	2024-05-18	CVE-2010-0492	71.17%	84.05%	+12.88
9	2024-05-18	CVE-2007-4478	36.60%	58.60%	+22.00
10	2024-05-18	CVE-2007-3122	3.25%	40.93%	+37.67

図 E-4 EPSS スコア履歴

3.4 節の脅威情報をモニタリングする際に、CVEdetails の EPSS スコア履歴を活用することで EPSS スコアが上昇した CVE を確認することが可能となる。

F) Vulnrichment

● 概要

Vulnrichment プロジェクトとは、NIST の NVD 更新停滞などの問題解決のために 2024 年 5 月 9 日に CISA が立ち上げたプロジェクトである。NVD で公開されている脆弱性情報に対して、関連する様々な情報を付加して公開することを目指している。このプロジェクトの背景として、NVD が公開する脆弱性情報に対して、ユーザ側でリスク評価を実施する際に CVSS・SSVC・KEV 等を活用しており、これらの情報を NVD で付加 (enrichment) するのが理想的であるがリソース不足により実施できていない。そこで CISA が、公開された CVE に対してエンリッチ化するための取り組みを始めている。この取り組みでは、CPE・CVSS・CWE・KEV を CVE へ追加することに重点を置いている。また、SSVC の「Exploitation」・「Automatable」・「Technical impact」に関する情報共有も実施される。これらの SSVC の情報は、リスク評価を実施する際の脅威情報に該当する。そのため、2.2 節の SSVC を利用する際にネックとなっていた脅威情報の収集が困難である課題を解決する一助となる。現状、この取り組みは開発段階であるが、CVE のエンリッチ化が進むことでユーザ側でのリスク評価の向上に繋がると考えられる。

ここで、Vulnrichment で情報が公開されるまでの流れは図 F-1 のとおり。まず、①CISA が各 CVE を SSVC の 3 項目に対して評価を実施する。該当する 3 項目としては、「Exploitation」・「Automatable」・「Technical impact」である。ここで、Technical impact は CISA 独自の重要インフラストラクチャ用の決定木で利用される項目である。②CPE・CVSS・CWE・KEV・SSVC に関する情報を付与し、③Github(<https://github.com/cisagov/vulnrichment>)にて公開される。

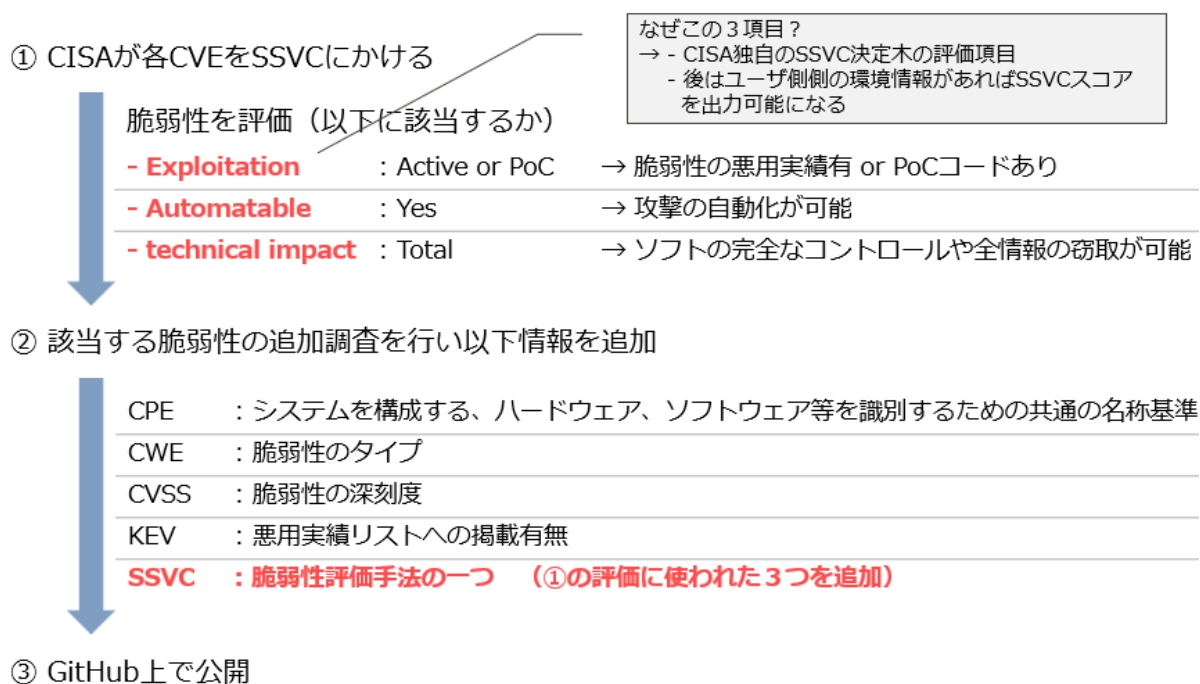


図 F-1 Vulnrichment

Vulnrichment を活用することで、SSVC を活用したリスク評価を簡易的にすることが可能である。SSVC において、ユーザ環境情報であるユーザ側で判断が必要な情報と脅威情報である Vulnrichment で公開される情報を活用することでリスク評価可能である。

SSVC の決定木ごとに活用する情報を図 F-2 に示す。デプロイヤーツリーの決定木における選択項目は、「Exposure」「Exploitation」「Automatable」「Human impact」である。この中で、「Exploitation」「Automatable」は Vulnrichment で公開される情報であり、

「Exposure」「Human impact」はユーザ側で判断が必要な情報となる。そのため、リスク評価の際には Vulnrichment で公開される情報を活用することで、ユーザ側で選択する項目を減らすことが可能である。

Vulnrichmentで公開される情報

ユーザ側で判断が必要な情報

判断基準	内容	決定木		
		CISA版	デプロイヤー	サプライヤー
Exposure	システムの外部アクセス可否	—	○	—
Exploitation	脆弱性の悪用状況	○	○	○
Utility	Automatable 攻撃の自動化可否	○	○	○
	Value Density 攻撃成功時に得られる価値密度	—	—	○
Technical Impact	攻撃を受けた際の技術的影響	○	—	○
Mission & Well-Being	事業継続への影響と人的影響	○	—	—
Human impact (Mission Impact, Situating Safety Impact)	安全への影響と事業継続への影響	—	○	—
Public Safety Impact	安全への影響	—	—	○

図 F-2 Vulnrichment と SSVc の関係

次に、Vulnrichment から取得できるデータについても紹介する。データ構造の概要は図 F-3 のとおりである。データ形式は json である。現時点では開発中のため、CVE ごとにデータ構造が異なる場合がある。データとしては、metrics に SSVc と KEV の情報、affected に CPE の情報、problem Types の CWE-ID の情報が記載されている。

■データ形式：json

■取得できる主なデータと対象キー

※ 現時点（2024/5/20）ではCVEごとにデータ構造が異なる場合があるため参考情報

metrics {

・SSVCの情報：

- role（決定木）

- Exploitation/Automatable/Technical Impact

・KEV への登録情報

affected {

・CPE

problemTypes {

・CWE-ID

図 F-3 Vulnrichment の取得データ概要

さらに、Vulnrichment の取得データ例は図 F-4 になる。この例では、CVE-2024-21762 の情報について紹介する。この CVE においては、SSVC・KEV・CPE の情報が記載されている。SSVC の情報としては、Exploitation が active、Automatable が yes、Technical impact が total となっている。この情報とユーザ側の環境情報を用いることでリスク評価可能となる。また、KEV は掲載日付があり、CPE の情報も記載されている。

対象 : CVE-2024-21762(024¥21xxx¥CVE-2024-21762.json)

SSVC :

- Exploitation : active
- Automatable : yes
- Technical Impact: : total

KEY :

- dateAdded: : 2024-02-09

CPE :

- 複数記載あり : (例)

cpe:2.3:a:fortinet:fortiproxy:1.0.0:*:*:*:*:*:*

図 F-4 Vulnrichment の取得データ例

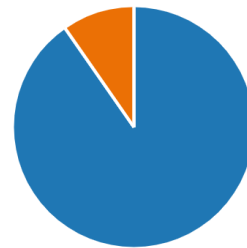
Vulnrichment は現時点では開発途中となっており、データ登録量も少なく、NVD のような API も用意されていないため、運用で利用されるのはまだ先となる。また、掲載される脆弱性の網羅性や記載される情報量等の課題がある。しかし、複数の情報を一括で掲載されるのはユーザー側としては非常に有益であり、活用することで運用負荷軽減が期待できるため、今後の開発に期待したい。

G) ICSCoE 参加企業へのアンケート結果

本書の「まえがき」にて、ICSCoE 参加企業へのアンケート調査結果の一部を紹介したが、それら以外にも多数の質問項目にて調査を実施したため、その結果を本節にて紹介する。

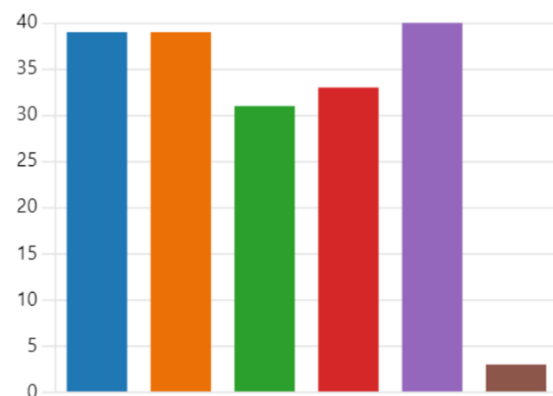
- 自社の IT 資産(PC、サーバ、NW 機器等)に対する資産管理/構成管理に課題を感じていますか

● はい	56
● いいえ	6



- 資産管理/構成管理のどのような点に課題を感じていますか（複数選択可）

● 取得している情報の項目(使用しているライブラリ情報、OSS情報、各種ソフトウェアバージョンなど)が不足	39
● 情報が適切に更新されていない	39
● 情報の信憑性が確認できない/できていない	31
● 運用負荷が高い(工数がかかりすぎる)	33
● 資産の網羅性が確保できていない(シャドーITなど把握できていない資産が存在する)	40
● その他	3



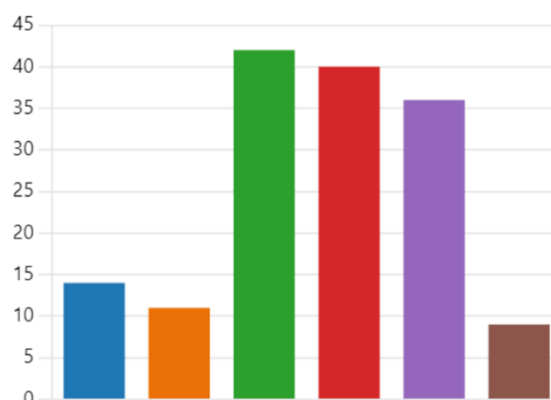
- 業務の一環として脆弱性情報を収集していますか

● 毎日している	19
● 定期的に収集している	29
● 不定期に収集している	13
● 収集していない	1



● 脆弱性情報をどのようにして収集していますか（複数選択可）

ベンダー/OSS自動収集ツールを活用	14
自社独自開発の自動収集ツールを活用	11
脆弱性情報配信サイト(CVE・JVN・JPCERT・KEV・CISA等)を手動でチェック	42
メーリングリスト、フォーラム、ブログやSNS(X、LINEオープンチャット等)	40
セキュリティベンダーもしくは製品ベンダーの情報	36
その他	9



● 脆弱性管理業務に対するリソース（人数）は適正ですか

適正	11
不足しており、増員の予定または検討している	18
不足しており、増員を検討しているが予算が不足している	13
収集していない	20

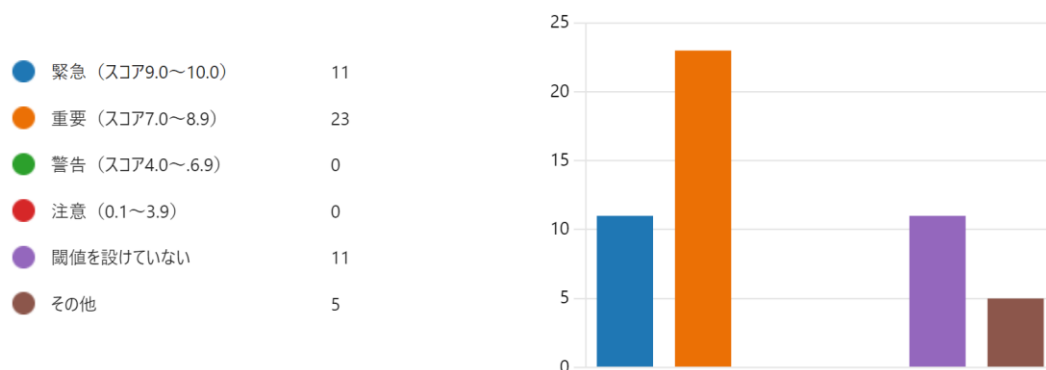


● 次の脆弱性のリスク評価に使用される各手法・指標について、どれを認知されていますか（複数選択可）

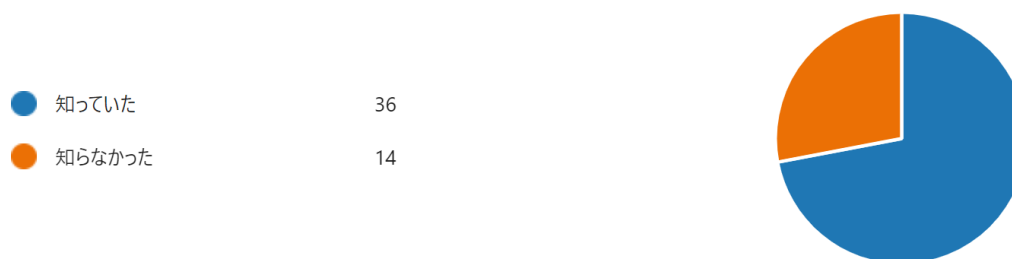
CVSS	57
EPSS	14
SSVC	21
KEV	30
該当なし	6



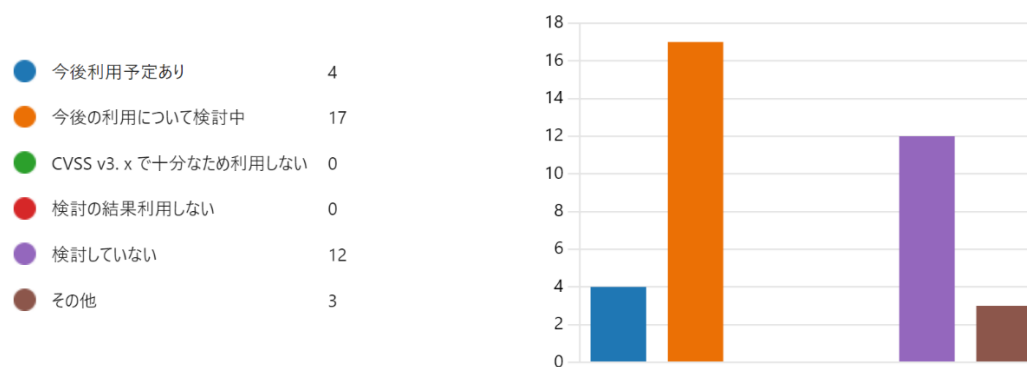
- 脆弱性に対する修正対応(修正パッチや回避策の適用等)を実施する判断の基準となる閾値として、どの値を設定していますか



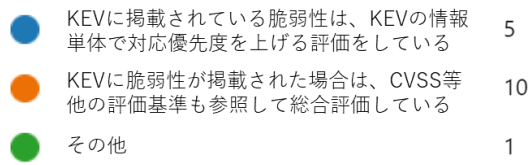
- 2023 年 11 月に CVSS v4.0 が新たにリリースされたのはご存じですか



- CVSS v4.0 を今後利用していく予定はありますか (CVSS v4.0 を知っている場合)



● KEV の利用方法を教えてください（KEV をリスク評価に活用している場合）



用語集

No	用語	意味・解説
1	ICSCoE	産業サイバーセキュリティセンター (Industrial Cyber Security Center of Excellence)
2	CSIRT	Computer Security Incident Response Team セキュリティインシデントが発生した際に対応するチーム
3	ICS	Industrial Control System 主に製造業や生産拠点で用いられる産業用設備をコントロールする情報システム
4	Exploit コード	コンピュータの OS やソフトウェアなどのセキュリティの脆弱性をつつく悪意あるコードやプログラム
5	PoC コード	コンピューターシステムの脆弱性やセキュリティホールが存在および悪用可能であることを証明するために作成された検証用プログラムコードの総称
6	機密性	情報に対するアクセス権限を徹底して保護・管理すること
7	完全性	改ざんや過不足のない正確な情報が保持されていること
8	可用性	情報やシステムが必要なときに利用可能であること
9	コンポーネント	システムやソフトウェアを構成する独立した機能単位で、特定のタスクや役割を持つ要素
10	802.11	IEEE により策定された、広く普及している無線 LAN 関連規格の一つ
11	IEEE 1394	AV 機器やコンピュータを接続する高速シリアルバス規格
12	オーソリゼーション スコープ	ユーザーやアプリケーションがアクセスできるリソースや操作の範囲を定義するアクセス制御の設定
13	IEC 61508	IEC (国際電気標準会議) が制定した基本安全規格(basic safety publication)であり、プロセス産業における電気・電子・プログラマブル電子(Electrical・Electronic・Programmable Electronic)機能安全に関する国際規格である
14	ダークウェブ	匿名性の高いインターネット上の領域を指す。一般的なブラウザではアクセスできず、アクセスには専用のブラウザが必要。
15	ディープウェブ	ディープウェブは検索エンジンからのアクセスができない Web サイトを指す。 アクセスするにはログインなど何らかの認証が必要である。
16	ハニーポット	あえてシステムへの不正侵入を許して攻撃手法や何をターゲットとしているのかを分析する、「おとり」のようなシステム

参考文献

- [1] CVE (MITRE)
<https://cve.mitre.org/>
- [2] Online Browsing Platform (OBP) (ISO)
<https://www.iso.org/obp/ui/#sio:std:iso-iec:27000:ed-5:v1:en>
- [3] 共通脆弱性評価システム CVSS v3 概要 (IPA)
<https://www.ipa.go.jp/security/vuln/scap/cvssv3.html>
- [4] CVSS バージョン 4.0 の変更点と活用可能性 (PwC Japan グループ)
<https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cvss-ver4.html>
- [5] PRIORITIZING VULNERABILITY RESPONSE: A
STAKEHOLDER-SPECIFIC VULNERABILITY
CATEGORIZATION (VERSION 2.0) (カーネギーメロン大学)
https://insights.sei.cmu.edu/documents/606/2021_019_001_653461.pdf
- [6] Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization
(SSVC) version 2.1.0-edb6c97 (カーネギーメロン大学)
https://github.com/CERTCC/SSVC/blob/main/pdfs/ssvc_2_1_draft.pdf
- [7] EPSS (Exploit Prediction Scoring System) を活用した脆弱性管理 (PwC Japan グループ)
<https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/epss.html>
- [8] 優先順位付けから予測へ Vol. 9 (Cisco)
https://www.cisco.com/c/dam/global/ja_jp/products/collateral/security/vulnerability-management/p2p-vulnerability-management-report.pdf
- [9] The Etiology of Vulnerability Exploitation (Jay Jacobs, Michael Roytman)
<https://www.rsaconference.com/library/presentation/usa/2019/the-etiology-of-vulnerability-exploitation>
- [10] 共通プラットフォーム一覧 CPE 概説 (IPA)
<https://www.ipa.go.jp/security/vuln/scap/cpe.html>
- [11] 共通脆弱性評価システム v4.0 (東京電機大学)
https://blog.isl.im.dendai.ac.jp/cti/cvss4_0
- [12] CISA Stakeholder-Specific Vulnerability Categorization Guide (CISA)
<https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf>
- [13] ユーザー企業における SSVC の導入と留意点 (PwC Japan グループ)
<https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/ssvc-introduction.html>

謝辞

本書の作成にあたりまして、JVN 関係者様、JPCERT/CC 様、株式会社ラック様、株式会社 FFRI セキュリティ様、NRI セキュアテクノロジーズ株式会社様また個人として IPA 寺田真敏様（50 音順）、他にもご協力いただいた組織及び個人の皆様に脆弱性対応管理の進め方についてヒアリングさせていただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる、門林雄基先生、満永拓邦先生には、本書の元となる脆弱性対応管理のメンター・講師として、ご指導・ご助言とともに、各検証機材のご支援を賜り続けてきました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトとともに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

<脆弱性対応管理プロジェクトメンバー>

【リーダー】

北谷 真聖

【サブリーダー】

谷原 侑馬 山本 将嗣

【メンバー】

井上 裕斗	橘田 渉	杉山 達哉	永田 将大
中野 貴裕	二本松 立朗	平橋 智史	茂木 亮太
山中 晋爾			

