脆弱性定量化に向けての検討報告書

2007 年 3 月 1 日

NPO 日本ネットワークセキュリティ協会

脆弱性定量化に向けての検討 WG

目次

図表番号

【参加メンバー】

郷間　佳市郎	京セラコミュニケーションシステム㈱　（ＷＧリーダ）
小野　泰司	㈱IRI ユビテック
鹿児島　健	㈱インフォセック
齊藤　伸雄	ウチダインフォメーションテクノロジー㈱
北島　健治	エス・アンド・アイ㈱
中嶋　一樹	住商情報㈱
金岡　晃	セコム㈱
小野　潤	大日本印刷㈱
川又　祥正	大日本印刷㈱
坂本　慶	㈱ディアイティ
松井　康宏	日本アイ・ビー・エム㈱
宮永　直樹	日本電気㈱
世良田　照治	日本電気㈱
奥原　雅之	富士通㈱
倉持　慎一郎	富士通サポート＆サービス㈱
鶴田　章浩	富士通サポート＆サービス㈱
能見　真也	富士通サポート＆サービス㈱
伊勢　俊介	富士通サポート＆サービス㈱
長谷川 喜也	㈱富士通ソーシアルサイエンスラボラトリ
伊澤　誠	マイクロ総合研究所
中山　和郎	みずほ情報総研㈱
伊藤　良孝	三井物産セキュアディレクション㈱
後沢　忍	三菱電機㈱
原田　道明	三菱電機㈱
横山　哲也	横河電機㈱
横地　裕	横河電機㈱
岩井　博樹	㈱ラック

（※ メンバーの所属は本ＷＧ活動中のものです）

1 はじめに

NPO 日本ネットワークセキュリティ協会[1]（以下、JNSA と略す）では、参加企業・団体の有志によってワーキンググループ（以下 WG と略す）活動を行っている。

「脆弱性定量化に向けての検討 WG」（以下、本 WG と略す）では、脆弱性というものに関して定量化が可能なのかということを検討することを目的に活動を行ってきた。

1.1 経緯と目的

定量化という手法がビジネスの現場で使われる理由は、多くの判断を限られた時間の中でスピーディに行えること、かつ、その判断についての説明責任として用いることができるからである。

脆弱性について定量化が求められる理由も同様である。定量的な数値として示されていれば、定性的な説明文をもとに比較・判断を行うことに比べて、短時間でそれを行うことが可能であろう。特に、セキュリティ関連の専門用語は、経営者や一般の社員には難解であり、システム管理者がその危険性を訴えたとしても、その切迫度を適切に伝えきれない場合がある。定量化というアプローチによって得られる「数値」という共通言語は、その溝を埋める方法論としても有効であるといえる。

本WG発足時の状況は、ベンダ各々が独自の判断で脆弱性の危険度を報告しており、同じ「危険度高」であっても、A社とB社ではその判断基準が違っていたり、判断基準そのものが公開されていないといった状況であった。このような中で、ベンダの差に依存しない脆弱性の定量化が可能かどうかということの検討をはじめたことが、本 WG 発足の契機であり目的であった。

1.2 WG 活動の概要

本WGの活動は、月１回～２回、主に工学院大学[2]内にて行われたが、一時期は、各参加メンバーのオフィス等の会議室等を借用して、持ち回りでの開催も行った。参加者それぞれの仕事の内容が異なることから、オフィスを行き来することで、考え方や立場の違いの原因を肌で感じられたらと考えた結果である。また、モデル図の作成の時期には合宿を行い、夜中まで十分な時間を使っての検討を行うことができた。度重なる改変を行いながら、少しずつ合意を形成していくようなア

プローチは、１～２時間の会議では難しく、このモデル図作成の時期に合宿の機会を持てたことは意義があった。

アンケートの収集にあたっては、JNSA のホームページ上で行った。このようなアンケート自体これまであまり行われていなかったため、参考にできる資料が少なく作成に苦労した。アンケート収集の開始に先立って公告を出したところ、セキュリティ情報ページや Blog 等で紹介された。より多くの人の目に公告が触れる機会となり、幸いなことであったと思う。

1.3 報告書の内容と基本的な考え方について

本 WG が活動を開始した時期は、ワーム・ウイルスといった外的脅威が増大し、社会問題になっていた時期である。このため、対策としてパッチの適用を優先するのか、それともパッチそのものによってサーバが停止する危険性を憂慮し、あえてパッチ適用を延期するのかといった判断基準について、参加メンバーの中での問題意識が高かった。このことが反映され、ＷＧの参加者にはソフトウェアベンダに所属するメンバーが多く含まれているにもかかわらず、ベンダ側の立場ではなく、サーバ管理者に代表されるユーザを主体とした立場での考え方を中心として WG 内の議論が進められた。この部分は、WG 発足当初から貫かれた立場であり、本報告書のひとつの特徴である。

また、単に数式を検討するということに終始せず、その背景となる用語の考え方や、脆弱性への攻撃が発生するメカニズムとしてのモデルの検討も行った。この結果、教科書的な内容ではなく、現場の視点から脆弱性とその脅威について整理をし直すという内容となっている。あえて教科書的な定義を捨てるというアプローチから始められたのは、時間的な制約に縛られない議論ができたからであると感じる。

しかし、一方で時間をかけてしまったがゆえに、本 WG が活動を開始した頃と比べて、世の中の意識にいささかの変化が生じている点もある。たとえば、パッチの品質に関しては、その悪影響が世の中で声高に語られることは少なくなった。これは WG 発足当時と比べると大きな社会的変化である。しかし、これはベンダ側の技術的努力の結果だけでなく、マーケティング的なアプローチが功を奏した点も大きいと言える。実際、本報告書の執筆中にも、大手 OS ベンダの提供するパッチに関する不具合が報告されており、依然としてパッチ適用に纏わるリスクは存在し続けている。このため、本書の内容としては、パッチ適用に伴うリスクは無視できないという立場を保っている。やもすると、最近はこのようなリスクに不感症になり、パッチがリリースされればとりあえずその全部を適用するといったアプローチが一般化している感があるが、このような考え方とは、あえて一線を画し、パッチ適用のリスクを前提とした内容である点に留意願いたい。

1.4 想定する読者層

本報告書が想定する読者層としては、ネットワーク機器やサーバ等の管理者、あるいはそれらの管理に対して作業の指示を与える人を想定しており、自宅で PC を利用しているホームユーザについては対象としては意識していない。このため、実施したアンケートについても、対象を同様とした。

1.5 本書で使われる用語・語句の定義

以下は、本 WG で定義した用語・語句の解説である。世の中には、それぞれに異なる意見を持つ人もいるかもしれないが、WG での議論を進めるために、これらの定義を行った。本報告書の内容についても、この定義に従っている。

- 脆弱性
  ソフトウェア及びハードウェアに存在するものであり通常期待されている安全性を損なっている要因
- フィックス
  脆弱性を除去するもの／こと
- パッチ
  ソフトウェアでフィックスするもの
- ワークアラウンド
  副作用のあるフィックス
- 開発ベンダ
  対象となるハードウェア、ソフトウェアを開発した人または組織
- ブラックハット
  攻撃者に手段や手段に関する情報を提供する人または組織（ウイルス作成者も含む）
- 社会情勢
  攻撃行為の動機に影響を与える事象一般
- ウイルス・ワーム
  攻撃者のうち自己の意思をもたないもの（ボットなども含む）

2 脆弱性

本 WG において脆弱性定量化の検討を開始するにあたって、まず始めに議論となったのは、「脆弱性とは何か？」ということであった。

脆弱性という言葉は、一見すると既に定義がしっかりとなされている用語のように思われる。しかし、実態は、その人の立場や、これまでの経験によって、それぞれ異なった認識を持っているということが、WGの中で認識され、最初に解決すべき問題として議論がなされた。また、脆弱性の数値化の試みについては、本WG以外にも試みが行われている。この点についても検討を行った。

例えばCVSS[3]（Common Vulnerability Scoring System）は、その網羅性という点で、現在一定の成功を収めているものである。CVSS は、米国家インフラストラクチャ諮問委員会[4]（NIAC: National Infrastructure Advisory Council）のプロジェクトとして 2004 年から検討が進んでいるものであり、その内容は３つの部分、Base Metrics（基本評価基準)、Temporal Metrics（現状評価基準)、Environmental Metrics（環境評価基準）に分かれている。

本WGでも、その活動の一部として CVSS に関する勉強会を行い、その内容について意見交換を行ったが、参加者の意見としては、Base Metrics の部分については、各ベンダ間での脅威レベルの定義の違いを吸収するという役目を果たせるものとなっているが、それ以外の、Temporal Metrics と Environmental Metrics については、その要素となる項目が十分であるとは言えず、現場の実情に即した数値を導き出すことは難しいのではないかという見解に至った。とくに、それを導出するモデルがシンプルすぎるがゆえの不十分性に問題があると言える。つまり、現在、CVSS が一定の成功を収めているのは Base Metrics の部分であり、それ以外については検討の必要性があるということである。

現場において、その数値だけを頼りにした一時対処を行う場面においては、どのようにしてその数値が生成されるかのロジックを示した事前合意は重要である。それは、その仕組みを事前に理解することによって、指示を出す人、それを受け取る人の間で合意が取れ、迅速な作業が可能となると考えるからである。

本WGでは、この点を重視し、どのようにすれば事前合意がとれるのかについても議論を行った。

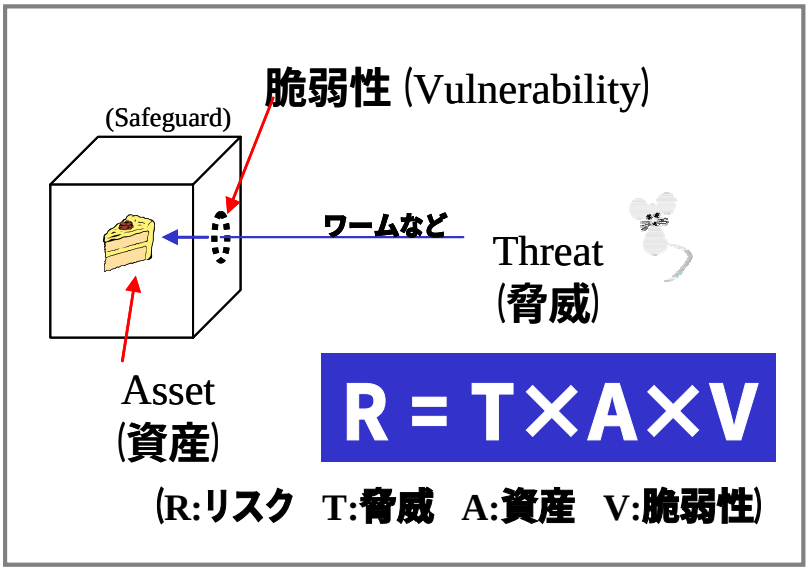
とくに、「脆弱性」と「リスク」が混同されて認識されているという点について、これをどのように捉えるべきかが、初期の議論におけるメインテーマとなった。

2.1 脆弱性とは何か

「脆弱性」と「リスク」が混同されて認識されているという点について、どのように考えるべきであろうか。

「リスク」をセキュリティ事故の発生する場合の被害の期待値として定義するならば、発生確率である「脅威（Threat)」、発生時の被害金額である「資産（Asset)」、被害の大きさを決める「脆弱性（Vulnerability)」の間には、以下の関係が成り立つ。

リスク ＝ 脅威 × 資産 × 脆弱性



このモデルでは、「脆弱性」と「脅威」を別なものとして捉えている。このような関係は、概念的には理解できるものである。しかし、脆弱性を数値化し評価するためには、脅威の要素も含めた危険度（リスクに近い概念）としてそれを捉えることで、より現実味のある表現が可能になると、本WGでは考えた。

すなわち、上記モデルのような、一般に教科書等に示されている概念での「脆弱性」は、本 WG の目標とする数値化のための一要素ではあるものの、定量化対象の『脆弱性』のすべてではないということである。つまり、脅威やリスク、資産の特徴などといった要素の影響も考慮しなければ、現実に感じる「危険度」とは遊離したものとなってしまうということである。

したがって、脅威やリスク、資産の特徴などといった要素の影響も考慮した捉え方をして、はじめて「ネットワーク上の資産に及ぼされる悪影響の度合いの定量化」が可能となり、「パッチ適用の判断」に有効な指標に成り得るという結論に至った。

2.2 『脆弱性』の構成要素

先にも述べたとおり、本 WG で扱う『脆弱性』は一般的な「脆弱性」の要素以外に、資産が受ける影響の度合いや脅威の大きさ等の要素を含んでいる。これらは時間と共に変化することも考慮し、『脆弱性』の構成要素について検討した。

その結果として、以下の 8 つの要素に分類を行った。

要素名	内容

手法	Exploit の存在、レースコンディョン、攻撃の難易度
影響	CIA（機密性、完全性、可用性）の要素 v.s. 権限＋ブランド、被害の深刻度
環境	プロトコルのリモート/ローカル認証
対策	対策をとれるか否か、それが一時的なものか 正式な対策が出ている・一時的(Workaround)・対策がない 副作用の話
原因	仕様・コーディング・設定 パッチの作り易さ
ターゲット属性	誘因性
ソフトウェア特性	ソフトウェアのシェア、ベンダ
社会情勢	定期的なもの、イベント的なもの、カレンダー的なもの

ここで抽出した『脆弱性』の構成要素をスタートラインとし、次章で述べる「モデル化」を実施した。

2.3 本 WG で定量化を目指す指標の定義

前節において、本 WG が扱う『脆弱性』に影響を及ぼす構成要素が明らかにした。これを起点にして、ターゲットとするネットワーク資産に及ぼす影響を定量化することで、フィックス（脆弱性を除去するもの／こと）を今行うべきかどうかを判断するための指標として、使用可能な数値を提供することが可能と考えた。このような指標は、これまで語られてきた脆弱性（Vulnerability）や脅威（Threat）、リスク（Risk）という用語では的確に表現することが不可能であると考え、新たな用語を用意することとし、その指標を「トリアージ値」と命名することとした。トリアージ（Triage）は医療における用語であり、災害などの発生時における多数の傷病者をその重症度と緊急性によって処置・搬送を行う優先順位を決定することを言う。

この指標を「*TV* 」とし、セキュリティ上「好ましくない影響(TV^+)」と「好ましい影響(TV^-)」との和により、実際に資産に及ぼす影響を表現するというアプローチを採ることとした。

従って、本 WG が定量化を目指す指標(トリアージ値、*TV*)は

「意思決定者がフィックス行為を実施するにあたって、その実行可否と実行タイミングを判断するために利用できる指標として使える数値」

と定義することができる。

3　攻撃発生のメカニズム

以上までの検討を踏まえ、本 WG では、脆弱性を利用した攻撃がどのように発生し、その結果どのような形で被害が発生するかというメカニズムの分析を試みた。なぜならば、現場において、数値だけを頼りにした一時対処を行う場面を考えた場合、どのようにしてその数値が生成されるかのロジックを示した事前合意が重要であると考えたからである。これにより、意思決定者と、その意思を受け取る人の間での合意が取れ、迅速な作業が可能となる。この事前合意のために、まずメカニズムを分析しモデル化することが必要であると考えた。

一般に、セキュリティリスクのモデルは「脅威」、「対策」、「脆弱性」、「資産」などの概念の組み合わせで説明されることが多い。例えば、JIS TR X 0036-1「IT セキュリティマネジメントのガイドライン－第１部：IT セキュリティの概念及びモデル」（通称「GMITS」）では、これらの関係をモデル化した図を定義している（図 3-1）。

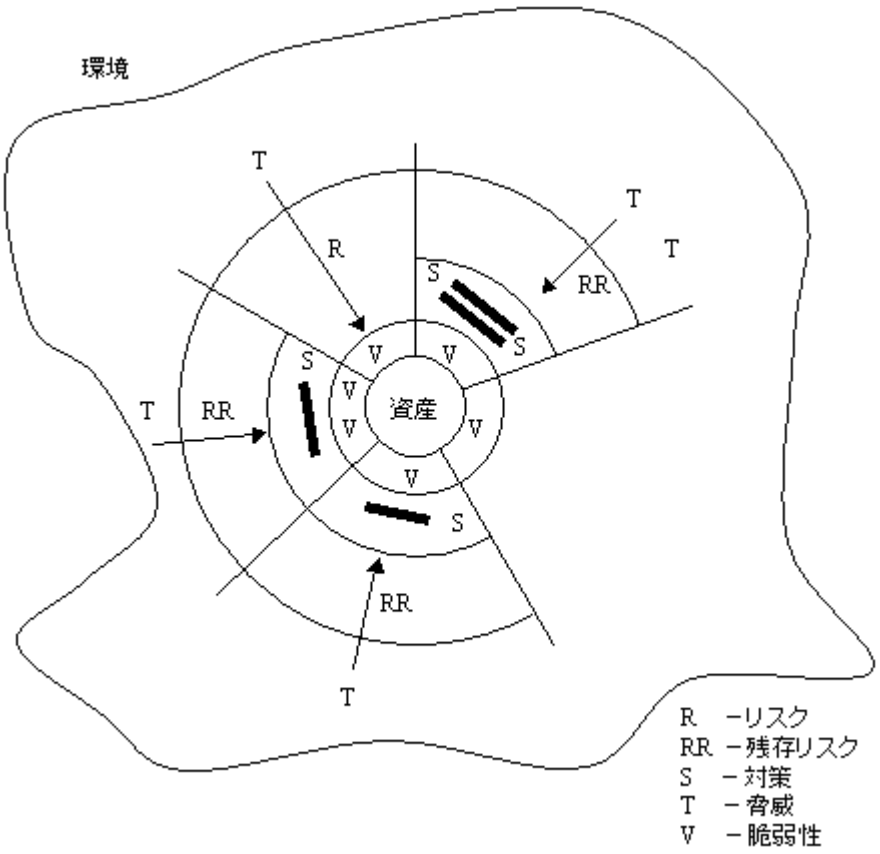


図 3-1 リスクの発生モデル（出典：GMITS）

しかしながら、実際の世界で発生するリスクを取り扱うには、このようなモデルは単純すぎ、十分な記述ができない。例えば、あるリスクが発生するためには複数の脅威が同時に発生しなければならないといった状況や、あるいは、複数の対策が同時に有効になっていることで、はじめてある攻撃を防御することができるなど、実世界のリスクは非常に複雑な背景や相互関係を持っており、簡単な（例えば IF…THEN…のような）ルールで記述することは困難である。これに加え、本WGで導出しようとしているものは、前章でトリアージ値（*TV*）と定義したものであり、GMITS のモデルにおける純粋な脆弱性の値とは別のものを目指している。従って、本 WG ではこれらの違いを反映したモデルを新規に組み上げる必要があった。

3.1 メカニズムのモデル前提

モデル作成の最初のプロセスとして、モデルの構成要素となる概念の洗い出しを行った。前章で提示された要素をスタートラインとして、それぞれの要素に関係のある属性を整理し、類似している要素同士を関連付ける等のブレインストーミングを実施した結果、少なくとも以下の概念についてモデルの構成要素候補として定義が必要であるという合意に達した。

表 3-1 モデルの構成要素の定義

用語	定義
脆弱性	ソフトウェア及びハードウェアに存在するものであり通常期待されている安全性を損なっている要因
フィックス	脆弱性を除去するもの／こと
パッチ	ソフトウェアでフィックスするもの
ワークアラウンド	副作用のあるフィックス
対象ハードウェア／ソフトウェア	脆弱性の保持者
開発ベンダ	対象となるハードウェア、ソフトウェアを開発した人または組織
ホワイトハット	開発ベンダ以外で、フィックスやフィックスに関する情報を提供する人または組織
ブラックハット	攻撃者に手段や手段に関する情報を提供する人または組織（ウイルス作成者も含む）
社会情勢	攻撃行為の動機に影響を与える事象一般

スキル	攻撃を実行するために必要となる知識及び技術（習得に時間を要するもの）
ツール	攻撃の実行を容易にするための情報、ハードウェア及びソフトウェア
ウイルス等	攻撃者のうち自己の意思をもたないもの（ワーム、ボットなども含む）

これらの構成要素のうち、モデルの中で、ある一定の「役割」を持つと思われるものを、モデル中の「オブジェクト」と呼ぶことにした。そしてオブジェクト間の相互作用を矢印型の「リンク」でつなぐことにより、オブジェクト間がどのような関係で成り立っているのかを表現する最初のモデル図の作成を試みた（図 3-2）。

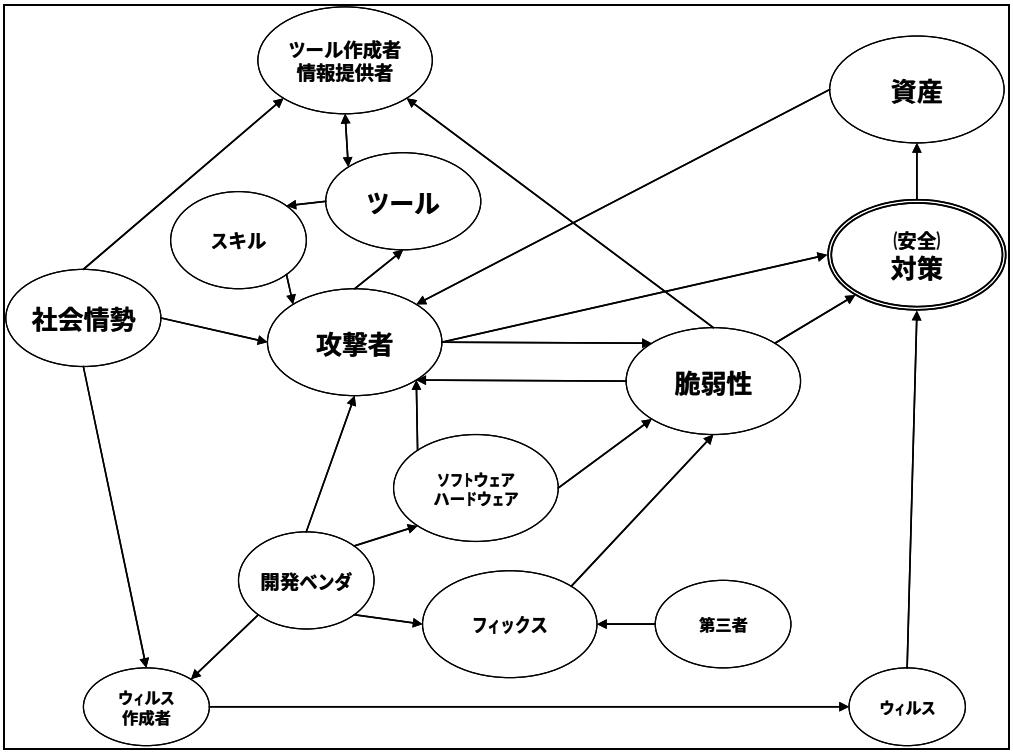


図 3-2 セキュリティリスクモデル（1）

モデル図の作成を進めるに従って、オブジェクト間の矢印に「意味」を与えた方が検討を進めやすいという事実が明らかになり、その結果、「プラスの影響を与える」矢印と「マイナスの影響を与える」矢印の二つの影響を区別して記載することとした。（図 3-3 では、この二種の影響をリンクの色を変えることで表現している。）

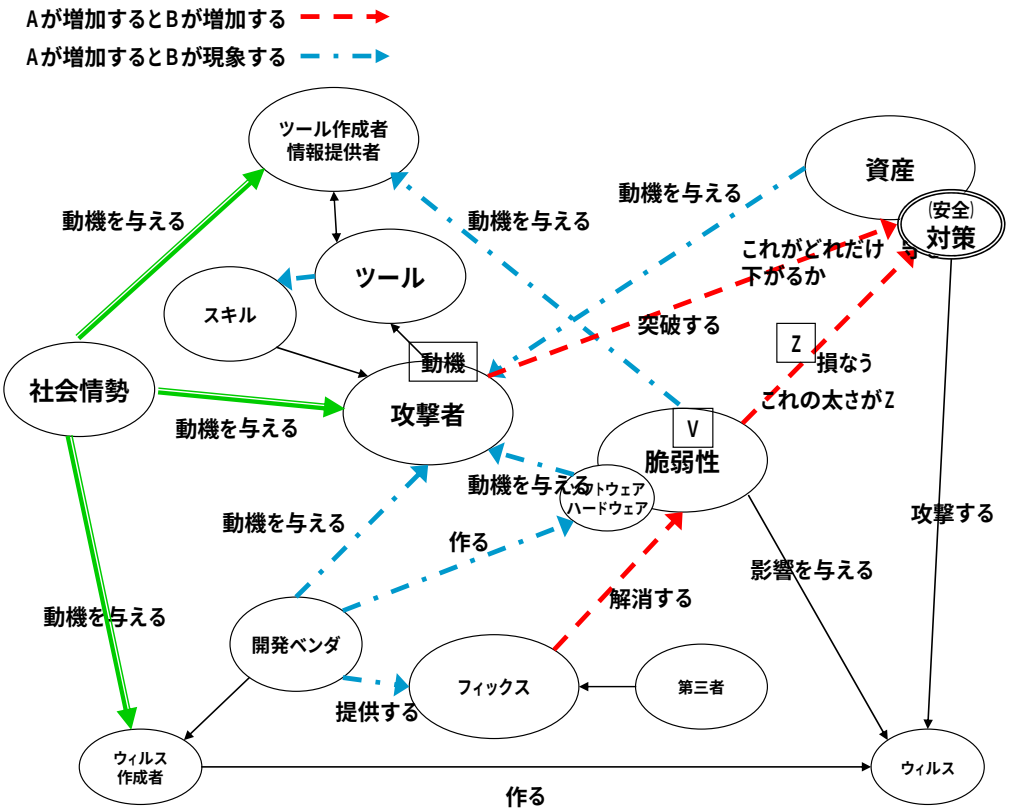


図 3-3 セキュリティリスクモデル（2）

さらに、各オブジェクトには、管理者にとって「好ましい」オブジェクトと「好ましくない」オブジェクトが存在するという考えに至り、これらを区別するために色分けを行った。また、前段の検討で定義した矢印の「増加」「減少」も、「好ましい」影響と「好ましくない」影響という観点で記述することができるので、これに合わせた色分けの見直しを行った。

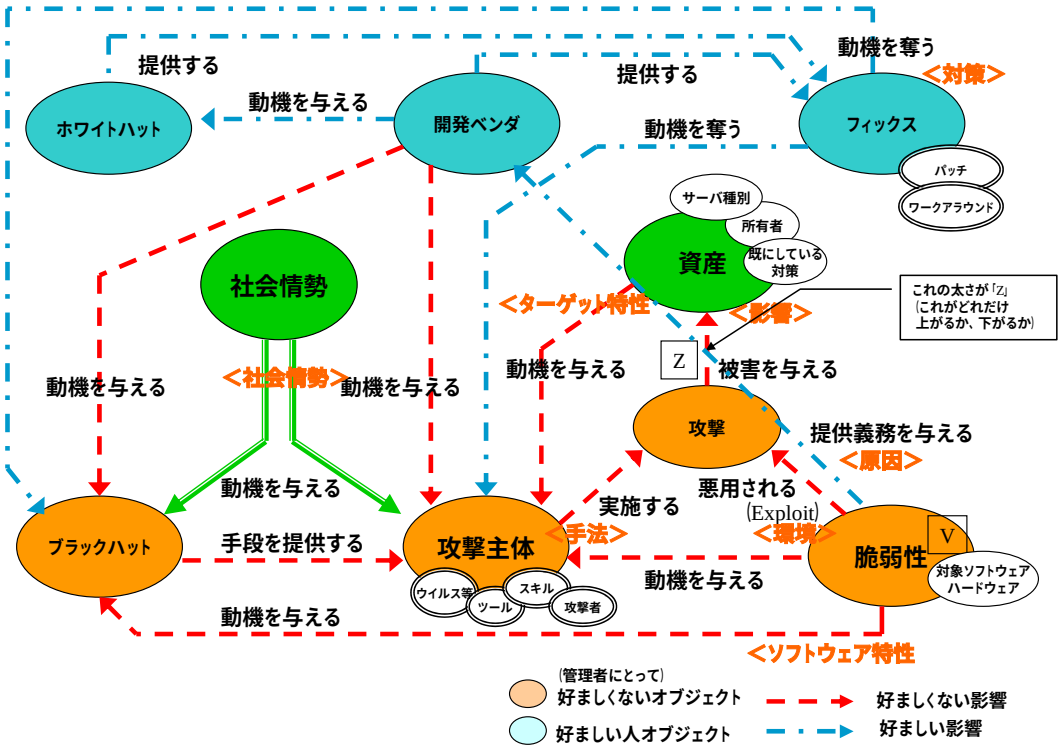


図 3-4 セキュリティリスクモデル（3）

これらのオブジェクトの関係は、同時に発生するのではなく、実際に脆弱性が発見されてから、いくつかの段階（ステージ）を経た後に、管理者の資産に影響が出るものである。これを、「脆弱性発生のステージ（1st ステージ）」、「世の中の動きのステージ（2nd ステージ）」「資産に影響のステージ（3rd ステージ）」の三つのに分けて考え、モデルに反映させた。

その結果、最終的に導き出されたものが、「攻撃発生のメカニズム」を表す、以下の図となった。

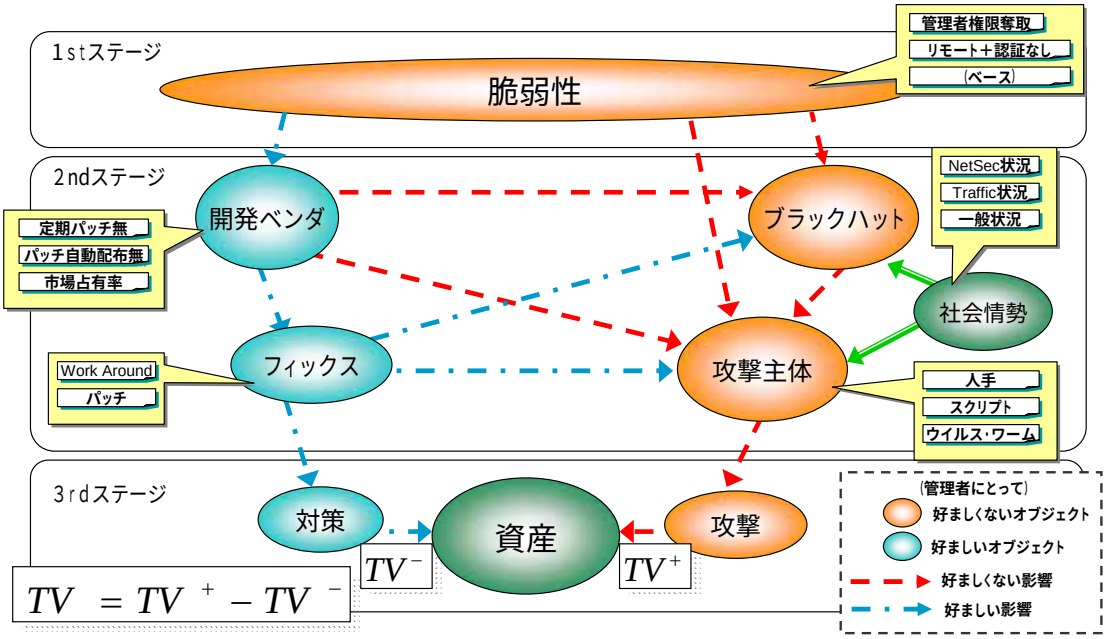


図 3-5 セキュリティリスクモデル（4）

3.2 オブジェクト間の関係

それぞれのオブジェクト間の関係性は、例えば、「脆弱性は、開発ベンダに、動機を与える」、「脆弱性は、ブラックハットに、動機を与える」、「ブラックハットは、攻撃主体に、手段を提供する」、「開発ベンダは、フィックスを、提供する」、「フィックスは、ブラックハットから、動機を奪う」といったものである。

これらを定義することによって、一般に言われている リスク＝脆弱性×脅威×資産 という式が表すものとは違う、リスクが発生する仕組みの、その背景までを説明するモデルを作成した点に、本 WG の取組みの特徴があるといえる。

4 トリアージ値の定量化

前章で示した攻撃のメカニズムを基に、本章ではトリアージ値（*TV*）の定量化を検討する。図 3-5 の示すメカニズムに従って考えた場合、オブジェクト間の関係性やオブジェクト自体は、以下のよう特徴を持つことがわかる。

(a) **オブジェクトは、他のオブジェクト群からの影響を受ける（他のオブジェクトから矢印が伸びている）**

(b) **オブジェクトは、自オブジェクトの属性を持つ**

(c) **オブジェクトは、他のオブジェクトへ影響を与える（他のオブジェクトへ矢印が伸びている）**

図 4-1 はそれを図示したものである。

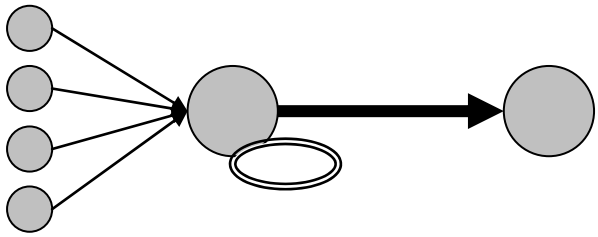


図 4-1 一般的なオブジェクト間の関係

したがって、図 3-1 の攻撃メカニズムは、図 4-1 の一般的なオブジェクトの関連が複数組み合わさって出来上がっているものと考えることができる。

TV の算定にあたり、まず図 4-1 の一般的なオブジェクトに関して数式モデルを検討し、攻撃メカニズムにあわせそれらを組み合わせることで、この値を求めるアプローチを取った。

以下、4.1 節では、一般的なオブジェクトに関する数式モデルについて解説をし、4.2 節では数式モデルで利用する数値の調整方法に関して解説する

4.1 定量化に用いた数式モデル

本節では、図 4-1 で示した一般的なオブジェクトに関する数式モデルを議論する。

TV の数値化の基本方針として、攻撃メカニズムの図上にある各矢印が値を持ち、最終的にそれが「資産」に与える影響の合計をトリアージ値とすることとした。個々のオブジェクトに関して一般化して表したものが図 4-2 である。ここでは矢印の値を d と表現し、特にオブジェクト i からオブジェクト j への矢印を $d_{i\to j}$ と表すこととした。また、オブジェクトが持つ属性を λ と表した。図 4-2 にこれらを反映したオブジェクトのモデルを示す。

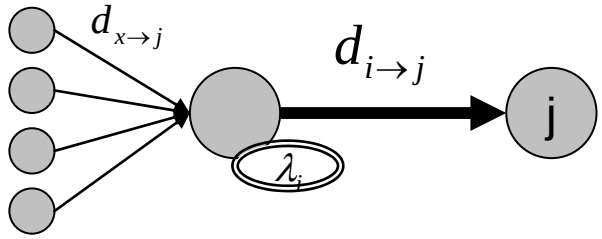


図 4-2 一般的オブジェクト表現モデル

$d_{i\to j}$ は、i へと入ってくる各オブジェクトと、自身が持つ属性群 λ、また影響を与える対象であるオブジェクト j に依存する値であることから、一般式として以下の式が得られる。

$$d_{i\to j} = f\left(d_{x_1}, d_{x_2}, \Lambda, d_{x_m}, \lambda_{y_1}, \lambda_{y_2}, \Lambda, \lambda_{y_n}, j\right)$$

関数 f は、それぞれの入力があった場合の処理方法であり、さまざまな形が考えられるが、ここでは最も単純なものとして、オブジェクトに入ってくる矢印の総和と、属性値の和に対して、影響を与える対象であるオブジェクト j に関する重みを掛け合わせる形を取った。

$$d_{i\to j} = w_{i\to j}\left(\sum_x d_{x\to i} + \sum_y \lambda_y\right)$$

この数式を攻撃メカニズムに適用することによって、最終的にメカニズム中の「資産」に影響を与える矢印の和を求めることで、本 WG で求めるトリアージ値（*TV*）が求められる。

矢印の和を求めるにあたって、我々が調整しなければならない値は、各オブジェクト間での重みと、各オブジェクトが持つ属性値である。図 4-3 にオブジェクト「フィックス」における w と λ の関係性を示す。

$$d_{i\to j} = w_{i\to j}\left(\sum_{a} d_{a\to i} + \lambda_i\right)$$

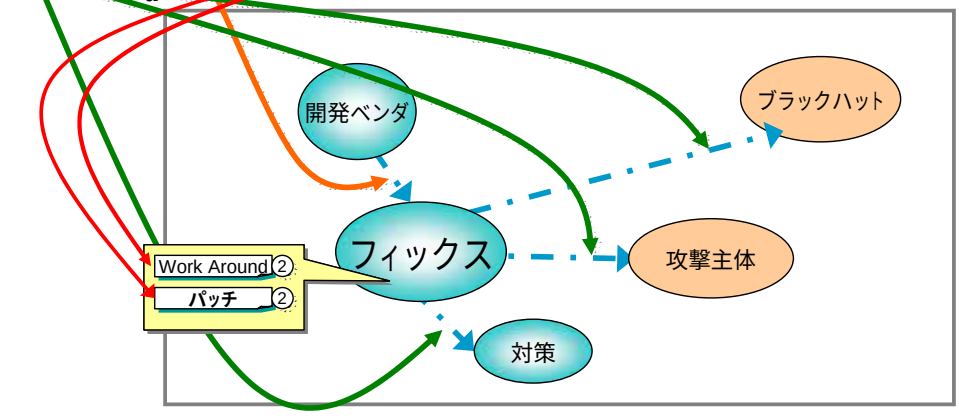


図 4-3 オブジェクトと数式の関係

まず、オブジェクト「フィックス」が影響を受けるオブジェクトは「開発ベンダ」のみである。

$$d_{i\to j} = w_{i\to j}\left(\sum_{a} d_{a\to i} + \lambda_i\right)$$

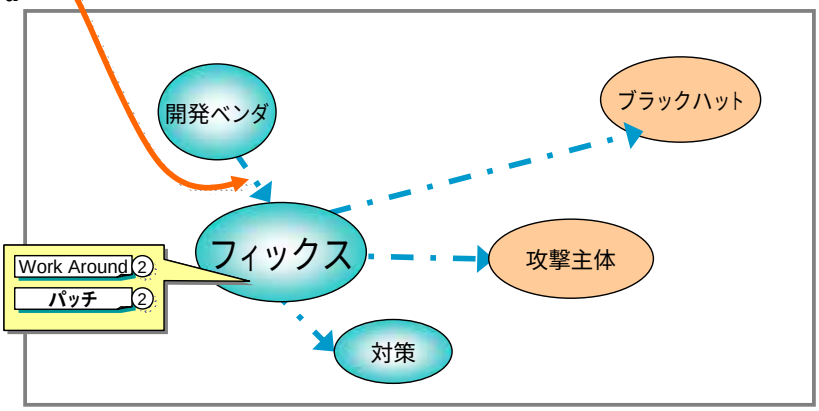


図 4-4 「フィックス」が影響を受けるオブジェクト

また、オブジェクト「フィックス」は自身の属性として「Work Around」「パッチ」を持つ。

$$d_{i\to j} = w_{i\to j}\left(\sum_{a} d_{a\to i} + \lambda_i\right)$$

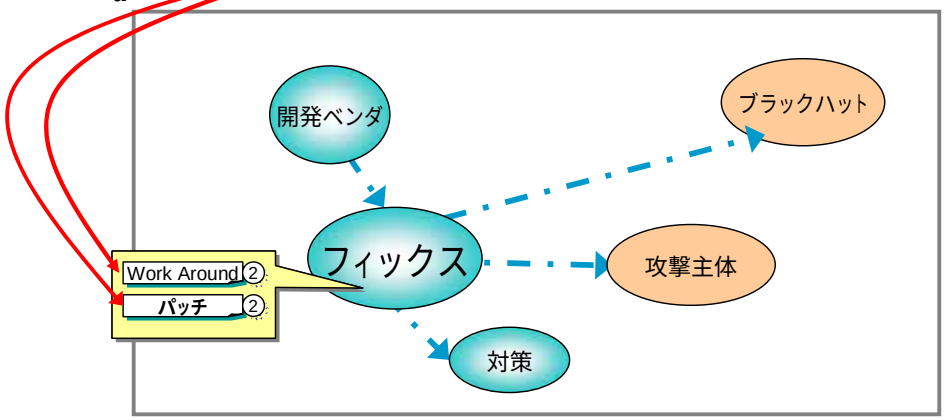


図 4-5 「フィックス」が持つ属性

そして「フィックス」は「ブラックハット」「攻撃主体」「対策」に対して影響を及ぼす。

$$d_{i\to j} = w_{i\to j}\left(\sum_{a} d_{a\to i} + \lambda_i\right)$$

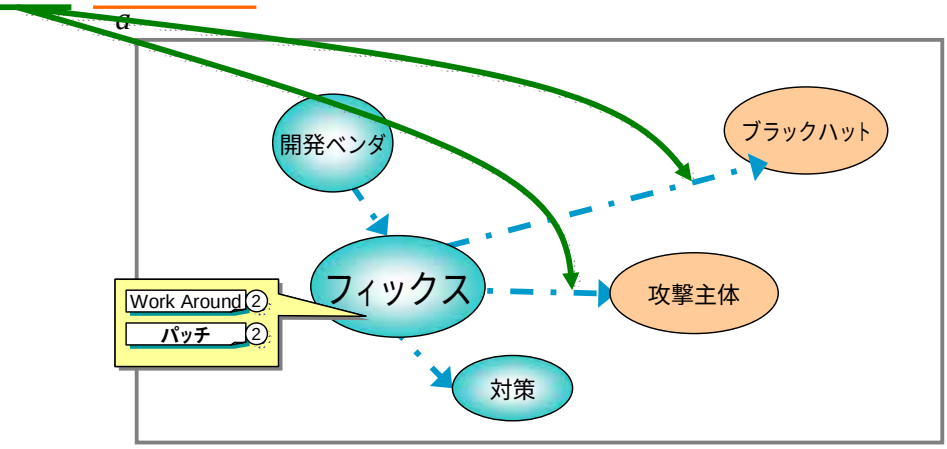


図 4-6 「フィックス」が影響を及ぼすオブジェクト

以上によって、総和を求めることができる。

4.2 数値調整方法

各オブジェクト間での重み w と、各オブジェクトが持つ属性値 λ を調整するにあたり、本 WG ではメンバー間の議論の結果から、それぞれの値を定義した。その値を暫定値として、いくつかの事例に基づいた数値を挙げ、議論を行い、さらに値の修正をかけていった。

4.3 数値化パラメータ

本節では、トリアージ値（*TV*）の数値化に利用する各パラメータの値を示す。4.3.1 節で属性値λのパラメータを示し、4.3.2 節でオブジェクト間の重みwを示す。また、

4.3.1 属性値

属性値のパラメータを表 4-1 に示す。項目「脆弱性」にある「(ベース)」は、常に 1 となる固定の値である。トリアージ値（*TV*）を求めるために、「管理者権限奪取可能」と「リモートからの認証なし利用可能」の有無が属性として存在するが、双方の属性が無い場合でもある程度の危険度を持つであろうという認識より、基本となる値として「(ベース)」を設定した。

また項目「攻撃主体」では、「ウイルス・ワーム」がある状態で「攻撃用ツール」が存在しないということは無いことから、このような前提のもとでの値ととして設定されている。そのために「ウイルス・ワーム」が存在するということは、同時に「人手」と「攻撃用ツール」の利用もあるということになる。「攻撃用ツール」がある場合も、同時に「人手」の利用もあるという設定になる。この考え方は項目「フィックス」にも適用されている。「パッチが存在する」という属性は、「ワークアラウンドが存在する」という属性を含んでいるという考え方である。

表 4-1 属性値パラメータ

項目	属性	入力値	属性値λ
脆弱性	（ベース）	常に 1	1
	管理者権限奪取可能	0 or 1	2
	リモートからの認証なし利用可能	0 or 1	2
攻撃主体	人手	常に 1	3
	攻撃用ツール	0 or 1	18
	ウイルス・ワーム	0 or 1	24
開発ベンダ	定期的なパッチ提供がない	0 or 1	2
	パッチ自動配布機能が無い	0 or 1	2
	市場占有率	0 – 4	0.25
フィックス	ワークアラウンドが存在する	0 or 1	2

	パッチが存在する	0 or 1	2
社会情勢	ネットワークセキュリティの状況	0 – 3	0.5
	ネットワークのトラフィック状況	0 – 2	0.5
	世の中の一般的安全状況	0 – 4	0.25

4.3.2 オブジェクト間の重み

オブジェクト間の重みを表 4-2 に示す。 表中の空欄はオブジェクト間に関連が無いことを示している。また赤字は図 3-5 の「好ましくない影響」のオブジェクトであり矢印が赤であるものを示し、同様に青字は「好ましい影響」を示すオブジェクトである。実際に計算する際には、トリアージ値（*TV*）の増減が適切になるように±が付される。

表 4-2 オブジェクト間の重み

	脆弱性	社会情勢	開発ベンダ	フィックス	ブラックハット	資産	攻撃主体	対策	攻撃
脆弱性			2.4		2.4		0.6		
社会情勢					0.8		0.6		
開発ベンダ				1.2	2.4		1.8		
フィックス					0.8		0.6	0.4	
ブラックハット							1.2		
資産									
攻撃主体									0.8
対策						1			
攻撃						1			

表 4-3 パラメータ付きセキュリティリスクモデル

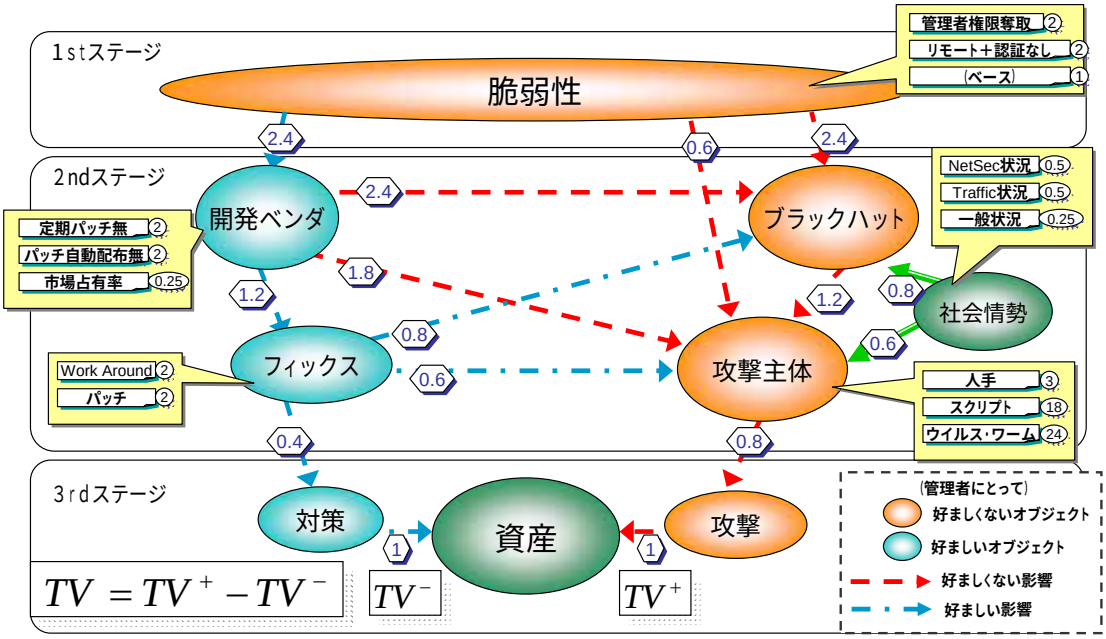


図 4-7 パラメータ付き攻撃モデル図

4.4 プロトタイプ版の数値計算ツール

本 WG では、得られた重みと属性値を用いてトリアージ値（*TV*）を計算するツールのプロトタイプ版を作成した。ツールは Excel シート上で作成されたものであり、ユーザが脆弱性に関連する事項を入力することで値が自動的に計算される。概観を図 7 に示す。ユーザにより入力がされると、各オブジェクト間での重みに従った計算が行われ、トリアージ値（*TV*）が示される。ツールは各オブジェクト間での重みを設定した表を持つ。

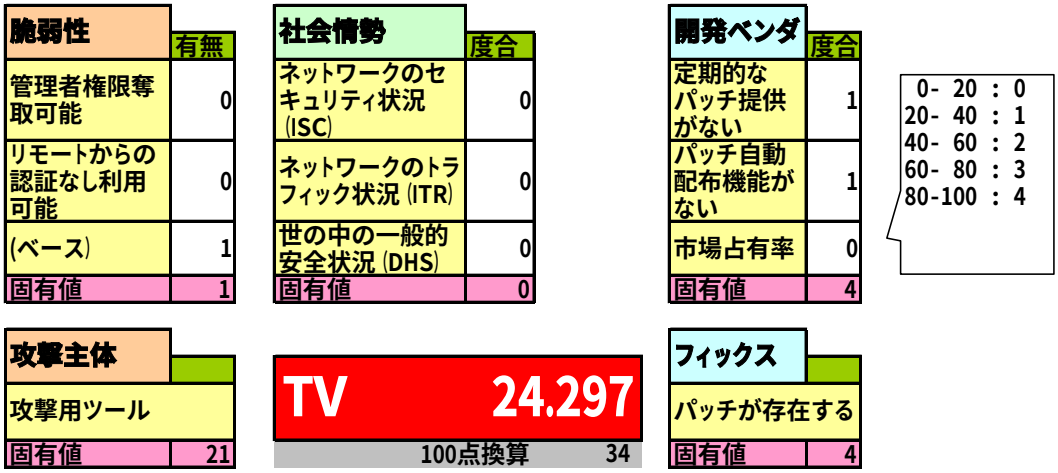


図 4-8 TV 算出ツール概観

			Destination																									
		固有値	脆弱性		社会情勢		開発ベンダ		フィックス		ブラックハット		資産		攻撃主体		対策		攻撃									
	到達オブジェクトの特		1	矢	1	矢	-1	矢印	-1	矢印	1	矢印	1	矢印	1	矢印	-1	矢印	1	矢印								
Source	脆弱性	5	0	0	0	0	2.4	-1	0	0	2.4	1	0	0	0.6	1	0	0	0	1								
	社会情勢	0	0	0	0	0	0	0	0	0	0.8	1	0	0	0.6	1	0	0	0	0								
	開発ベンダ	5	0	0	0	0	0	0	1.2	-1	2.4	1	0	0	1.8	1	0	0	0	0								
	フィックス	4	0	0	0	0	0	0	0	0	0.8	-1	0	0	0.6	-1	0.4	-1	0	0								
	ブラックハット	0	0	0	0	0	0	0	0	0	0	0	0	0	1.2	1	0	0	0	0								
	資産	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0								
	攻撃主体	45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.8	1								
	対策	0	0	0	0	0	0	0	0	0	0	0	1	-1	0	0	0	0	0	0								
	攻撃	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0								

図 4-9 オブジェクト間重みの設定表

5　トリアージ値の評価

本章では、4 章において求められたトリアージ値（*TV*）の評価を行った結果について説明する。評価としては、客観的な情報を得るためにアンケートを行った。

5.1　アンケート概要

アンケートは、ある脆弱性について、対象となる OS やソフトウェアの情報や、それらをめぐる状況・影響を詳細に記述した情報をもとに、危険度を 7 段階で回答する形式のものを用意した。アンケートは 30 の設問から成るものであり、Web 画面から回答できる形式の「Web アンケート」として公開した。この Web アンケートは JNSA（日本ネットワークセキュリティ協会）の Web サイト内に設置された。アンケートの対象は「サーバ管理者」とし、2006 年 10 月 11 日より 11 月 20 日の 41 日の間に回答の受付を行った。この期間中に得られたアンケートの回収数は 50 であり、そのうち重複回答を除くなどして得られた有効回答数は 44 であった。アンケートの詳細に関しては付録に記載する。

アンケートで示される各脆弱性の説明については、文面だけでは記述が分かりにくいことから、その特性（属性）の理解を容易にすべく、各設問について表 5-1 のような表を付記した。また、アンケート各設問の選択肢は 0 から 6 までの 7 段階の危険度とした。各危険度を示す凡例を表 5-2 に示す。

表 5-1 脆弱性の特性情報を示す表

項目		特性情報
脆弱性	管理者権限の奪取が可能	○ or ×
	リモートから認証なしで利用が可能	○ or ×
攻撃状況		ウイルス・ワームが存在する/攻撃用ツールが存在する/ウイルス・ワーム、攻撃用ツール共に無し
対策状況		パッチあり/パッチ無し・回避策あり/パッチ・回避策共に無し
社会状況	ネット上の危険度	0～3
	ネットのトラフィック	0～2
	社会全体のセキュリティ	0～4

表 5-2 アンケート回答の選択肢

レベル		凡例
レベル 6	今すぐ対処	運用中のサーバを今すぐ停止してでも対処が必要
レベル 5	今日中に対処	今夜のデートを断ってでも今日中に対処
レベル 4	2～3 日中に対処	２～3 日中に対処する
レベル 3	今週末に対処	今週末に対処する
レベル 2	数ヶ月先に対処	次の定期保守等の機会（数ヶ月先を想定）に対処する
レベル 1	年内に対処	次回システム更新時／バージョンアップ等（年内を想定）に対処する
レベル 0	対策しない	対策を実施しない

以下は、本アンケートの内容の例である。

アンケート文例

- Microsoft 社の Windows Kernel に脆弱性が発見されました。
- この脆弱性により、管理者の権限が第三者により取得される可能性はありません。また、この脆弱性は、ネットワークを介して、認証を経ずして利用することはできません。
- 現在、この脆弱性を悪用するウイルスやワームが存在します。
- 対策として、Microsoft 社よりパッチが提供されています。
- また、関連する社会的状況として以下の情報があります。
- インターネット上の危険度を示す Infocon は緑（4 段階中の上から 4 番目）
- インターネット上のトラフィック状況を示す ITR の日本は赤（3 段階中の上から 1 番目）
- 米国の国土安全保障省のセキュリティレベルは High（5 段階中の上から 2 番目）

5.2 アンケート結果分析概要

本節ではアンケートで得られた結果の統計的分析を概説する。分析の詳細については付録 A を参照されたい。

まずアンケート回答の全体傾向を見ていく。表 5-3 はアンケート全体での対処レベルの回答分布を示している。すべての対処レベルについて回答を得られており、それが対処レベル 3 を中心とした山型の回答分布になっている状況がわかる。

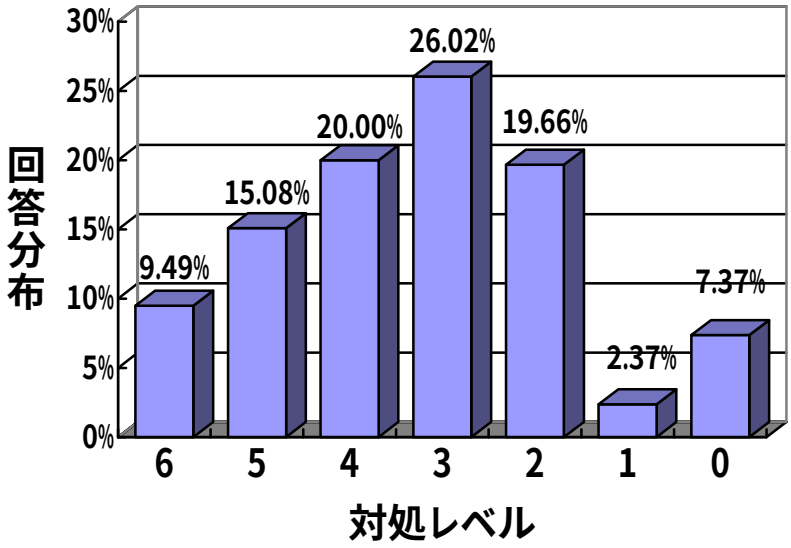


図 5-1 アンケート全体の回答分布

表 5-3 は、それぞれの設問に対し、回答者がどういった対処レベルを選択したかの分布を示す表となっている。

表 5-3 アンケート回答分布

	対処レベル						
	6	5	4	3	2	1	0
Q1	8	11	11	6	6	0	0
Q2	3	10	7	11	10	0	1
Q3	12	9	13	5	2	0	0
Q4	2	4	4	18	11	1	2
Q5	6	7	6	14	8	0	0

Q6	3	1	7	13	9	2	3
Q7	1	5	10	13	8	1	2
Q8	4	7	13	8	5	2	1
Q9	0	4	4	17	13	0	0
Q10	1	3	4	16	12	2	1
Q11	1	7	14	12	3	1	1
Q12	3	5	9	7	6	1	7
Q13	5	4	7	2	10	4	7
Q14	5	7	11	12	4	0	1
Q15	1	4	8	4	13	2	7
Q16	13	7	8	8	2	0	1
Q17	2	7	13	10	3	0	3
Q18	2	6	3	14	10	1	3
Q19	3	6	7	13	6	1	3
Q20	2	7	3	15	7	2	3
Q21	3	9	5	6	8	0	7
Q22	5	8	9	13	5	0	1
Q23	4	6	8	8	8	1	3
Q24	3	4	10	4	9	0	9
Q25	1	1	3	6	14	1	11
Q26	4	9	7	7	13	0	0
Q27	1	2	5	13	13	3	2
Q28	4	9	7	10	3	1	4
Q29	5	4	11	10	6	0	2
Q30	5	5	9	12	5	2	2

5.3 **アンケート結果とトリアージ値（TV）の比較**

本節では 5.2 節で得られたアンケートの結果とトリアージ値の比較を行う。まず表 5-3 のアンケートの回答分布より、回答者の平均対処レベルを設問ごとに求めた。そして、それぞれの脆弱性に対してトリアージ値（*TV* ）を求め、平均対処レベルとトリアージの散布図を作成した。図 5-2 に散布図を示す。

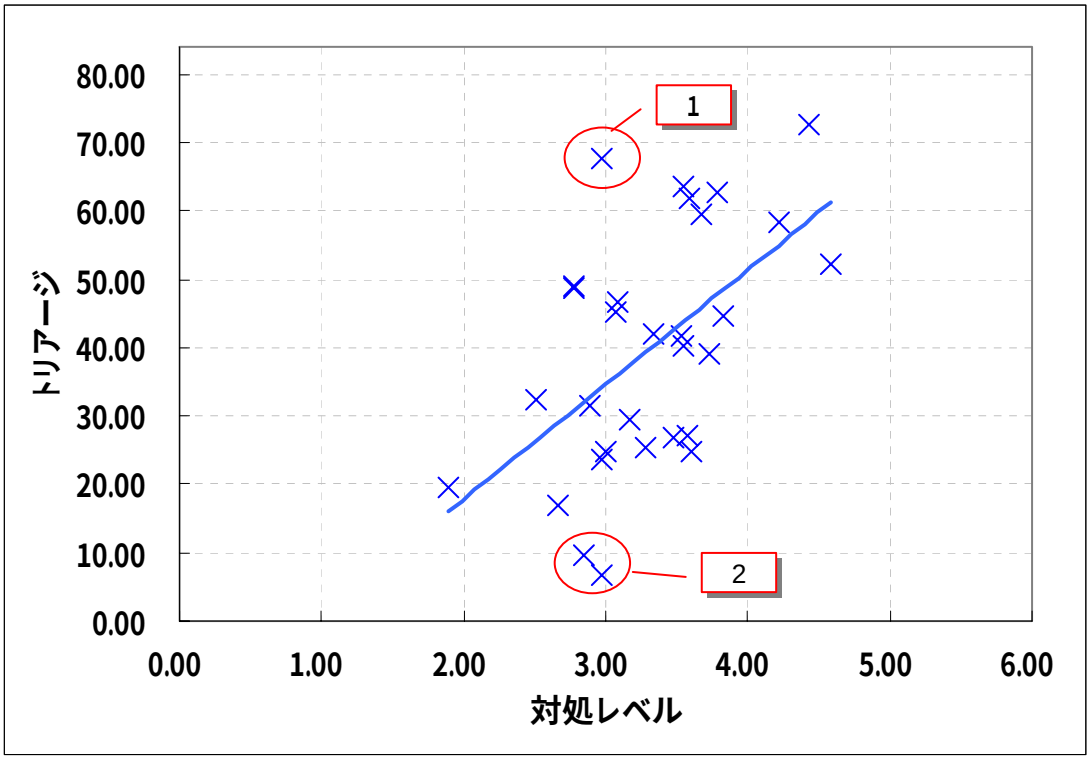


図 5-2 アンケート結果とトリアージの関係

図 5-2 の散布図には、線形近似を行った結果の直線も記入している。これら 2 つのデータ列の相関係数は 0.54 であった。相関係数とは-1 から 1 を取る値であり、1 に近いときには 2 つのデータ列に正の相関があることを示す値である。ここでは相関係数の値が 0.54 であったことから、回答者の対処レベルとトリアージとの間に正の相関があり、トリアージが脆弱性に対する回答者の対処意識と近いものを示していることが言える。

次に、図 5-2 中の特異点に注目してみる。散布図中の各点と線形近似の直線をみた時に、直線から目だって離れた点があることがわかる。図中にはそれをわかりやすくするために円で囲み数字をつけている。特異点として挙げたのは全部で 3 点であり、お互いが近い 2 点をまとめて円で囲んでいる。まず「1」の囲みを見ていこう。これは Q12 についての点である。平均の対処レベルは 2.94 であるのに比べ、トリアージは 67.64 と全設問の中で 2 番目に高いものとなっている。Q12 は Samba の脆弱性に関するものである。表 5-4 に Q12 の脆弱性特性を示す。

Q12 は脆弱性特性だけをみると、リモートから認証を経ずして脆弱性を利用した攻撃を行うことが可能であり、既にウイルス・ワームが存在している状態であり、さらにパッチや回避策がない状態、と状況としてはかなり悪いといえよう。トリアージではそういった危険性が反映され、67.64 と高い値をだしている。しかし脆弱性を持つ対象が Samba であり、これは社内 LAN 内のようなファイアウォールで守られた安全な場所で利用される場合が多い。このため、インターネット

に接する環境の管理者は、回答として低い点数をつける傾向があったことが考えられる。

表 5-4 Q12 の脆弱性特性

項目		Q12：Samba
脆弱性	管理者権限奪取可能	×
	リモートから認証なしで利用可能	○
攻撃状況		ウイルス・ワーム
対策状況		パッチ・回避策共に無し
社会状況	ネット上の危険度	2
	ネットのトラフィック	1
	社会全体のセキュリティ	1

逆の状況が「2」の囲みでもみることができる。「2」の囲みは Q4 と Q10 についての点である。Q4 は平均対処レベルが 2.98 であり、全回答の平均対処レベル 3.31 に近い値であるが、トリアージは 6.78 と全設問中でもっとも低い値となっている。また Q10 は平均対処レベルが 2.85 であり、トリアージは 9.77 となっている。こちらも平均対処レベルは全回答の平均に近いものの、トリアージは全設問中で 2 番目に小さいものとなっていた。Q4 は Microsoft 社 Windows の脆弱性、Q10 は Microsoft 社 Windows Server Service についての脆弱性に関するものであった。表 5-5 に Q4、Q10 の脆弱性特性を示す。

それぞれの脆弱性特性では、双方ともに管理者権限を取ることはできず、リモートから認証を経ずして脆弱性を利用することはできない。さらに攻撃をするにあたっての補助ツールやウイルス・ワームなどは存在していない。Q4 と Q10 ではパッチと回避策という違いがあるものの、脆弱性属性と攻撃状況を踏まえて双方ともトリアージが低い値となっている。しかし、Q12 と異なり、双方では回答者の平均対処レベルが平均に近いものとなっていた。これら双方の脆弱性が Microsoft 社の Windows に関する脆弱性であったことが、アンケート回答者が高い点数をつける傾向になったことが考えられる。

表 5-5 Q4,Q10 の脆弱性特性

項目		Q.4 Microsoft Windows	Q.10 Microsoft Windows Server Service
脆弱性	管理者権限奪取可能	×	×
	リモートから認証なしで利用可能	×	×
攻撃状況		人手	人手
対策状況		パッチあり	回避策あり
社会状況	ネット上の危険度	2	0
	ネットのトラフィック	0	2
	社会全体のセキュリティ	3	2

これら 3 つの特異点より、脆弱性の対象の認知度や普及度といったものがアンケート回答者の対処レベル決定に関わっていることが考えられる。

その仮定を検証すべく、別の 2 つの脆弱性を比較してみた。ここでは、もっとも顕著に見えている例として Q.4 の Microsoft 社 Windows に関する脆弱性のものと、Q.25 の IBM 社 Tivoli Directory Server の脆弱性のものを取り上げる。双方の脆弱性はともに「管理者権限奪取可能」と「リモートからの認証なし利用可能」が共に×であり、攻撃状況も同じとなっている。通常であればこれら 2 つの対処レベルは非常に近いものになることが考えられる（表 5-6）。しかし実際に分布をみるとその違いは大きい（図 5-3）。これら 2 つの例をみても、対象となっている製品やベンダに依存した脆弱性の評価がされていることがわかる。

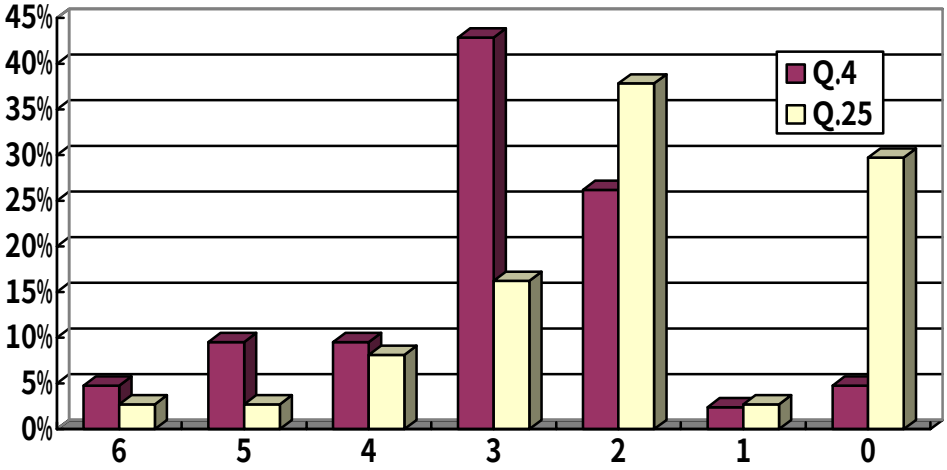


図 5-3 製品・ベンダに依存した対処レベル例

表 5-6 Q4,Q25 の脆弱性特性

項目		Q.4 Microsoft Windows	Q.25 IBM Tivoli Directory Server
脆弱性	管理者権限奪取可能	×	×
	リモートから認証なしで利用可能	×	×
攻撃状況		人手	人手
対策状況		パッチあり	パッチ、回避策共に無し
社会状況	ネット上の危険度	2	2
	ネットのトラフィック	0	2
	社会全体のセキュリティ	3	2

これら 3 つの特異点を除いてあらためて相関係数を求めてみると、0.60 となり高い相関があることがわかった。

以上述べてきたように、トリアージ値とアンケート回答の対処レベルには相関があることがわかった。しかし一方では、強い相関とは言えない側面もある。それは、ベンダ・製品など脆弱性の対象となっているものの認知度や適用範囲、さらには脆弱性対象に関する情報の流通度合などが、対処レベルを決定する要素として影響を与えていることが十分に考えられるということである。

WG では、これらの結果を踏まえて改めてトリアージ値計算方法の再検討を行ったが、しかし、ベンダ・製品といったものの影響度を組み入れることは行わなかった。

理由は、アンケート回答が必ずしも脆弱性対処のあるべき姿を反映したものではないということである。図 5-3 に示すように、ベンダや製品によりアンケート回答者の対処レベル分布は異なっているが、これは本来のあるべき姿ではないと WG としては判断した。つまり、その脆弱性の特性が危険であれば、そのベンダ・製品がどうであれ対処は公平にされるのが本来の脆弱性対処のあるべき姿なのではないだろうかということである。このような理由から、WG としては、ベンダ・製品による影響を再検討して、より大きな影響を持つものとして組み入れることは行わなかった。

6 まとめ

以上に述べてきたように、本 WG では、脆弱性定量化の検討を開始するにあたって、まず、はじめに、「脆弱性とは何か？」という検討を行った。そして、その上で、脆弱性の発生メカニズムのモデル化を行い、モデル図を作成した。

このように、モデル図を元にした数値化を試みた点に、本WGの特徴があると考える。

さらに、このモデル図に基づいたトリアージ値の計算ツールを作成し、その結果を検証するためにアンケートを実施し、その結果と、求められた数値との間の相関関係について検証を行った。

本WGで作成したモデル図は、それ自体に何らかの入力があった場合、これを変化させる、いわば「アンプ（amplifier）」、あるいは「アッテネータ（attenuator）」の機能を有するといえる。したがって、この仕組みを、他の数値化モデルと組み合わせることも可能である。

たとえば、CVSS で言えば基本評価基準(Base Metrics)の部分を入力とすることも可能であり、それによって、CVSS での現状評価基準(Temporal Metrics) や環境評価基準(Environmental Metrics)に代わるものを導き出すことも可能であると考える。

今後の課題として、このように、本WGで検討した結果を、既存の数値を変化させる仕組みとしての応用を検討することが考えられるだろう。

付録A アンケート結果分析

本節ではアンケートで得られた結果を統計的に分析する。まずアンケート回答の全体傾向を見ていく。図 6-1 はアンケート全体での対処レベルの回答分布を示している。対処レベル 0、1 の部分が崩れているものの、対処レベル 3 を中心とした山型の回答分布になっている状況がうかがえる。一般に、連続値や段階評価を求めた場合、統計として見ると中央値（あるいは平均値）付近を中心に山型となった分布を得られることは自然なことであるが、ここではもう 1 つの理由も考えられた。

もっとも回答が多かった対処レベル 3 は、対処の程度を「今週末に対処する」と定義したものである。これは、週を単位として仕事のサイクルをつくっている現場が多い現実がうかがえる。ウィークデーの営業日中のシステム・サービス停止などのインパクトを考慮し、よほどの危険な脆弱性でない限り、対処を週末に行うという運用傾向があることうかがえる。

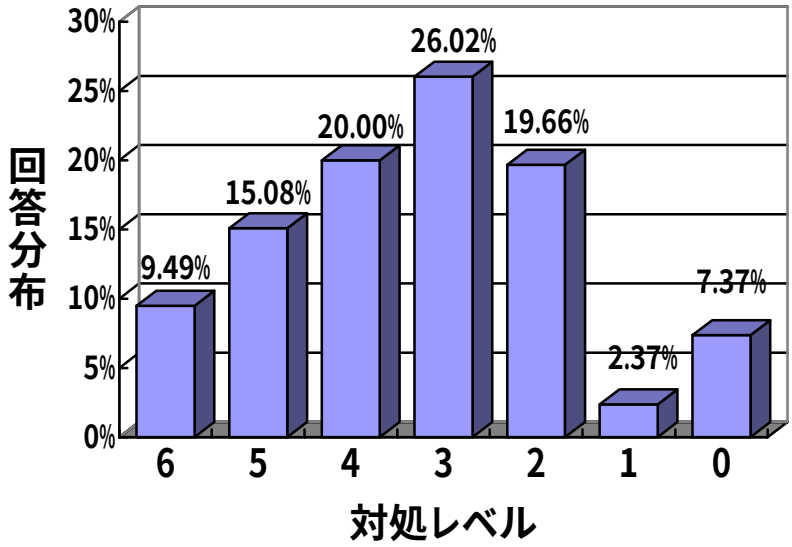


図 6-1 アンケート全体の回答分布

なお、この分布ではレベル 0 が山型を崩していることが特徴的である。これは、「パッチ・回避策共に無し」の場合には、対処をあきらめてしまうという回答がこの部分に含まれているからである。図 6-2 は、対策状況の特性として「パッチ・回避策共に無し」となっている設問すべてに関しての対処レベルの回答分布を示したものである。ここではさらに顕著に 0 が増えていることがわかる。しかし、これは、今後一切対策をしない、という意味とはことなり「現状は対処しない」という意味合いを含んだものとなっていることも考えられる。

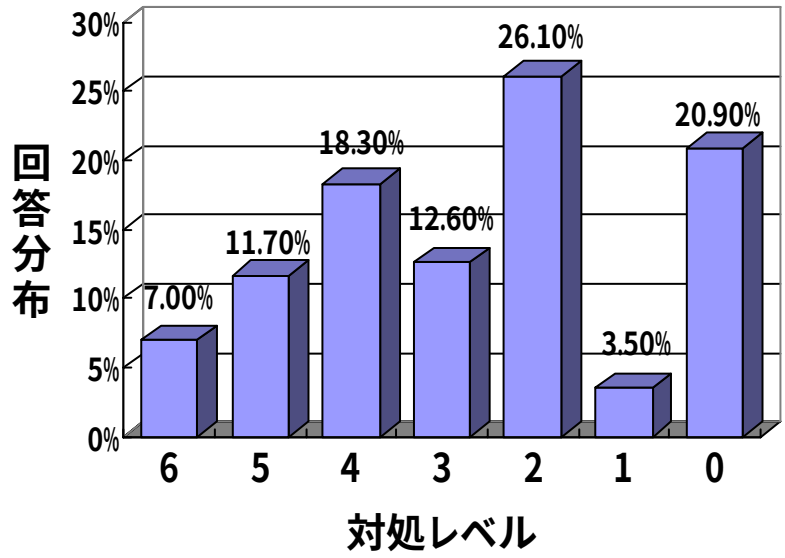


図 6-2 パッチ/回避策なしでの回答分布

つぎに、各特性（属性）による回答分布の違いを見ていこう。まず「脆弱性」の 2 つの属性「管理者権限奪取可能」と「リモートからの認証なし利用可能」について分析する。図 6-3、図 6-4 に属性値別の回答分布を示した。それぞれの図には比較対象として図 6-1 で示した全体の回答分布も示してある。

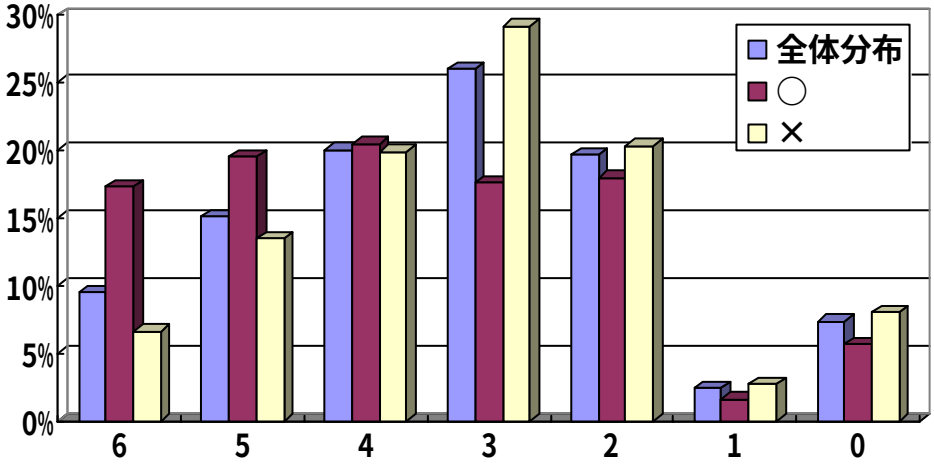


図 6-3 「管理者権限奪取可能」属性別回答分布

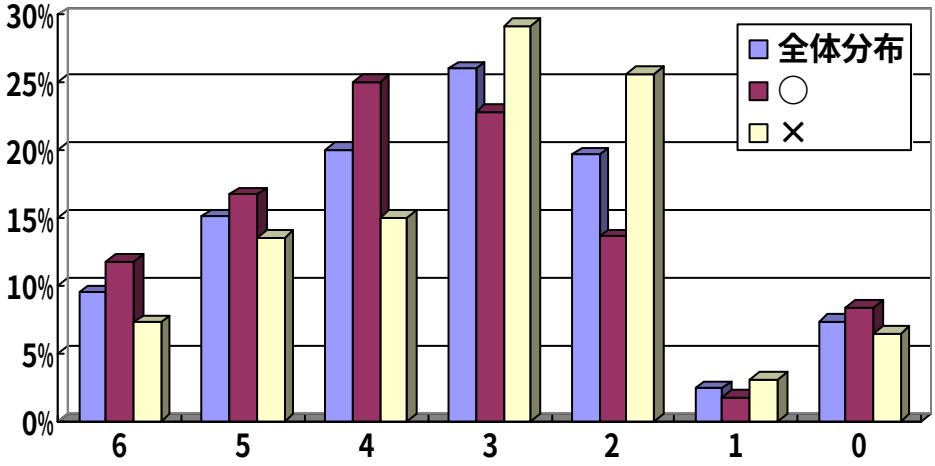


図 6-4 「リモートからの認証なし利用可能」属性別回答分布

図 6-3、図 6-4 の双方において共通することとして、全体分布と比較すると、その属性が○の場合は回答の分布がより対処レベルの高い方に偏っていることが見て取れる。同様に、×の場合は回答の分布がより対処レベルの低い方に偏っていることがある。これら 2 つの属性が、回答者の対処レベルを決定する要素になっていることがわかる。

続いて「攻撃状況」に注目する。図 6-5 にその分布を示す。攻撃状況が「ウイルス・ワーム、攻撃用ツール共に無し（人手)」のものに比較して、「攻撃用ツール」の分布は、より対処レベルの高い方に偏っていることがわかる。同様に「攻撃用ツール」と比較すると「ウイルス・ワーム」の分布がより対処レベルの高い方に偏っていることがわかる。つまり、攻撃状況は、「人手」＜「攻撃用ツール」＜「ウイルス・ワーム」という順序で対処レベルの高低を決定する要素になっていることがわかる。

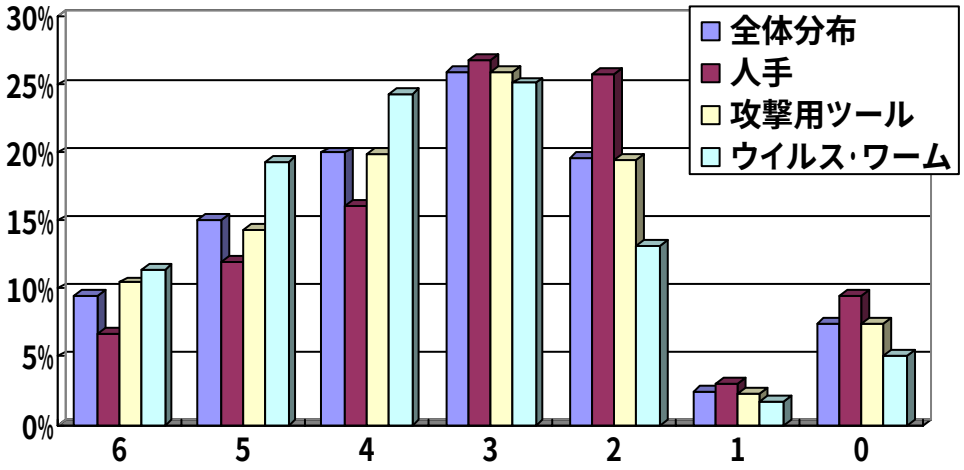


図 6-5 攻撃状況別回答分布

「対策状況」の分布を図 6-6 に示す。先述したように、対策状況が「存在しない」状況では対処レベル 0「対策しない」を選択する回答が多くなっていることがわかる。全体的に見てみると、パッチやワークアラウンドの存在による対処レベルの傾向は、全体分布のものと大きく変わったものではないことがわかる。同様に、対策状況が存在しない場合でも対処レベルが高い方に偏る傾向などは見られない。つまり、パッチあるいはワークアラウンドの存在は、かならずしも対処レベルを決定する要素になっていないという結果となっている。

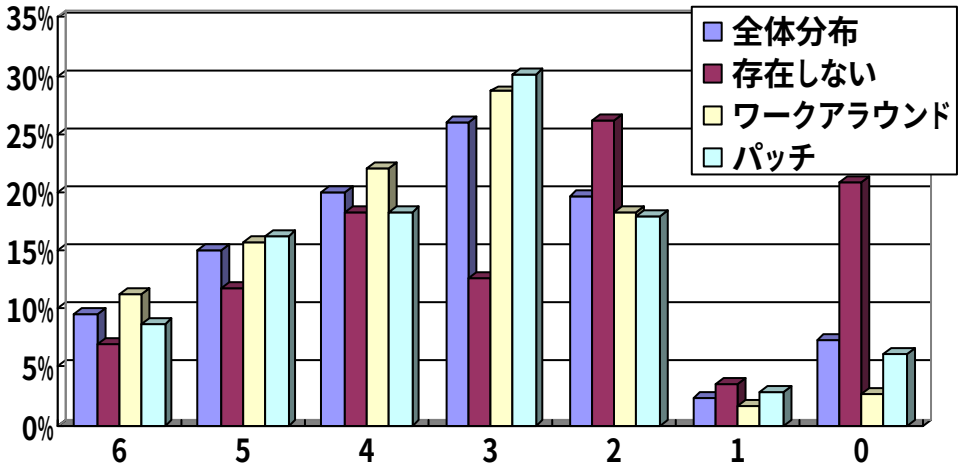


図 6-6 対策状況別回答分布

最後に、「社会的状況」の 3 つの属性「ネット上の危険度」「ネットのトラフィック」「社会全体のセキュリティ」について分析しよう。それぞれの属性別分布を図 6-7、図 6-8、図 6-9 に示す。

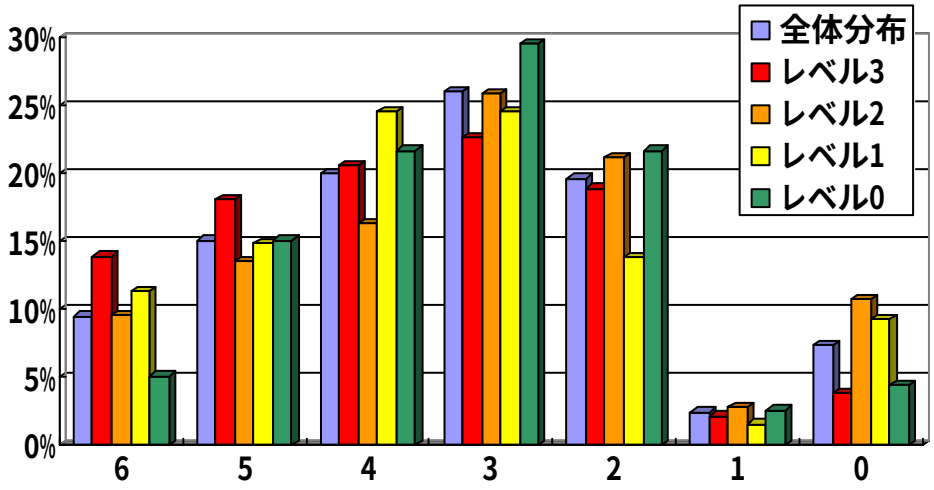


図 6-7 「ネット上の危険度」属性別回答分布

図 6-7 では、レベル 3 とレベル 0 の比較をするとその分布は全体分布を挟み対処レベルの高低が偏っていることがわかる。しかし、レベル 2 やレベル 1 に関しては必ずしもそういった偏向が読み取れるわけではない。顕著な偏向が見て取れないことは、回答者がこの属性に依存した対処レベルの決定を、今回の回答においては行っていないことが考えられる。

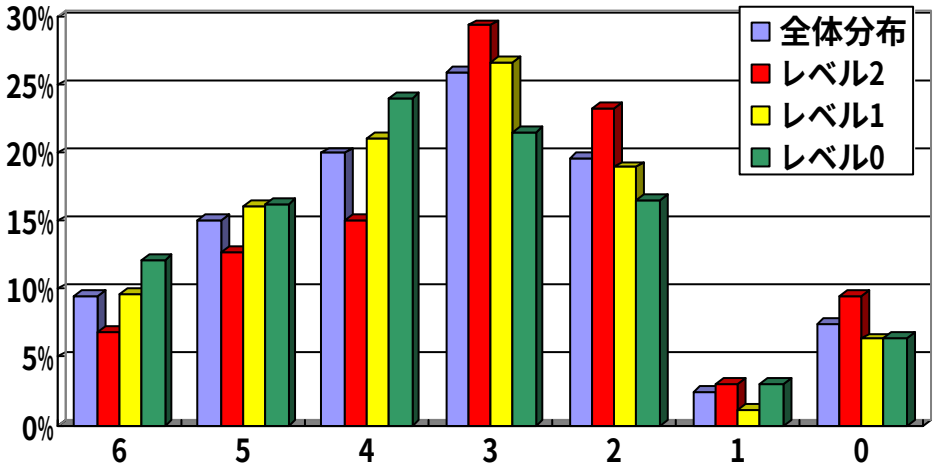


図 6-8 「ネットのトラフィック」属性別回答分布

図 6-8 をみると、高レベルであるほうがより対処レベルの分布が全体と比較して低い方に偏っていることがわかるが、いずれも程度は低く、こちらも対処レベルの決定に強い影響を及ぼしているとは考えにくい。

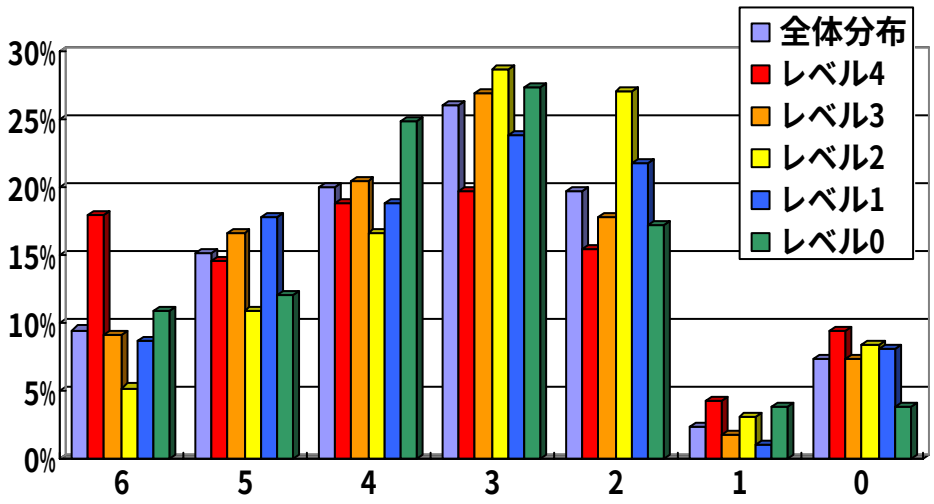


図 6-9 「社会全体のセキュリティ」属性別回答分布

図 6-9 では対処レベル 6 におけるレベル 4 の突出が印象的であるが、それぞれの属性間で大きな偏向が見て取れるわけではない。

社会的状況の 3 つの属性に関しては、脆弱性の属性や攻撃状況と比較すると、回答者が必ずしも対処レベルの決定に利用していないことがうかがえる。これはその属性の定義値を見るとさらに顕著である。たとえば、「ネット上の危険度」の指標として Internet Storm Center の InfoCon を採用しているが、ここでのレベル 3「赤」は、インターネットの大部分が接続不能になっているような状況を示しており、危機的な状況を示しているといってよい。同じくレベル 2 の「オレンジ」も高い危険度を示しており、SQL Slammer ワームが発生した当初や、Code Red が爆発的に広まった時期に設定されており、こちらも相当な危険度でないと設定されないレベルとなっている。しかし、そのレベルが意味する状況と比較して、この回答分布の偏向は小さな範囲での差異でしかないと言ってよいだろう。

付録B CVSS 概要（本 WG の勉強会用に作成した参考資料）

CVSS（Common Vulnerability Scoring System）は、米国家インフラストラクチャ諮問委員会（NIAC: National Infrastructure Advisory Council）のプロジェクトとして 2004 年から検討が進んでいるものであり、その内容は３つの部分、Base Metrics（基本評価基準)、Temporal Metrics（現状評価基)、Environmental Metrics（環境評価基準）に分かれている。

CVSS における定量化の要素

1．Base Metrics ＝ 10 × AV × AC × AT × ((CI × IB) + (II × IB) + (AI × IB))

略称	要素名	意味	要素	係数
AV	Access Vector	脆弱性を遠隔から攻撃できるか	Local: 遠隔から攻撃できない	0.7
			Remote: 遠隔から攻撃できる	1.0
AC	Access Complexity	攻撃が成功するための複合条件	High: 条件がそろわないと成功しない場合がある	0.8
			Low: 常に成功する	1.0
AT	Authentication	脆弱性に攻撃を行う場合に認証が必要か	Required: 必要	0.6
			Not Required: 不必要	1.0
CI	Confidentiality Impact	機密性への影響度	Nome: なし	0
			Partial: 部分的	0.7
			Complete: 全体的	1.0
II	Integrity Impact	完全性への影響度	Nome: なし	0
			Partial: 部分的	0.7
			Complete: 全体的	1.0
AI	Availability Impact	可用性への影響度	Nome: なし	0
			Partial: 部分的	0.7
			Complete: 全体的	1.0

IB: Impact Bias（影響度に対する偏差）			
Nomal	Conf.	Inte.	Avil.
0.333	0.5	0.25	0.25
0.333	0.25	0.5	0.25
0.333	0.25	0.25	0.5

2．Temporal Metrics ＝ Base Metrics × EX × RL × RC

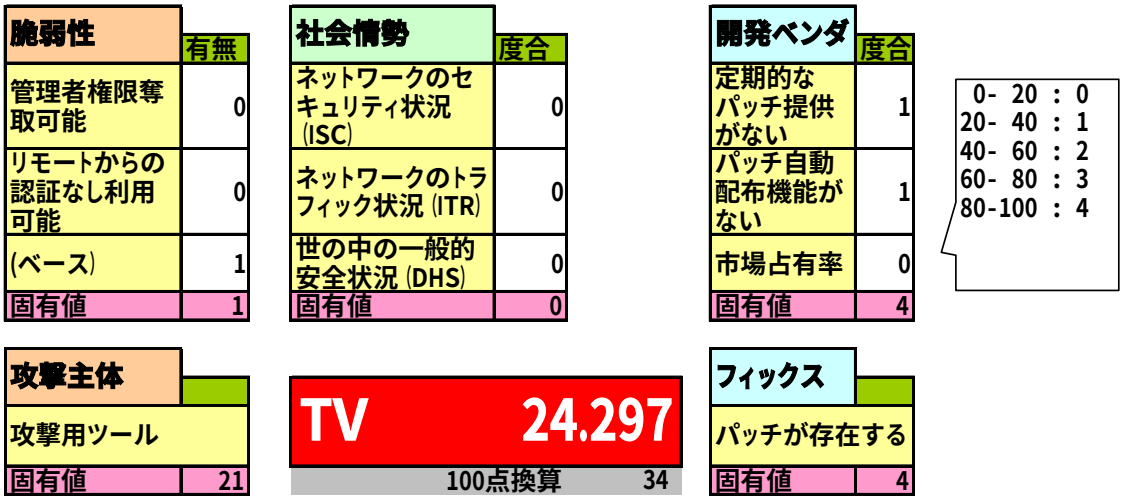
略称	要素名	意味	要素	係数
EX	Exploitability	脆弱性への攻撃手法の存在状況	Unproven: 攻撃を行うプログラムが存在しない	0.85
			Proof-0f-Concept: 攻撃手法の考え方を示した基本プログラムが存在	0.9
			Functional: 機能的な攻撃手法が存在する場合	0,95
			High: 自動的な攻撃モジュールが存在する	1.00
RL	Remediation Level	修復方法のレベル	Official-fix: ベンダーから正式な解決策が提示されている	0.87
			Temporary-fix: 暫定的な解決策が提示されている	0.90
			Workaround: 解決策はあるが、正式なものではない	0.95
			Unavailable: 解決策が無いか、解決策を適用できない	1.00
RC	Report Confidence	報告書の信頼度	Unconfirmed: 正式な確認はされていない	0.90
			Uncorroborated: ベンダーの正式報告は無いが、複数の組織が報告をしている	0.95
			Confirmed: ベンダーがすでに報告を出しており、それが確認されている	1.00

3．Environment Metrics ＝ （Temporal Metrics + (10 - Temporal Metrics) × CD) × TD

略称	要素名	意味	要素	係数
CD	Collateral Damage Potential	損害の可能性	None: 損害の可能性はない	0
			Low: 少し影響がある	0.1
			Medium: 重大な影響がある	0,3
			High: 破壊的な影響がある	0.5
TD	Target Distribution	影響を受ける対象の数	None: 影響をうける対象が存在しない	0
			Low: 1～15% に影響	0.25
			Medium: 16～49% に影響	0.75
			High: 50～100% に影響	1.00

付録C TV 算出ツール利用方法

本 WG では、得られた重みと属性値を用いてトリアージ値（*TV*）を計算するツールのプロトタイプ版を作成した。この節では、TV 算出ツールの利用方法を示す。



ツールは Excel シート上で作成されたものであり、ユーザは「TV の計算」シート（上図）において、各オブジェクトの属性の有無または度合を入力することで TV を得ることができる。TV は中央赤色セル部に表示される。また TV を 0-100 点で換算した点数も併せて表示される。

実際の計算は「矢印の重み付けマトリクス」シート内で計算されている。一般的にユーザはこれを変更する必要はない。

参考文献

[1]NPO 日本ネットワークセキュリティ協会（JNSA），協会公式サイト，
http://www.jnsa.org/
[2]工学院大学，大学公式サイト，
http://www.kogakuin.ac.jp/
[3] FIRST, Complete CVSS Guide,
http://www.first.org/cvss/cvss-guide.html
[4]NIAC, Fact Sheet
http://www.dhs.gov/xlibrary/assets/niac/NIAC_Brochure.pdf
[5]日本工業標準調査会, TR X 0036,
http://www.jisc.go.jp/app/TPS/TPSO0020.html
[6] Internet Storm Center，アラートアイコン，
http://isc.sans.org/infocon.html
[7]The Internet Traffic Report, Japan(Tokyo) of Details for Asia,
http://www.internettrafficreport.com/history/293.htm
[8] 米国土安全保障省, Homeland Security Advisory System,
http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm
[9] SANS Institute,　Internet Storm Center,
http://isc.sans.org/
[10] FIRST, Complete CVSS Guide,
http://www.first.org/cvss/cvss-guide.html

平成 19 年 3 月発行

発　行：特定非営利活動法人日本ネットワークセキュリティ協会

東京都江東区新砂 1-6-35 NOF 東陽町ビル 1F
E-mail: sec@jnsa.org　　URL:http://www.jnsa.org/