CISCO SECURE | Cyentia 119

ホワイトペーパー
Cisco Public

優先順位付けから予測へ vol. 9

リスクベースの脆弱性管理における、悪用された既知の脆弱性カタログの役割

目次

前書きと主な調査結果

「サイバーセキュリティ インフラストラクチャ セキュリティ庁の拘束力のある運用指令 22-01 – 悪用された既知の脆弱性による重大なリスクの軽減 (Binding Operational Directive 22-01–Reducing the Significant Risk of Known Exploited Vulnerabilities)」とは、何とも長い名称です。お世辞にも覚えやすいとは言えない名前ですが、この指令は脆弱性や攻撃者の活動に関する重要な情報源となっています。「KEV」(Known Exploited Vulnerabilities) と通称されるこの情報は、サイバーセキュリティ インフラストラクチャ セキュリティ庁 (CISA) が把握しているエクスプロイトの標的となる脆弱性をリストにしたものです (正確な意味については後述)。

このレポートをお読みになっている方なら、KEV のような情報を押さえておくべき理由は明らかでしょう。データサイエンティストとしてこうしたデータに注目する際、私たちは手に入る他のデータとの関係性の中に KEV を当てはめて統計データに目を向けます。本書はシスコ (以前は委託先の Kenna Security 社) の後援で Cyentia Institute 社が作成した「優先順位付けから予測へ」調査シリーズの最新版であり、調査を通じて KEV にはどのような意味があるのか (および無いのか) に一定の説明を与えています。また、KEV とリスクベースの脆弱性管理プログラムとの関係性についても説明します。ここにいくつかの重要な調査結果をまとめていますが、ぜひレポート全体をお読みいただき、調査の成果をお役立てください。

- KEV は頻度は不定期ながら急激に拡大していますが、脆弱性全体に占める割合はごくわずか (0.5% のみ) です。
- KEV に登録されているものは大多数の脆弱性や、悪用された既知の脆弱性とは異なります。より重大度が高く (KEV の 3 分の 1 は重大度が「クリティカル」で、脆弱性全体に占める割合は 15% に上る)、性質も異なります(最近のものが多く、さまざまなベンダーに及ぶ傾向)。
- ほぼすべての組織 (98.3%) が自社ネットワークで KEV 脆弱性の検出を経験しています。
- KEV はエクスプロイトを見極めるうえで有用な情報源ですが、脆弱性を網羅しているわけではありません。実際に悪用が確認されている CVE の 94% は、KEV に掲載されていません。
- リスクベースの脆弱性管理戦略で使用されるデータソースは数多くありますが、KEV は間違いなくその 1 つに加えるべき情報源です。

KEV カタログの詳細

CISA KEV カタログが初めて公開されたのは、前述の強制指令と同じ 2021 年 11 月 3 日です。ここでは KEV の規模、拡大の過程、掲載されている脆弱性、想定よりも高頻度（または低頻度）で発生する脆弱性について説明します。まずは、ある脆弱性がどのようにして KEV に掲載されるのか、その仕組みを明らかにします。KEV の掲載基準は次の 3 つです。

1. 脆弱性に Common Vulnerabilities and Exposures (CVE) ID が割り当てられ、その CVE ID が公開されている（予約ではない）こと。
2. アクティブなエクスプロイトを試行した証拠があること（エクスプロイトの成否は問わない）。
3. 影響を受ける組織が脆弱性を修復するために取る対処法が明確化されていること。

1 つ目と 3 つ目の基準について説明してから、最後に「アクティブなエクスプロイト」について少し詳しく説明していきます。1 つ目の基準があるおかげで私たちの作業は容易になります。この基準はつまり、脆弱性の追跡にはほぼ例外なく CVE ID[1] が使用され、KEV も同じ方法で脆弱性を追跡していることを示します。ひいては CVE の豊富な情報を自由に使って KEV の情報を細分し、関連付けて検証できることになります。CISA は長年にわたって収集してきた豊富な情報に加えて、次の 2 点の内容を追加することにしました。

1. その脆弱性に対処するための推奨措置。
2. 指令の対象者に求める脆弱性の修復期限。

修復が必要な脆弱性はどれか（さらには修復対応に求める迅速さ）という予測情報を提供していることを考慮しても、この情報は非常に重要であり、興味深い分析の役に立ちます。過去に指摘した人がいるように、修復の手立てがないエクスプロイトに関する情報を公開すると、誰にとってもリスクを高めてしまうおそれがあります。CISA が第 3 の基準に実行可能な修復方法を挙げているのは、妥当な判断です。実際、KEV から CVE が削除されることがあるとすれば、その修復手段が何らかの理由で使えなくなった場合だけです。

1 つ目と 3 つ目の掲載基準について説明しましたが、2 つ目の基準は、KEV の情報に触れる際に注目される情報です。つまり、その脆弱性が「アクティブなエクスプロイト」であることです。このエクスプロイトは、あるシステム上でシステム所有者の許可を得ずに悪意のあるコードが実行されたという信頼できる証拠があるものと定義されます。

脆弱性が KEV に掲載されるには、CVE ID が公開されていて、悪用された証拠があり、さらに修復可能でなければなりません。

CISA はまた、情報はエクスプロイトの成功例と失敗例のどちらも含むものであることを明言しています。データ主義のシスコとしては「信頼できる証拠」が厳密にどのような意味を持っているのか疑問がないでもありませんが、今のところ CISA はこの件の情報提供には及び腰です。脆弱性スキャンやコンセプト実証（PoC）コードなどは、証拠要件を満たさないとしていますが、この説明は、何らかの形で悪意あるエクスプロイトを実際に捕捉することを暗に示しています。とは言え、CISA の情報を鵜呑みにするつもりはありません。他の情報源から得たアクティブなエクスプロイトとの関連性を検証していきます。

KEV の歴史と定義を整理したうえで、シスコ独自のデータ主義の視点から掘り下げてみましょう。

KEV カタログの規模

公開が開始された 2021 年 11 月の時点で、KEV にはベンダー 84 社 287 件の CVE が掲載されていました。その後、脆弱性の掲載数は 3 倍以上に増え、2023 年 7 月 1 日の時点でベンダー 199 社 965 件という規模に拡大しました。1 ヵ月あたりの脆弱性は合計で約 34 件になり、1 日にほぼ 1 件という着実な増加ペースだと思われるかもしれませんが、ひとまず図 1 をご覧ください。

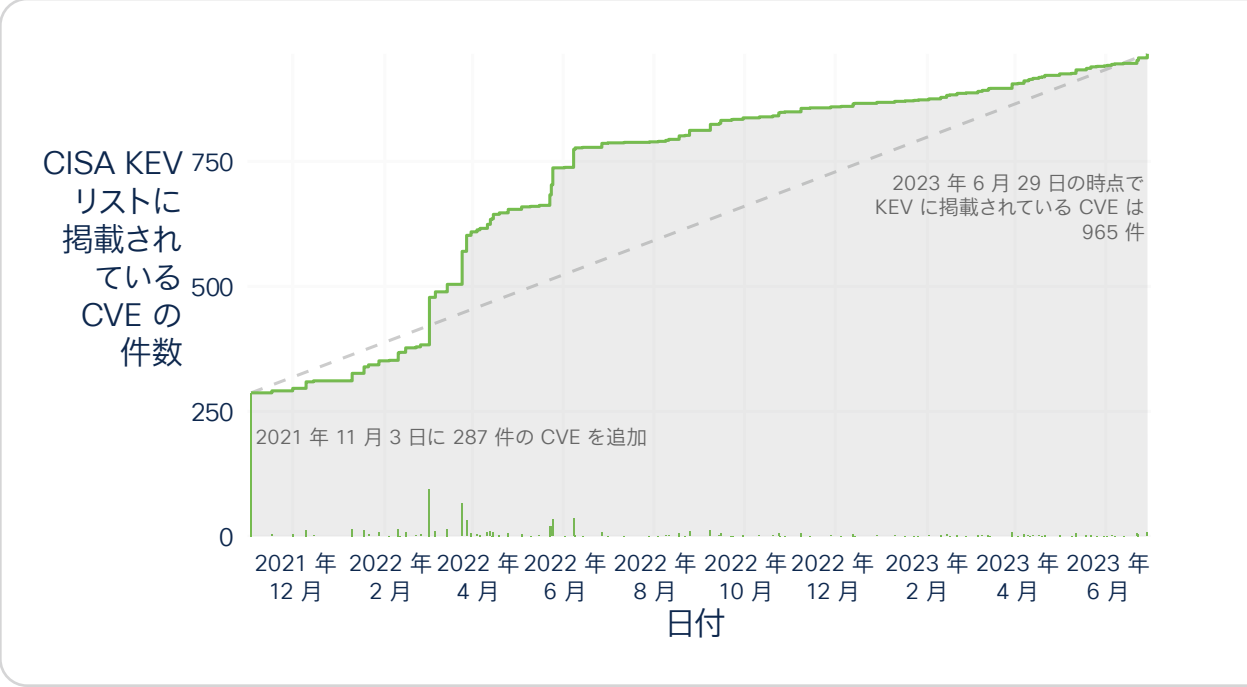

図 1. KEV カタログの拡大速度

ここで重要なのは、KEV に追加される脆弱性が増えるときは急に増え、次に追加されるまでの間隔が長いという特徴があることです。懸念すべき脆弱性の発生が途絶えた期間として最も長かったのは 2021 年 12 月 15 日から 2022 年 1 月 10 日の間で、延べ 26 日間の間隔が空きました。最初の 287 件を除けば、最も追加件数が多かったのは 2022 年 3 月で、95 件の脆弱性が追加されました。

本レポートで取り上げる脆弱性の性質を考えると、1 年強で規模が 3 倍になるというのは少し恐ろしいことのように思えますが、それでも 965 件という数字は掲載されている約 206,000 件の CVE に対しわずか 0.47% に過ぎず、大半の脆弱性は KEV に掲載されていないことがわかります。

重要なポイント：KEV には 1 ヵ月あたり平均 42 件の脆弱性が追加されます（ただし増えるときは急に増える）。

KEV カタログの網羅性

前述の検討結果から、KEV の規模が CVE 全体の 0.5 パーセント弱にあたるという事実を好意的に捉えるかもしれません。200 件に 1 件の脆弱性のみを優先するのであれば、昨年の 3 倍という増加率はそれほど悪くないと思えるかもしれません。しかし KEV カタログの網羅性については疑問が残ります。CISA は KEV カタログ内の脆弱性が、アクティブなエクスプロイトの状態である証拠があると断言していますが、アクティブなエクスプロイトはこれですべてだとは言っていません。

では、実際に悪用が確認された脆弱性[2]について、シスコ独自の情報源から入手した情報を検証してみましょう。具体的には、エクスプロイトに関する官民合わせた多くの情報源、たとえば Cyentia 社の Exploit Intelligence Service の情報を追跡している Cisco Vulnerability Management を使用します。2 つの情報源を比較したのが図 2 です。

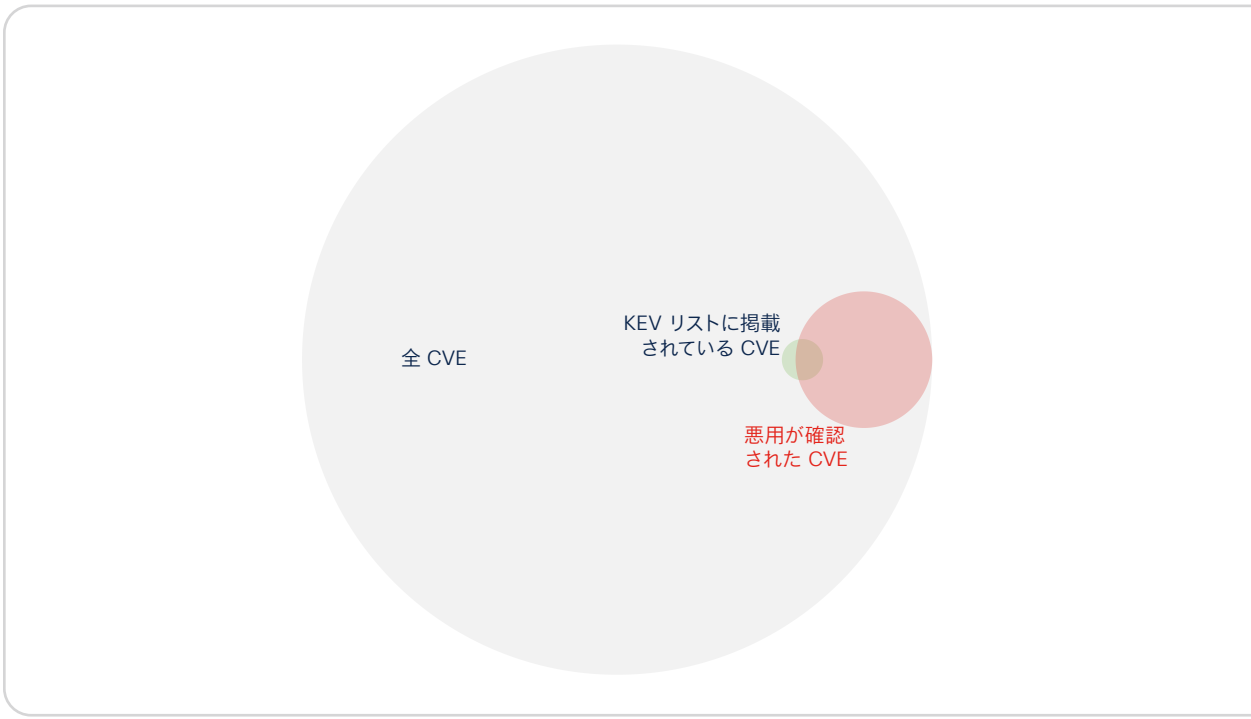

図 2. さまざまな情報源を基に作成した、悪用が確認された脆弱性の割合

ピンク色の円の部分はシスコのサービスをよくご存知の方にはおわかりかと思いますが、当社の情報源によれば、公開されている脆弱性全体の約 5% でエクスプロイトの活動が確認されたことを示します。はるかに小さい（10 分の 1）緑色の円は、掲載されている脆弱性が CVE 全体のわずか 0.45% にあたる KEV を表しています。円の大部分が重複していることから、KEV の脆弱性の大半（約 3 分の 2）が、シスコの悪用の実績データにも現れていることがわかります。このように、KEV の「K（既知）」を示す確かな証拠があり、攻撃者がその脆弱性を今現在標的にしている（もしくは少なくとも標的にしたことがある）ことに、シスコは強い確信があります。つまり KEV に登録されている脆弱性を修復するのは、決して時間の無駄ではないということです。このことは修復の優先順位付けを行う脆弱性管理プログラムにおいても、有力な材料となります。

ですが KEV と重ならないピンク色の部分についてはどうでしょうか。シスコが把握している脆弱性の約 94% は、実際に活発に悪用されていますが KEV には掲載されていません。このような齟齬が生じるのはなぜでしょうか。データの収集方法の違いが主な原因と考えられますが、KEV における「アクティブなエクスプロイト」の意味を正確に捉えなければ、具体的な結論を導き出すのは困難です。ここで 1 つの仮説を取り上げます。それは KEV が登場したのが比較的最近であり、新しい脆弱性を重視する傾向があるというものです。つまりこの仮説では、シスコが追跡している脆弱性で比較的古くても依然として悪用されているものは、KEV に取り上げられる可能性が低いことになります。ポイントは、KEV がエクスプロイトを見極めるうえで有用な情報であり、これに注目すればリスクを軽減できますが、エクスプロイトの活動を網羅しているわけではないということです。

KEV が重視するのは活発に悪用が確認されている脆弱性ですが、エクスプロイトコードに目を向けることにも大いに意味があります。なぜならシスコが過去に行った調査では、エクスプロイトコードが公開されている脆弱性を標的にしたエクスプロイト活動が、15 倍に増加したというデータがあるからです。図 3 は前掲の図 2 に似ていますが、違うのはエクスプロイトコードという切り口でデータを抽出している点です。

悪用が確認された CVE が KEV で網羅されていない理由

選択基準についてはすでに説明しましたが、こうした基準があり、基準を満たすすべての脆弱性が KEV に掲載されているわけではないことを踏まえたうえでなお、「なぜリストにはこれだけしか掲載されていないのか」と尋ねるのは無意味ではありません。シスコは（CISA ではないので）満足のいく答えを持ち合わせていませんが、だからと言って私たちなりの考えを引っ込める理由にはなりません。以下に挙げるのは、推測を交えずに実際のデータを基に分析を行うための注意事項です。

KEV の一義的な目的は、問題点を修正する必要がある政府系機関を一定の期間内に特定することです。これは米国政府が使用しているソフトウェアが脆弱性の影響にさらされることを懸念しているという、暗黙の基準が（レポートでは言及していませんが）あることを示しています。そのため、Candy Crash のようなゲームアプリの脆弱性が KEV に登録される可能性は低いと言えます。このアプリが連邦政府レベルでサポート対象のソフトウェアに認定される見込みが薄いことを考えれば、当然です。この暗黙の基準によって、「悪用が確認された脆弱性」であっても一定の割合は候補から除外されます。公開されていない暗黙の基準は他にもあるかもしれませんが、当局に睨まれないとも限らないので憶測は差し控えたいと思います。

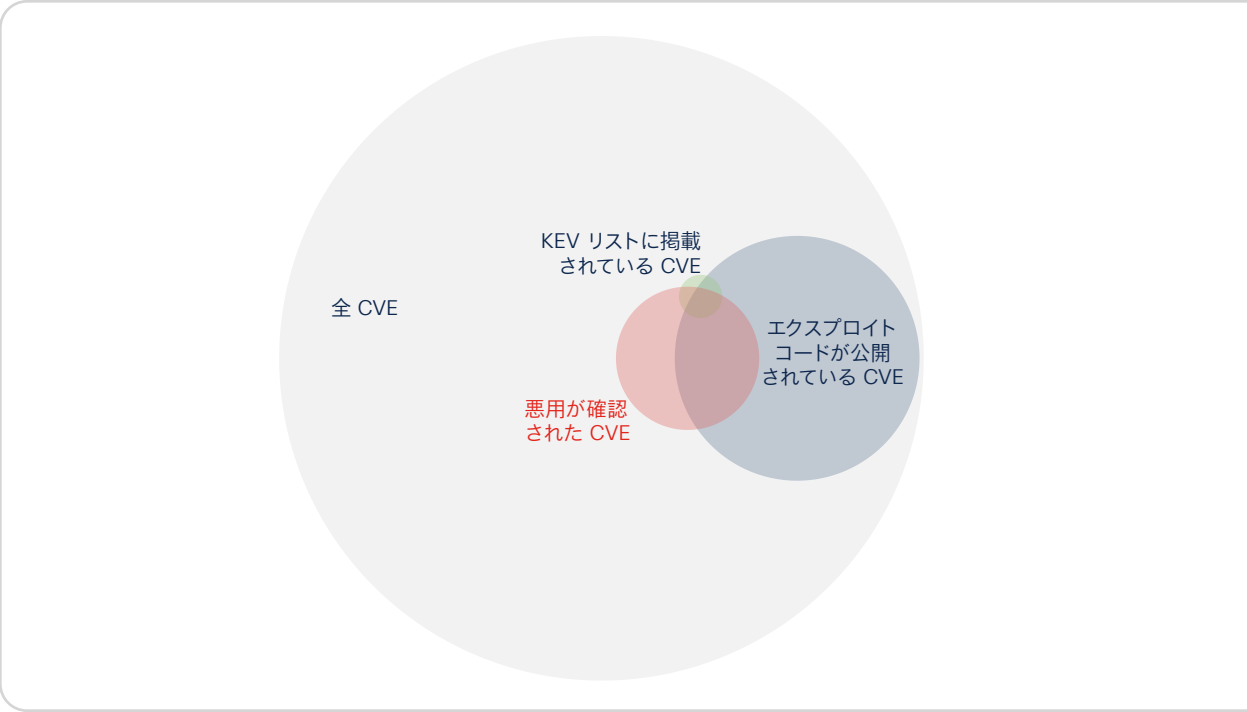

図 3. エクスプロイトコードが公開されている脆弱性、実際に悪用が確認されている脆弱性、KEV に掲載されている脆弱性の重複状況

KEV に掲載されている CVE の 3 分の 2 以上（68%）に、使用可能なエクスプロイトコードがあります。このデータはシスコが過去に行った調査の結果を裏付けるものです。興味深いのは、以前はあった大きな差異（KEV には見られないエクスプロイトが多くあること）が、ここでは顕著でないことです。悪用された証拠がある CVE の約 55% は、エクスプロイトコードが公開されています。エクスプロイトの統計の取り方にかかわらず、エクスプロイトコードが公開される可能性は（大雑把に言えば）同じということです。

重要なポイント：KEV は出発地点としては有効ですが、これ 1 つでリスクベースの脆弱性管理戦略を完結させることはできません。

KEV に掲載されている脆弱性の年代

KEV の脆弱性の大部分は悪用が確認されたものであり、他にも同様に悪用が確認されている脆弱性があることはわかっています。新しい脆弱性の方が重視されているために差異が出てくるという推測を立てましたが、裏付けとなるデータがあるか調べてみましょう。

図 4 は、公開日別に見た KEV の脆弱性（青い棒グラフ）と悪用の証拠がある脆弱性（赤い棒グラフ）の分布を示したものです。KEV が登場してから 1 年半弱になりますが、確認時期が特に早いもので言えば 2003 年 4 月 2 日に公開された CVE-2002-0367 など、かなり古い脆弱性が含まれています。KEV に掲載されている CVE の 5% は 2012 年以前に公開されたもので、81% は KEV が誕生した 2021 年 11 月 3 日より前に公開されたものです。

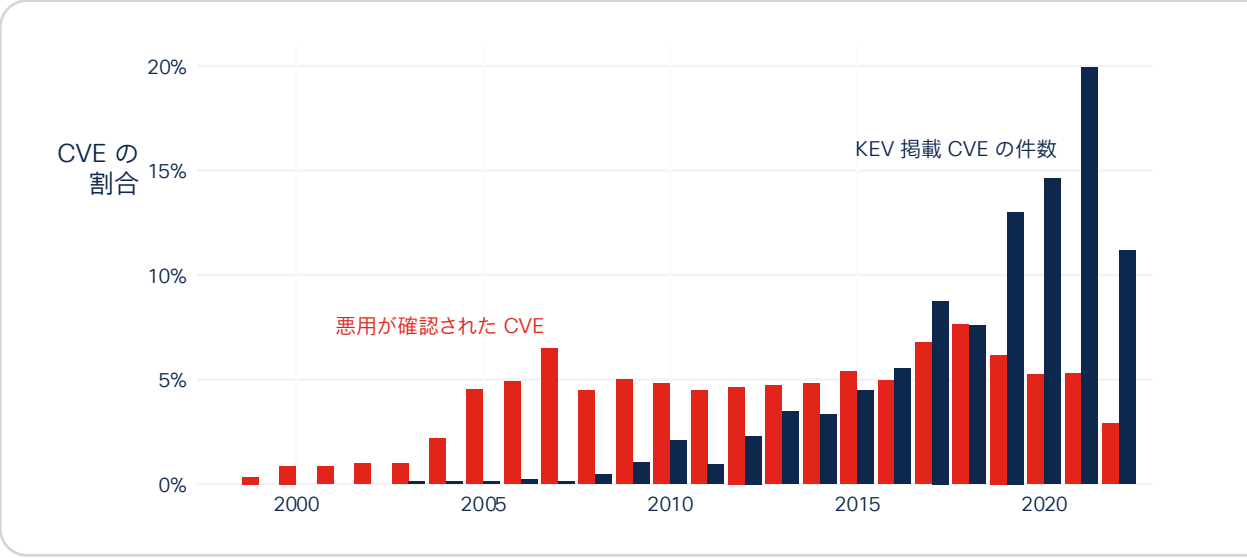

図 4. 悪用が確認された脆弱性の公開データの分布

KEV の公開日の分布と、悪用が確認された脆弱性の分布を比較すると面白いことがわかります。独自のデータでは新しいものが重視されている傾向があることを考慮し、図 4 の赤い棒のグラフには、過去 90 日間に悪用された形跡のある脆弱性だけが反映されています。KEV は最近の脆弱性を重視している傾向がありますが、攻撃者に今現在悪用されている脆弱性の方が、分布のばらつきがはるかに少ないことは一目瞭然です。かつては格好の標的であった CVE の中には、かえって攻撃者に見落とされてしまうものもあります。

重要なポイント：KEV の脆弱性には新しいものを重視する傾向があります。KEV を頼りに脆弱性に優先順位を付けると、ハッカーにとっては今も有用な手段と考えられている古い脆弱性を見落とす可能性があります。

掲載率の高いベンダー

では KEV の掲載率が高いソフトウェアベンダーはどこでしょうか。脆弱性のリストはどのようなものであれ、その傾向が一番に気になるという人は多いものです。KEV の場合も例外ではありません。また、これにはもっともな理由があります。脆弱性管理のプロセスはたいてい製品が中心となることです（たとえば、Microsoft によるセキュリティ更新プログラムの定例アップデートを思い浮かべてください）。

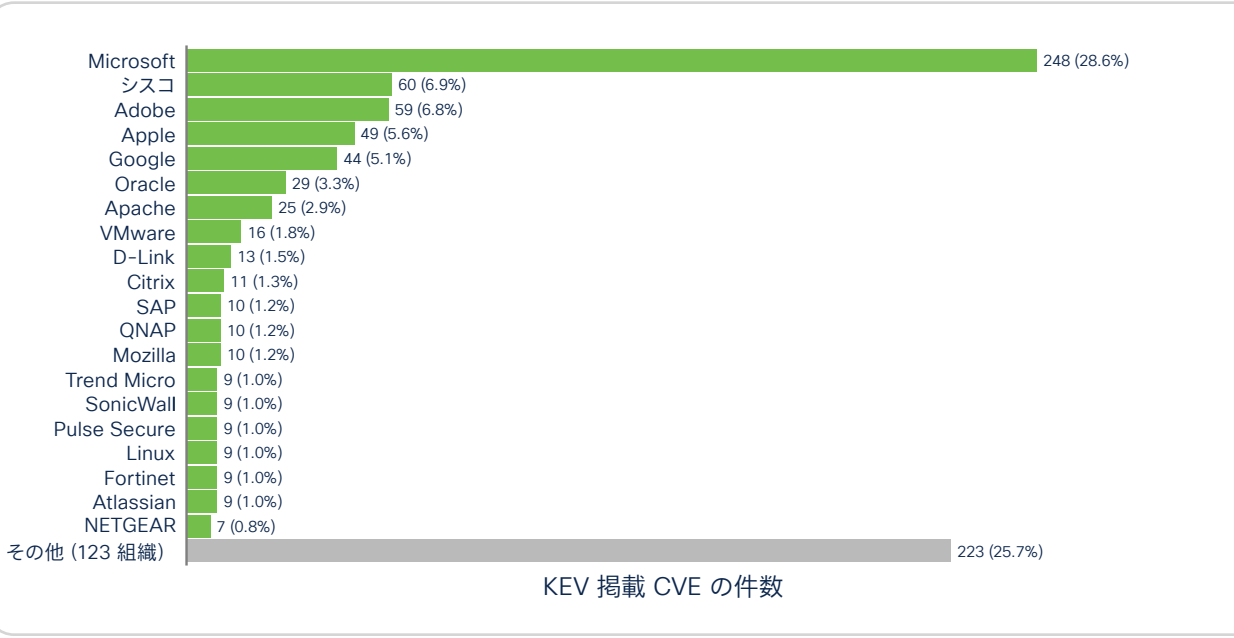

図 5. ベンダー別に関連付けられた KEV 内の CVE の件数と割合

図 5 は、KEV の上位 20 社の内訳（および割合が 0.8% 未満の「その他のベンダー」）を示しています。Microsoft 社について言えば、KEV に掲載されている脆弱性で同社の製品に影響を与えるものは、他社とは比較にならないくらい多くなっています。とは言え、安易に非難するものでもありません。と言うのも、Microsoft 製品が他の製品よりも本質的に脆弱であるとは限らないからです。KEV に掲載数が多いのは、Microsoft 製品に「既知の」エクスプロイトが多いという意味です。これは Microsoft 社が膨大なインストールベースを持つ製品を数多く提供しているという事実とも大いに関係があります。同社がエクスプロイトを追跡し、報告に努めている結果、数が多くなっているとも考えられるわけです。加えて、できるだけ手間をかけずにパッチやセキュリティ更新プログラムを作成できるように取り組んでいるため、Microsoft 社の CVE は、KEV の掲載基準である「修正が必要」という項目を満たしやすい傾向があります。

Microsoft 社があらゆる面で際立って KEV の脆弱性に掲載されやすいことを考えると、悪用が確認されているすべての CVE の中に Microsoft 社の名前が出てくる割合は、釣り合っていないのではないかという疑問を提起してみることは有意義です。この質問に対するシスコの答えはこうです。「いいえ。実際はその逆です」。その証拠が図 6 になります。

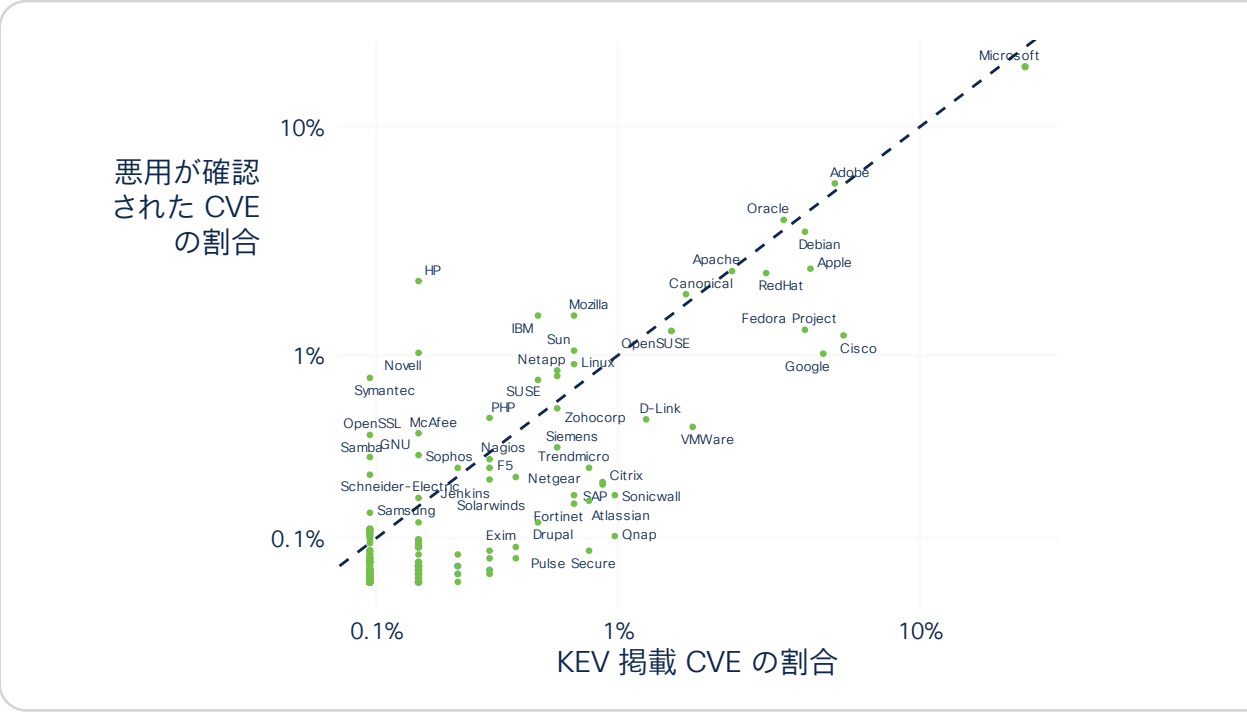

図 6. KEV に掲載されている CVE と悪用が確認されているすべての CVE の比率をベンダー別にまとめた図

図 6 で重要な目印となる手がかりは、対角線に伸びる破線です。この破線の左上側にあるベンダーは、KEV に掲載されている CVE の割合が低いのに対し、悪用が確認されている CVE の総数が多くなっています。一方、破線の右下側のベンダーは、KEV に掲載されている件数が多くなっています。KEV には Microsoft 社 の登録が 22.2% とやや多く見られるのは確かですが、悪用が確認されている CVE 全体に占める割合は 18.2% となっています。興味深いのは HP 社です。KEV 内の CVE 全体に占める割合は 0.1% ですが、悪用が確認されている CVE 全体で見ると 2.1% と、かなり高い数値になっています。かつて市場を席巻した HP 社も、往時ほどの影響力を持っていないことに原因があるのかもしれません。あるいは KEV が登場してからまだ 1 年と少ししか経っていないことを考えると、先ほど説明した新しいものを重要視するバイアスが作用している可能性もあります。

KEV に必要以上に取り上げられている企業はどこでしょうか。Google、シスコ、Fedora 社はどちらの数値も上位を占めていますが、KEV の掲載率が高くなっています。すべてのベンダーに関して説明が付くようなもっともらしい理由はありません。シスコの場合は企業環境で普及しているインターネットとの接続用デバイスを製造していることが理由でしょう。Fedora 社の場合、多くの企業インフラが Red Hat Linux 系統の OS を搭載したサーバーで動いていることが理由と考えられます。Google については、どのくらいの方が Chrome や Android フォンでこのレポートをダウンロードして読んでいるかを考えていただければ十分でしょう。

重要なポイント（参考情報）：ベンダーによっては悪用が確認された脆弱性の総数に比べて、KEV に掲載されている割合が多い場合もあれば、少ない場合もあります。

脆弱性の特定の性質が KEV への掲載を左右する可能性

脆弱性に対して責任を持つのはどのベンダーであるかや、脆弱性が発見されたタイミングを示す情報が個々の脆弱性に関する情報の中で占める割合は、わずか数ビット（もしくは数バイトか）です。ですがそれ以外にも重要な機能があることを説明しておきます。それこそが KEV に脆弱性が掲載される可能性を左右します。脆弱性を分類してコンテキスト化するのは難しいため、注意が必要です。データソースにはさまざまな種類があり、その多くは複雑で解析するのに骨が折れる形式（たとえば、フリーテキストで記述されているものや階層的な CWE）をしています。このやや雑然としたデータから、「この特徴がある脆弱性は KEV に掲載されやすい」ことを読み取るのは容易ではありません。

それを承知のうえで、少しでもカーテンに閉ざされた向こう側が見えるように、共通脆弱性評価システム（CVSS）と脆弱性の説明という 2 つの重要な特性について確認していきます。CVSS は（良くも悪くも）「この脆弱性をどの程度警戒すべきか」を判断するためのものです。そのため、ベクトルを細かく分けて確認することに意味があります。図 7 はそのような分析の結果です。

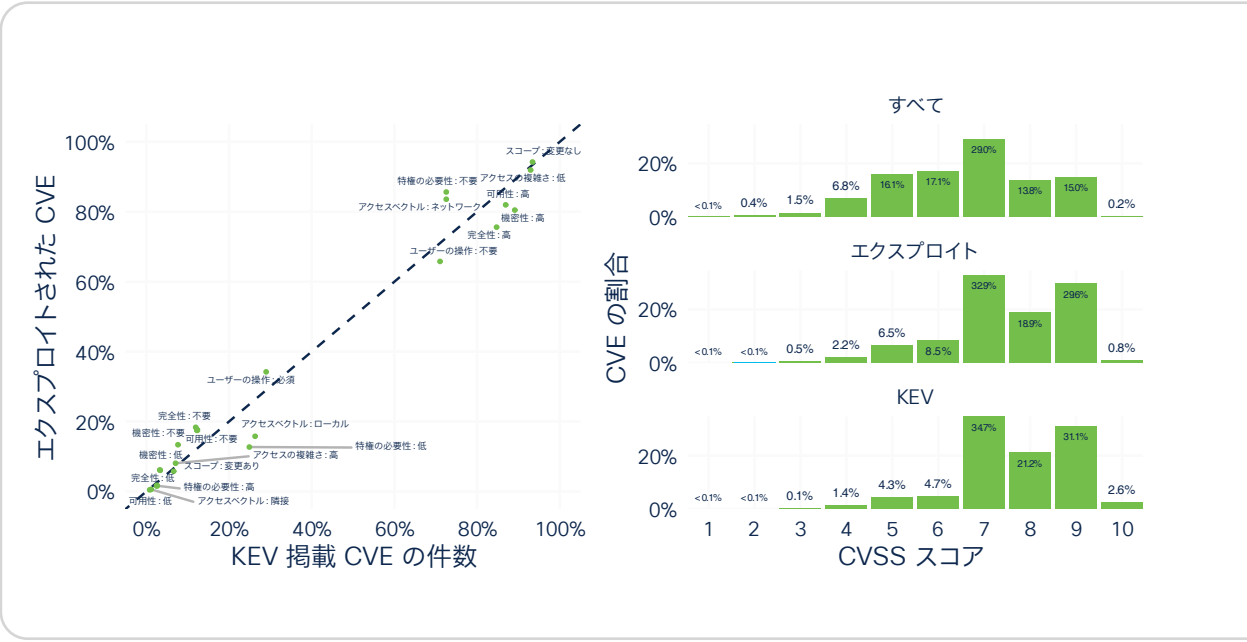

図 7：左側のパネルは図 6 と同様、悪用されたすべての脆弱性に対する KEV の指標の相対的な拡散度を示したもの。右側はすべての CVE、悪用が確認された脆弱性、KEV それぞれの基本スコアの分布

まず全体を見てわかるのは、悪用された脆弱性と KEV の脆弱性では、CVSSv3 のベクトルの分布がおおむね一致していることです。どちらのリストも攻撃者にとって価値の高いものを中心にしているため、この結果は驚くにはあたりません。注目すべきいくつかの違いをこれから説明します。まずは不評な CIA の 3 要素についてです。3 要素（機密性、完全性、可用性）のいずれについても、「高」が多く反映されていることがわかります。KEV には最も危険度の高いグループが含まれていることから、損害を与える可能性があるものに重点を置くのは理にかなっています。むしろ感覚的にわかりにくいのは、「必要な権限：なし」と「アクセスベクトル：ネットワーク」があまり反映されていない点です。考えられる原因は、IDS センサーから取得した悪用された脆弱性に関するデータは、多くのケース（すべてではなく）で、シークレットをほとんど必要とせずにネットワークを介して悪用可能なものの比重が多いことです。

図 7 の右側のグラフを見た方がわかりやすいかもしれません。簡単に言えば、実際に悪用された CVE は全般的に CVSSv3 基本スコアが平均よりも高く [3]、KEV に掲載されている CVE のスコアもやはり高いということです。基本スコアには脆弱性を悪用する際の難易度に関する情報が含まれています。悪用が容易であればあるほど、エクスプロイトリストや KEV の中に出てくる可能性が高いことを考えれば、グラフのような結果になるのは必然です。

もし CVSS のベクトルとスコアの組み合わせが、ある脆弱性をどの程度懸念すべきかの判断材料になるとしたら、脆弱性の説明は無用の長物です。脆弱性に関する説明によって、基本的な特徴についてはおおむね理解できるでしょう。ただしこれまで行ってきた分析方法では、膨大な量のテキストを分析することはできません。このテキストによる記述を高度な自然言語処理（NLP）で変換し、興味を引く特定のキーワードを抽出したうえで、前の 2 つの図と同じタイプの比較結果としてまとめたのが、図 8 です。

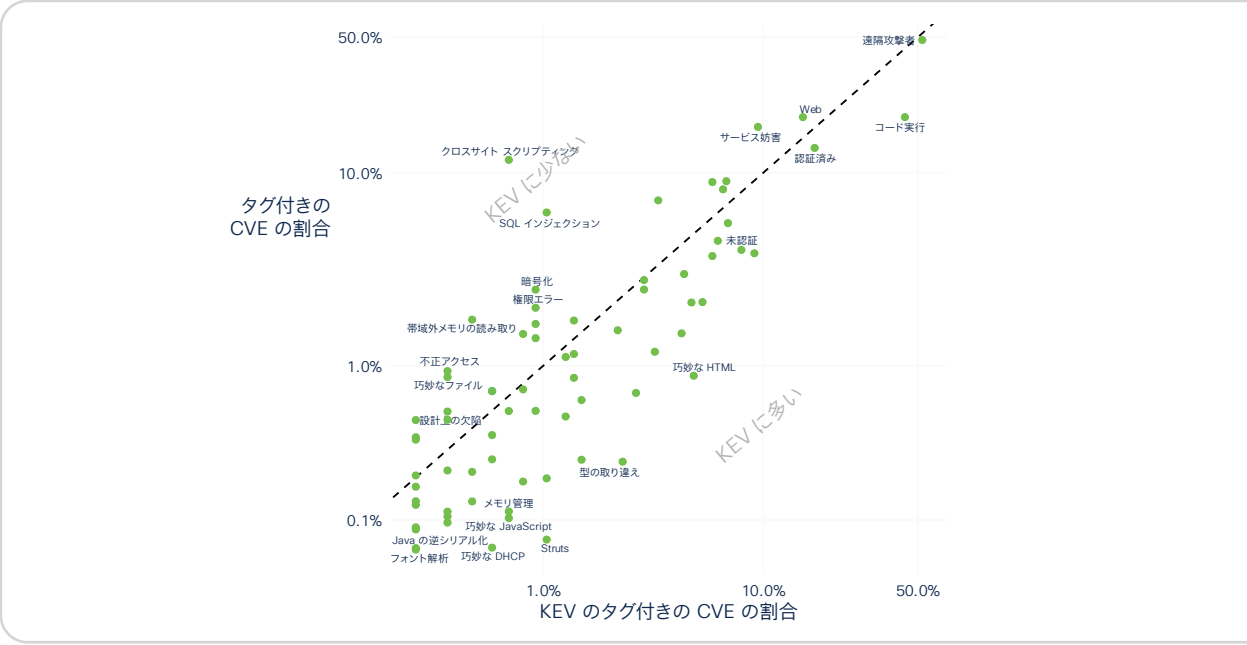

図 8. タグ付きの KEV に掲載されている CVE と公開されたすべての CVE の割合

興味深いのは KEV の中に「巧妙な」脆弱性が多く見られることです。たとえば「巧妙な HTML」、「巧妙な JavaScript」、「巧妙な DHCP」などのタグです。これは政府系組織で巧妙な標的型攻撃が目撃されていることの表れかもしれませんが、この分析は少々推測めいています。

KEV に掲載されている CVE の説明に「認証された（authenticated）」と「認証されていない（unauthenticated）」の両方が多く現れるのが、この分析方法の特異な点です。そうなるのは説明の中で 1 つの言葉を 2 つの異なる意味で使えるためであり、矛盾ではありません。攻撃者が「認証される」必要があるという意味にもなれば、脆弱性をつくことで攻撃者が「認証される」ようにできるという意味にもなります。こうした言葉が出現する数が多い場合は、後者の可能性が高いということです。

対角線の反対側に多く見られるのは、クロスサイト スクリプティングや SQL インジェクションなどです。これは、蔓延している「乱れうち」の手法で脆弱なシステムを見つけようとする攻撃者を検出する傾向が高い、エクスプロイトデータ狙いへの回帰が考えられます。

重要なポイント：悪用が確認された脆弱性と KEV の脆弱性は、一般的な脆弱性に比べて重大度が高くなります。

企業内部に見られる KEV 脆弱性

「世界のどこか」で活発に悪用されている脆弱性は、実際のネットワーク上のコンピュータのソフトウェアに影響を及ぼしさえしなければ、それほど影響がない場合もあります。これは P2P シリーズで長年扱ってきた、よくあるテーマです。注意が必要なのは、すでに悪用されたことのある(あるいは PoC コードが公開されているため悪用が簡単な）脆弱性や、実際に自社の環境の中に存在している脆弱性です。ネットワークに影響しない脆弱性を警戒する必要はありません。この点を踏まえて Cisco Vulnerability Management が追跡している 960 万点の現用資産を検査し、6 億 3,750 万件ある脆弱性の中に、KEV に掲載されている CVE が現れる率を確認しました。

現用資産に影響を及ぼす KEV の割合

上記の見出しは、最初に浮かぶもっともな疑問を呈しています。過去の P2P では、多くの組織は公開されている CVE 全体の約 3 分の 2 に気付いていないか、検出されていない状態であることがわかりました。基盤となるデータは日々変化しているので、過去の成果に満足することなく最新のデータに基づいて一部の統計情報を更新しましたが、状況は変わっていません（図 9 左手の左側の 2 つの象限）。

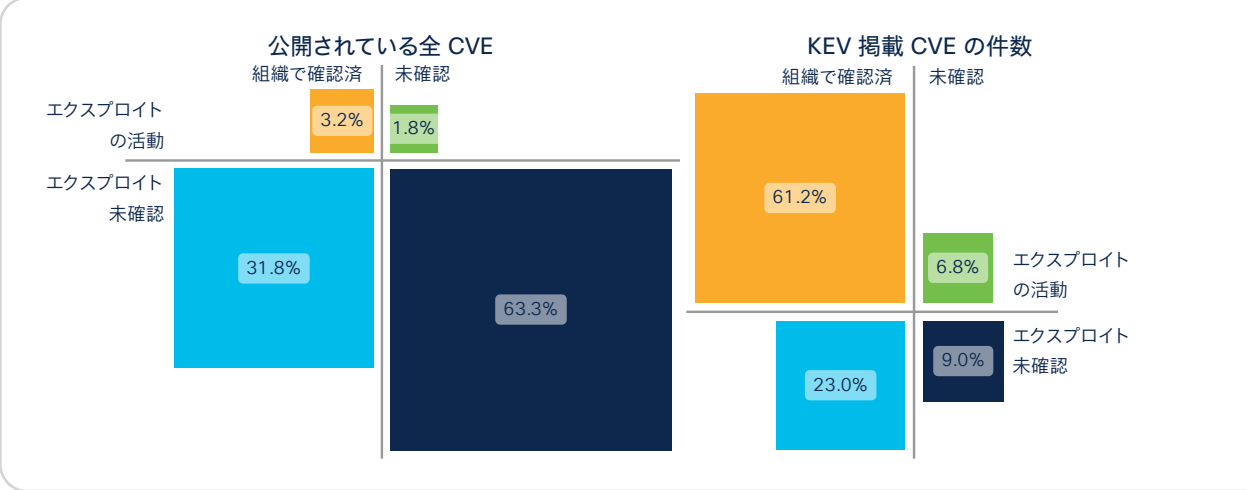

図 9. 全 CVE と KEV のリストで確認または悪用された脆弱性の割合の比較

ここでは図 9 の左側の図に絞って読み方を手短に確認します。

- 横軸は、既知のエクスプロイトが確認された CVE（約 5%）を切り分けたものです。
- 縦軸は、組織内部で確認された CVE を切り分けたものです。
- したがって、公開されているすべての CVE のうち、組織にとって現実的なリスクとなる脆弱性（組織内で確認された CVE と実際に悪用が確認された CVE の両方）は 3.2% しかありません。
- 脆弱性管理プログラムでは、この高リスクの脆弱性に優先的に対処するよう推奨しています。

「公開されている全 CVE のうち現実的なリスクとなる脆弱性はわずか 3.2% ですが、KEV の 60% は最優先で修復が必要です」

では、KEV カタログに掲載されている CVE だけを見た場合はどうでしょうか。右側の図を見ると、大きな違いがあります。まず、右下の濃青色の象限は、KEV に掲載されている CVE の中でははるかに集団として小さい、簡単に優先度を下げることができる（確認も悪用もされていない）脆弱性がずっと少ないことを示しています。逆に、KEV に掲載されている CVE は確認も悪用もされている脆弱性の割合がはるかに多く、KEV の 60% が優先的に対処する必要があります。

注意深い読者の方は、図 9 の右側と、図 2 および図 3 のベン図との違いに注目されるでしょう。これらのデータを総合すると、KEV は非常に効率が良く、登録されている脆弱性はどれも軒並み悪用されていることがわかります。一方で網羅性に関してはあまり期待できません。KEV でカバーされていない多くの脆弱性が、実際に悪用されているからです。これについては鋭い読者の方もすぐに納得していただけるように、後の節で詳しく説明します。

重要なポイント：KEV の大部分は組織にとって現実的なリスクであり、優先的に修復する必要があります。

組織全体への KEV の広がり

次に取り上げるのは、前述の疑問を裏返したものです。ここに 8,600 万という数字があります。何かと言うと、組織の資産に KEV の脆弱性が見つかった件数です。合計した結果 1 つの数字になったというだけに見えるかもしれませんが、おそらく脆弱性や資産、組織などの複数の要素をさまざまな方法で横断的に分析する必要があります。実際にそうした分析を行ったのが図 10 です。

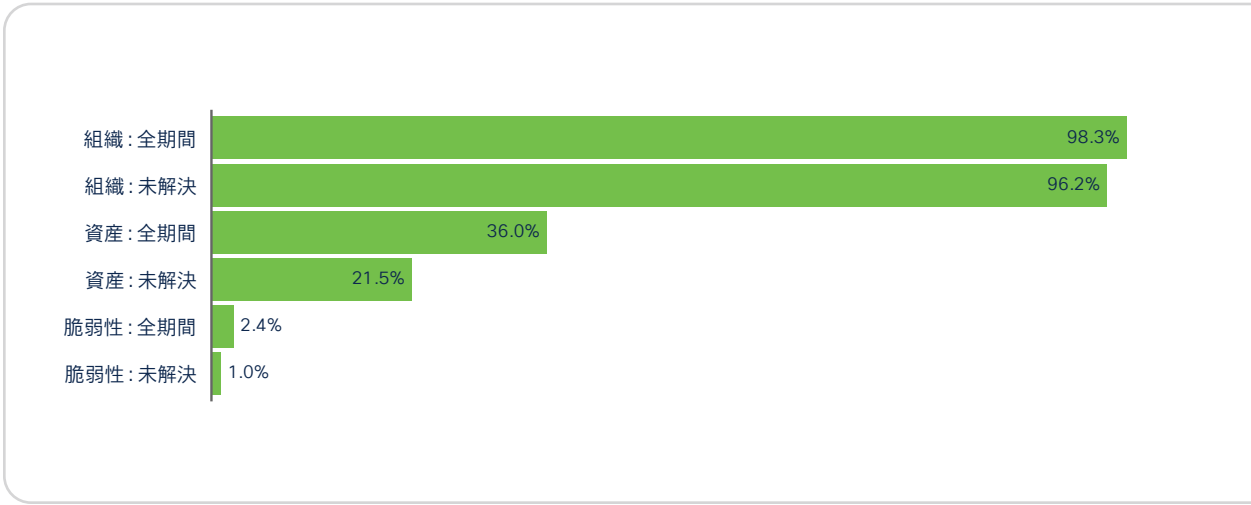

図 10. 複数の指標による組織内の KEV 掲載 CVE の広がり

図 10 の面白い点は、読者の方が気になるであろう大体の疑問にこのグラフで答えられそうなことです。これまでに KEV の脆弱性を経験しているという組織の割合[4]は、「未解決」（96.2%）と答えた組織に限定しても、ほぼすべての組織（98.3%）が該当します。資産という切り口で見ると、KEV の脆弱性を発見したことがある資産および脆弱性のうち、未解決の資産の割合はそれぞれ 36% と 22% という極端でない普通の数値にまで下がります。最後に、資産の中で見つかった 35 億件の脆弱性のわずか 2.4%、調査時点で公開されていた 8 億 1,500 万件の脆弱性の 1.1% であることを考えると、非常に稀と言えます。

これは何も出し惜しみをしているわけでも、効果的な見出しになるように曖昧な言い方をしているわけでもなく、さまざまなレベルに分けて分析を行った結果でしかありません。次はもう少し掘り下げて、KEV の個々の脆弱性が組織内で発生する頻度に目を向けてみましょう。図 11 を見ると脆弱性によって広がりが大きく異なることがわかります。本レポートの中でよく見られる傾向です。

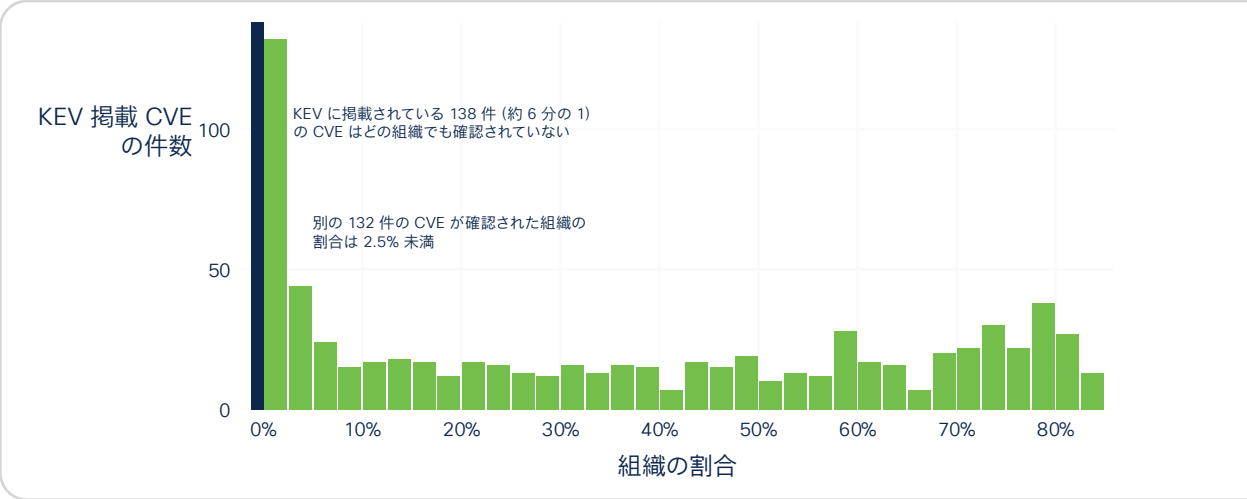

図 11. 組織における KEV 掲載 CVE の分布

目を引くのは KEV の脆弱性の 16%（866 件中 138 件）は、一度も組織の脆弱性スキャンで検出されたことがないという点です。それとは別の 130 以上の脆弱性も 2.5% 未満の組織でしか確認されていません。合計しても KEV の 4 分の 1 弱にしかならないのです。ただし広がりは相当なものです。KEV 掲載 CVE の 9 件に 1 件は 75% 以上の組織で確認されています。また、KEV の脆弱性の多くは 85% の組織で確認されており、リスト最上位の CVE-2020-1147 も組織でのスキャンによる検出率が 84% に上ります。これは SharePoint のリモートコードを実行する脆弱性として悪名高く、相当数の Microsoft 製品に影響を与えており、検出されない方が珍しいくらいです。次のセクションでは、各所で確認されている KEV の脆弱性について詳しく見ていきます。

ポイント：KEV の脆弱性は組織の至る箇所に存在しますが、脆弱性全体で見れば、そのごく一部で修復の優先順位を争っているにすぎません。

最も広がっている KEV

CVE-2020-1147（シスコが知る限り最も広範囲に認められる脆弱性）は内容を詳しく見ていく口実としてはうってつけです。ここからは図表、グラフ、統計情報などを使って個々のレベルで KEV CVE の共通点を調べてみましょう。ここでも「共通性」を測る方法は複数あります。図 12 は、CVE が確認された組織の割合と、脆弱性があり影響を受けた資産の割合という 2 つの指標を用いて散布図にしたものです。

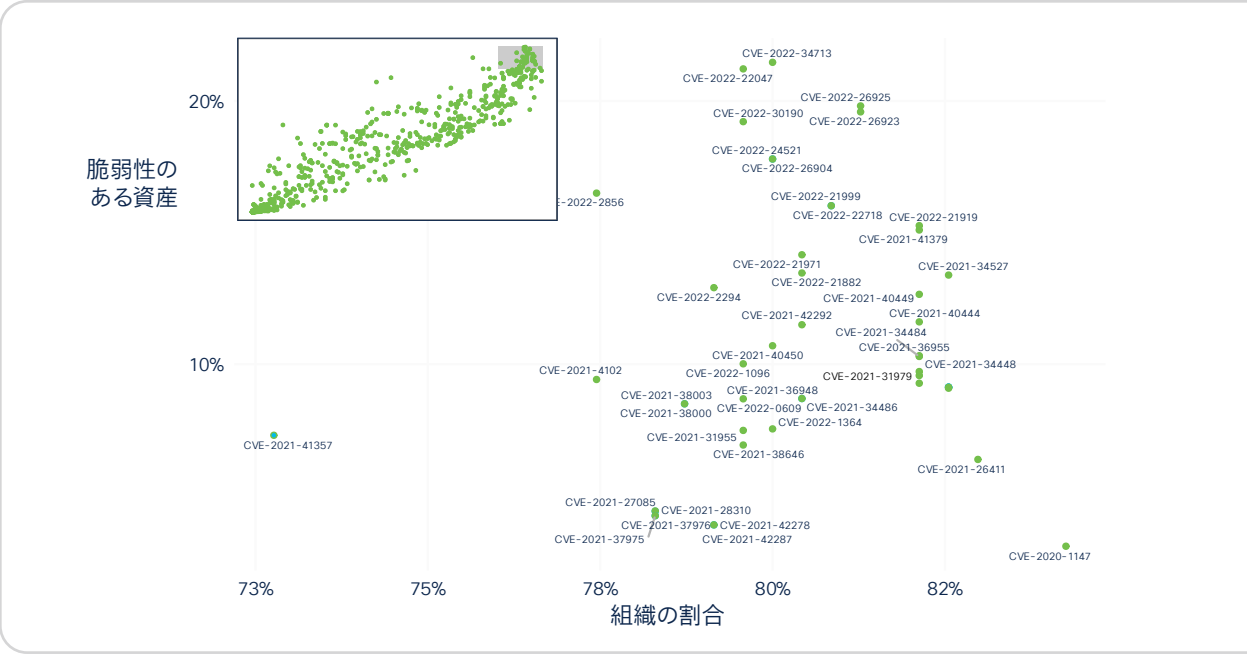

図 12. 最も広く確認されている KEV 掲載 CVE の組織と資産それぞれにおける割合

この散布図から、あらゆる領域に CVE が確認されていることがわかります。一番右上にある CVE は、組織と資産どちらにも広がっていることを表しています。この図では、最も広がっている CVE のいずれにも 2020 年以降の ID が付与されていることから、前述の新しいものほど重要視されるというバイアスが見て取れます。もう一つ別の要因として、組織が古い脆弱性の修復により多くの時間を割いているため、比較的新しい脆弱性についてはまだ対応途中ということも考えられます。読者の方にも図 12 から独自の推察を行っていただければと思います。

KEV 登場以前の脆弱性の割合

最後の事実はサブセクションのタイトルを連想させるかもしれませんが、シスコのデータ内の資産に見られる 8,600 万件の KEV 掲載 CVE の大半（63%）が、KEV が作られる前に修復されていることは、データから簡単に確認できます。KEV にその脆弱性が掲載されているかどうかは修復の優先度に影響しないため、この事実は注目に値します。

もちろん、KEV のすべての脆弱性が一度に現れたわけではありません。古い資産を初めてスキャンできたとき、新しい資産がオンラインになるとき、脆弱性のあるソフトウェアバージョンがインストールされたときなど、さまざまです。次の図 13 は脆弱性の発見日を、KEV への脆弱性情報の追加日および公開日（参考情報）との相関関係からグラフ化したものです。

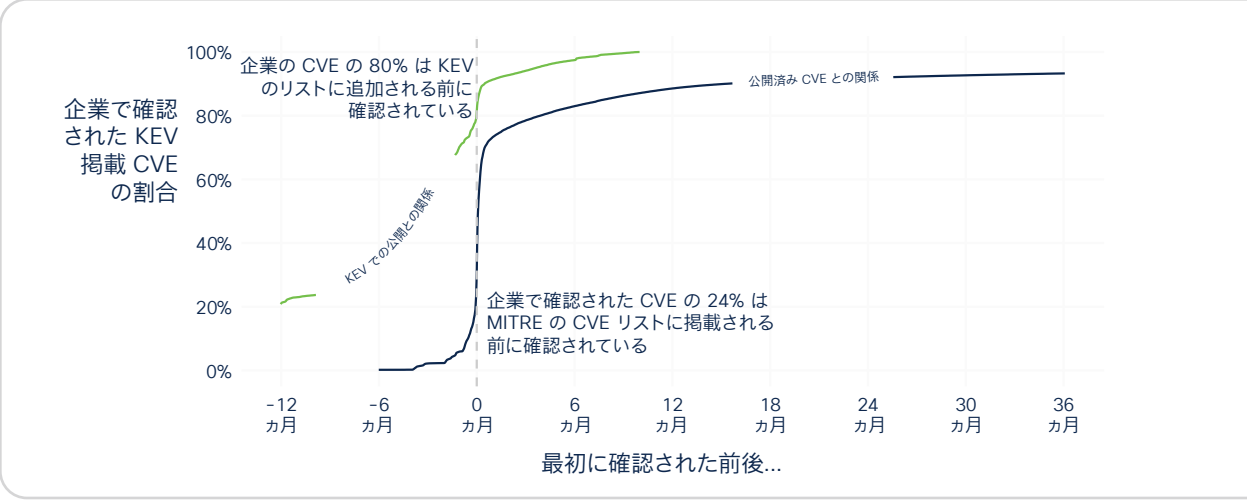

図 13. CVE が最初に発見された日と KEV への登録日および公開日との相関関係

KEV の脆弱性のほとんどは公開されるまで発見されず、そのため発見件数も急激に増加（濃青色の線）しています。緑色の線も同じタイムラインです。青色の線との違いは、公開日との相関関係ではなく、KEV に CVE が追加された日との相関関係を示している点です。その違いは明らかです。後者はほとんどが KEV に公開される前に発見されています。そのため、KEV カタログに脆弱性情報と併せて「修復期限」を設定して公開するのは奇妙な考えのように思われます。追加後しばらくのうちに発見される脆弱性はごくわずかです。このデータが意味するのは、カタログ追加後に発見された脆弱性の修復タイムラインを短縮した方がよいということでしょうか。でなければ、修復がたちまち手遅れになるということでしょうか。「発見から x 日以内に修正すること」という通知を出す方が、日付を決めてしまうよりも合理的に思えますが、誰からも疑問は出されませんでした。

修復済みの KEV の割合

検出後の次のステップは修復です。KEV で公開された後に未解決になった、または検出されたという 37% に焦点を当ててみましょう。この調査を行った時点では、75% は解決済みでしたが、25% は今も未解決のままです。

KEV には米国政府系機関に対して「これらの脆弱性を速やかに修正する」よう求める拘束力のある指令が含まれていることを考えると、解決済みの 75% が業界全体でどのような内訳になっているかを調べるのは、出発点としては面白いと思います。図 14 は各業界の反応を正確に表したものではありません。

「KEV の公開後に未解決になった、または検出された CVE の 25% は、今も未解決のままです」

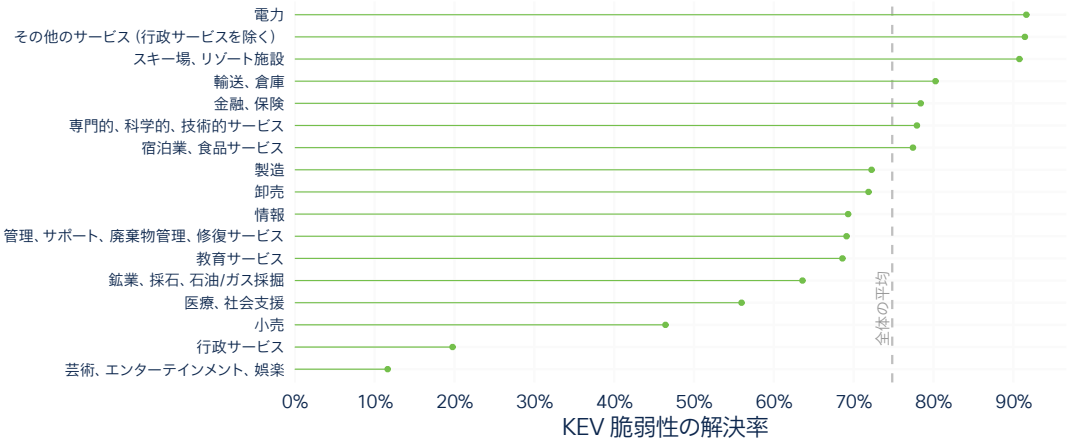

図 14. KEV に追加された後に発見され、解決された KEV の脆弱性の割合

上のグラフの「公共部門」には、KEV の脆弱性を速やかに修正することになっている米国の政府系機関が含まれますが、解決済みの機関は 20% 程度に過ぎず、平均を大きく下回っています。一つ留意点として、公共部門には 230 万件の脆弱性がありますが、そのうち 5 万 8,400 件は KEV の脆弱性です。両方のカテゴリを合わせても 0.06% のため、サンプルとしては少量です。

期日までに修正される KEV の割合

KEV の面白い点は「修復期限」を推奨する文言が含まれていることです。ほとんどの脆弱性にはこのような基準は含まれていません。KEV に追加された後の修復期限までの期間は、たいていの場合 4 つのカテゴリに分類されます。

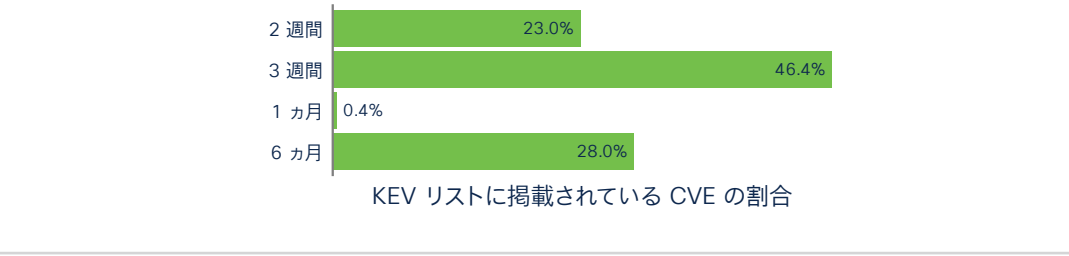

図 15. KEV リストに掲載されている CVE に対する修復期間の設定

数字に強い方は、この 4 つの期間を合計しても 97.8% にしかならないことに気づくでしょう。残りの 2.2% には追加された日よりも前の期日が設定されていて、一度限りの不自然な期間が設定されてるものもあります。

一般的には、統計ツールキットを使用して信頼できる「生存率分析」を行いますが、今回はあまり意味がありません。大半は KEV が登場する前に発見されて修正されていたものであり、KEV への掲載優先順位に影響を与える見込みが薄いためです。

では、KEV に登録された時点またはその後に未解決になった 37% を見てみましょう。75% は解決済みであることには言及しましたが、KEV に設定されている期日までに修正された割合はどの程度でしょうか。

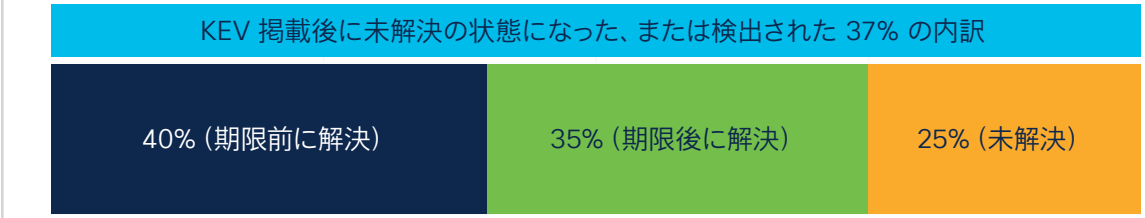

図 16. KEV に設定された期日までに修正された KEV の脆弱性の割合

40% は合格点というわけではないものの、期日を過ぎてから解決された脆弱性が 35% であることを踏まえれば (遅ればせながらも) 手堅いと言える数字です。ただし、データのほとんどは政府以外の情報源から提供されたものであり、KEV に準拠している必要はありません。

KEV に掲載されるには、CVE の修復が可能であることが要件の 1 つであったことを思い出してください。もちろん、ソフトウェアの種類によって修復にかかる負担は異なります。たとえば、ネットワークアプライアンスのファームウェアの更新は、ブラウザをバックグラウンドで再起動させるのと比べれば難易度がやや上がります。図 17 は、いくつかのソフトウェアカテゴリにおける KEV 脆弱性の何パーセントが、期日までに修正されるかを示したものです。

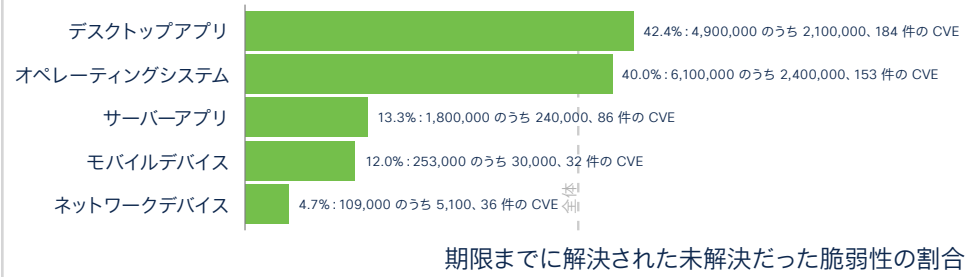

図 17. KEV に設定された期日までに修正された KEV の脆弱性の割合 (デバイスタイプ別)

なおこの図の脆弱性は、KEV の中で CVE が公開された時点で未解決だったものを表しています。図 16 は、前段で推測したとおりになっています (予想どおりでした)。デスクトップ アプリケーションとオペレーティングシステムの修正が期日 (KEV で定められた期限) までに完了する割合は 40% 強です。一方、「電源を切ってから再度電源を入れる」のがやや困難な傾向にある脆弱性については、それほど首尾よく進むことはなく、期限内に修正されたネットワークデバイスの脆弱性はわずか 4.7% でした。

KEV に焦点を当てたレポートも 4 分の 3 まで終わりましたが、これでも KEV 独自の事情は語られていません。具体的には、ネットワーク対策に関する問題であり、ネットワークデバイスを最新の状態に保つような厄介で手間のかかる作業が、いかに大変かという問題です。ネットワークデバイスはインターネットに対応した資産であり、「実際に悪用された」脆弱性が含まれます。資産を最新の状態に保つことは組織の安全を確保するうえで不可欠ですが、そつなくこなせている企業は滅多にありません。その理由の 1 つは、ネットワークデバイスのような資産のソフトウェア更新に伴う煩わしさです。更新作業は Windows マシンで [今すぐ更新] をクリックするような単純な作業ではありません。また、ファームウェアの更新時に発生するダウンタイムは、日々の事業活動に影響を及ぼすおそれがあります。企業各社にはこの困難に打ち勝ち、基本的な対策を怠らないように励んでいただきたいと思います。

現実的に期限までにすべての KEV を修正できるか

vol.7 の中で、平均的な組織では所定の月に未解決の脆弱性に対処し、全体の 15.5% を修正しているという調査結果を確認しました。KEV が脆弱性全体に占める割合はごく一部であることは認識していますが、シスコが定義した対処能力から見て、15.5% の修正で KEV の脆弱性を完全に排除できるのかと疑問に思うのも無理はありません。この問題に対処するには、KEV の脆弱性で未解決の割合を、月ごとに確認する必要があります。

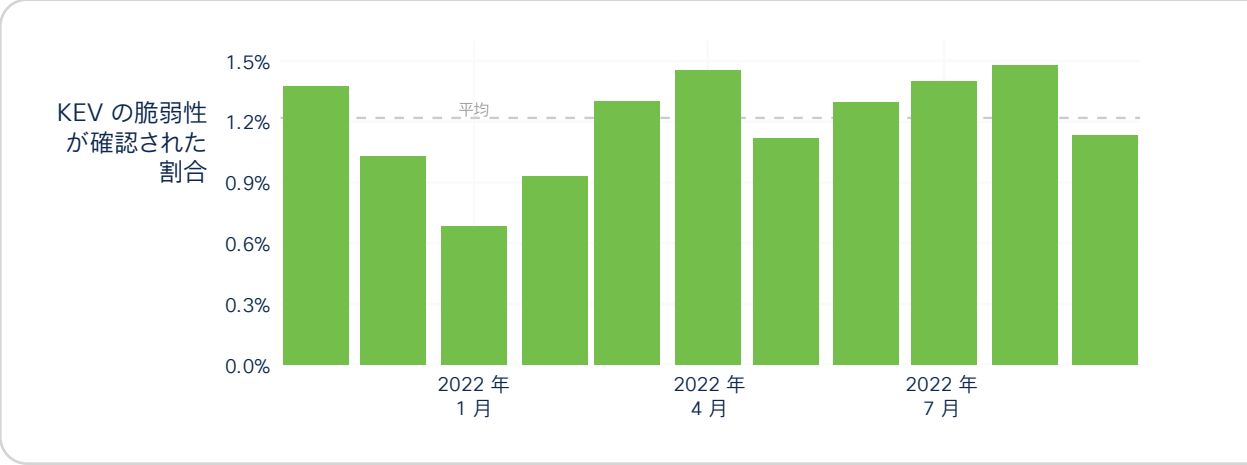

図 18. 月単位で見た未解決の KEV 脆弱性の割合

KEV は修復の優先順位を競う脆弱性全体の 1.5% に過ぎず、一般的な対処能力である 15% を下回っています。つまり、ほとんどの組織には KEV に対処するのに十分な能力と、悪用が確認されているその他の脆弱性にも注意を払うだけの余力があるということです。

重要なポイント:一般的な組織でも、KEV の更新に対応するために必要な能力の 10 倍 (15% 対 1.5%) の対処能力があります。

リスクベースの脆弱性管理にとっての KEV

ここまで KEV の規模と形式、そのカタログが企業内でどのように機能しているかを説明してきました。リスクベースの脆弱性管理プログラムにとって有用な情報が KEV に含まれていることに、疑問の余地はありません。では、その戦略にどのような形で KEV を取り込めばよいでしょうか。何しろ、企業システムの中に見つかった無数の脆弱性によるリスクを軽減するための手段であるデータソースはとにかく豊富にあります。最後となるこのセクションではいくつかの可能性を探り、KEV が巨大な全体像の一部を構成する要素であることを示したいと思います。

適切な修復戦略の要素とは何かをどのように判断すればよいでしょうか。シスコは主な尺度として、網羅性と効率性の 2 つを採用しています。

- **網羅性**：エクスプロイトの活動が確認され、修復が行われる脆弱性の割合
- **効率性**：エクスプロイトの活動が確認されているが、すべて修復済みの脆弱性である割合

要点については（過去の P2P ですでに基礎固めが終わっているため）ここでは割愛しますが、大事なのはこの 2 つの概念が重要である理由を確認しておくことです。この 2 つは、脆弱性修復において両立が難しい関係性にあります。あらゆる脆弱性を修復できるわけではないため、どちらを優先するかを選択する必要があります。考え方としては、危険性の高い脆弱性を可能な限り多く選択（網羅性）し、危険性の低い脆弱性に過剰な労力を払わない（効率性）ようにします。

では、「あるリストに掲載されている脆弱性に更新プログラムを適用したらどうなるか」という問いを立ててみましょう。この設問に答えるにあたって、まず 56,600 件の一意の CVE が記録されたデータセットを考えます。このデータセットには、組織全体の全資産で 5 億 8,460 万件の未解決の脆弱性が含まれています。次に、さまざまなデータソースにあたり、それらに掲載されている脆弱性をすべて修復したらどうなるかを想像します。たとえば、Exploit Prediction Scoring System（EPSS）のスコア 90% 以上の脆弱性をすべて修復した場合、網羅性と効率性はそれぞれどうなるでしょうか。あるいはリモートコード実行についてはどうか、Metasploit のモジュールに脆弱性が存在する場合はどうかなど、さまざまな条件を仮定して検討します。比較のため取り上げる戦略は 12 種類です。図 19 は各修復戦略のデータソースのみを使用した場合の網羅性と効率性を分布図に落とし込んだものです。

CISA KEV：CISA KEV カタログに掲載されているもの	**RCE**：リモートコード実行により悪用可能なもの
Metasploit：MetaSploit モジュールに含まれるもの	**EPSS クリティカルレベル**：EPSS スコアが 98% のもの
ExploitDB：ExploitDB に登録されているもの	**EPSS 高レベル**：EPSS スコアが 90% のもの
Github：Cyentia 社の Exploit intelligence Service により GitHub でエクスプロイトコードとして特定されたもの	**CVSS 中レベル以上**：CVSSv3 の基本スコアが中以上（CVSS 4 以上）のもの
Reversing Labs：同社が保有する悪用の証拠	**CVSS 高レベル以上**：CVSSv3 の基本スコアが高（CVSS 7 以上）のもの
	CVSS クリティカルレベル以上：CVSSv3 の基本スコアがクリティカル（CVSS 9 以上）のもの

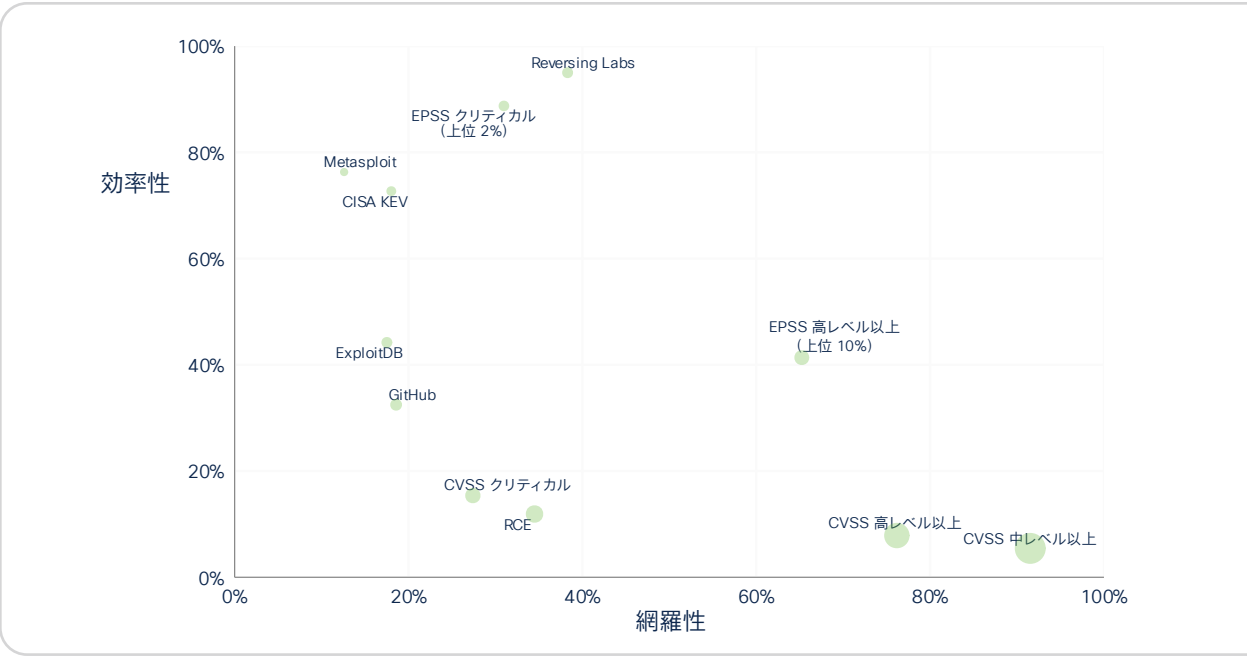

図 19. 単一のデータソースを使用した場合の、多様な修復戦略のパフォーマンス（右上にあるほど良好）

全体の傾向として、図 19 には網羅性と効率性の両立が難しいという特徴がよく表れています。悪影響を及ぼすおそれのあるすべての要素（CVSSv3 中レベル以上のすべて）に更新プログラムを適用すると、セキュリティチームにとっては不要な作業が増え負担になりますが、網羅性に優れます。対照的な位置（左上）にあるのが KEV です。KEV の脆弱性に更新プログラムを適用するだけであれば、さほど無駄な労力はかかりませんが、実際に悪用が確認されている脆弱性のおよそ 19% しかカバーできません [5]。この図を一つひとつ説明することはしませんので、読者の方は自由にデータソースを選んで検討してください。

ただし、図 19 の単一のデータソースは机上の空論の気味があります。修復対応にあたるうえで、データを 1 つだけ選んで修復戦略の根拠とする組織などありません。「上記のソースを論理的にどう組み合わせれば、最も右上に近づけるか」を検討することが、合理的な戦略と言えるでしょう。データソースの組み合わせから考えられる修復戦略のパターンは、膨大な数 [6] に上ります（「データソースが Metasploit または EPSS のクリティカルレベルと CVSS の高レベル、RCE で、ただし ExploitDB ではない場合など」）。そこで正反対の方向性である次の 2 つのアプローチを考えてみます。1 つ目のアプローチは、効率性を重視する組織のケースです。ある脆弱性がすべてのデータソースのサブセットに確認できた場合のみ、修復を行う方針とします。2 つ目のアプローチは、網羅性を重視する組織のケースです。複数のデータソースから任意のサブセットを選択し、ある脆弱性がいずれかのデータベースで確認できれば修復を行う方針とします。先ほどのデータソースのすべてのサブセットに対して、この 2 つの戦略を落とし込んだのが、図 20 です。

図 20. 複数のデータソースを使用するさまざまな戦略の組み合わせ

ここでの重要なポイントは、最善の戦略とは、さまざまな情報源を選び、そのいずれか（すべてではなく）に脆弱性が確認された場合に対処することです。左上の緑色の点は、非常に効率的ではありますが、網羅性はほとんどありません。無駄な労力はほぼ生じないものの、潜在的なリスクは増加します。対照的に濃青色の点（複数のデータソースの組み合わせ。いずれかのソースに CVE が見つかった場合は修復予定）は、はるかに広範囲に分布しています。多くの点は右下の方に集まっており、これらは労力はかかるものの高い網羅性を得られるのは確かですが、網羅率が 50% を超え効率性が 75% を達成している組み合わせも一定数あります。これは相当の効果です。パフォーマンスの高い戦略をいくつか挙げると、EPSS の上位 98% と Cisco Vulnerability Management の情報および Reversing Labs を組み合わせたものは特に優れた戦略と考えられます。KEV と Metasploit を追加することで網羅性をある程度向上させることができますが、その分効率はやや低下します。表の組み合わせから 1 つ選ぶ前に、ここで注意点を 1 つだけお伝えしておきたいと思います。これは当社のデータセットに含まれるすべての組織を対象にしたデータですが、お客様には適さない場合もあります。どの組織にもそれぞれ違うところがあり、したがって上記の組み合わせが馴染まないことも考えられます。大事なのは、適切な戦略とソリューションを選ぶことなのです。

まとめと推奨事項、振り返り

データ分析を通じて、KEV をさまざまな角度から眺め、それが脆弱性修復プログラムのどこに収まるのかを詳しく検討してきました。KEV は悪用された事実が他のソースによって証明できる脆弱性のリストであり、その規模は継続して拡大しています。KEV の脆弱性は同リストに掲載されていない脆弱性よりも重大度が高い傾向があり、たいていどの組織でも、1 度は自社資産でその脆弱性が確認されています。また KEV にはより大規模な脆弱性修復の領域で見られる傾向の多くが見られます。特に、修復が簡単な脆弱性は速やかに対応され、修復が困難な脆弱性は幾分対応に時間がかかるというものがあります。ネットワークのセキュリティ対策に関わる修復困難な脆弱性は、しばしば最重要事項であるにもかかわらず、同じような傾向があるのです。

最も重要なポイントは、KEV は脆弱性修復プログラムにとって有用な目安となる情報ではあるものの、これだけでは対策として不十分という点です。KEV の脆弱性の大半は、他のデータソースでも「悪用された」ことが確認されていますが、悪用が確認されている脆弱性の多くは、KEV ではカバーされていません。つまり KEV はどの組織にとってもこれ 1 つで完璧な対策ではなく、組織で KEV への準拠が求められていても、考えられるデータソースはすべて採用して脆弱性管理プログラムを構築する必要があります。

プログラムの構築にあたっては、脆弱性修復の特効薬になるようなデータソースはありません。中には確かに優れているもの（図 20 の EPSS、Reversing Labs、KEV カタログを参照）もありますが、全体像を把握するにはさまざまな情報源が不可欠です。その点、上のグラフは全体像を掴むにはちょうどよく、他のデータソースの組み合わせがそれぞれの組織にとって有益である可能性を示しています。とは言えさまざまなソースが必要になると複雑さが増すうえに、それらの脆弱性を取り込んで管理するためのプラットフォームがなければなりません。このまま続けるとセールストークになりかねないので、今回はここまでにします。参考にしていただけたなら幸いです。

詳細はこちら：cisco.com/jp/go/secure

注釈

1. 本レポートでは、CVE ID、CVE、脆弱性という用語を同じ意味で使用しています。同じものとして捉えてください。
2. 「エクスプロイト」の意味は人によって異なることに注意してください。シスコでは、既知のエクスプロイトコードまたは PoC を含む脆弱性と、活発に悪用されている脆弱性を区別し、言及する際に矛盾がないようにしています。
3. 経時的なスコアが表しているのは、ここで評価を試みているエクスプロイトのほんの一部です。汎用性があるわけでもないため、このスコアについては詳しく説明しません。また、CVSS のメトリクスの環境グループは組織固有のものであり、すべての組織に当てはまるわけではないため、ここでは無視します。
4. 的確な分析を行うため、現用資産が 100 未満の組織は除外しています。
5. この点はすでに説明しましたが、重要なことなのでもう一度触れておきます。
6. 2^{2047}-1 は、正確には「≈ 1.6 * 10^{616}」です。