脆弱性に関する動向（I）

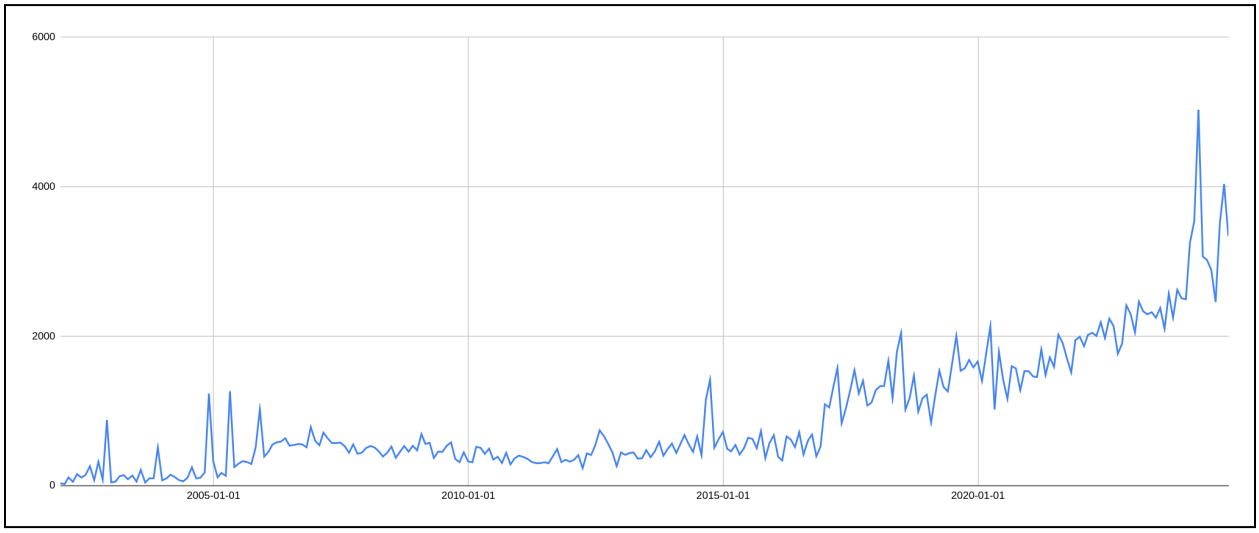
1. 2024年の脆弱性に関する動向

CVE/CVSSの情報から、2024年までの脆弱性に関する動向を見てみます。

1-1. 全体的な脆弱性動向

1-1-1. Totalの脆弱性動向

下図が2002年1月から2024年12月までに公開された、月ごとの脆弱性数の推移になります。



（脆弱性の動向・Rejectedのものは除く2002年1月～2024年12月）

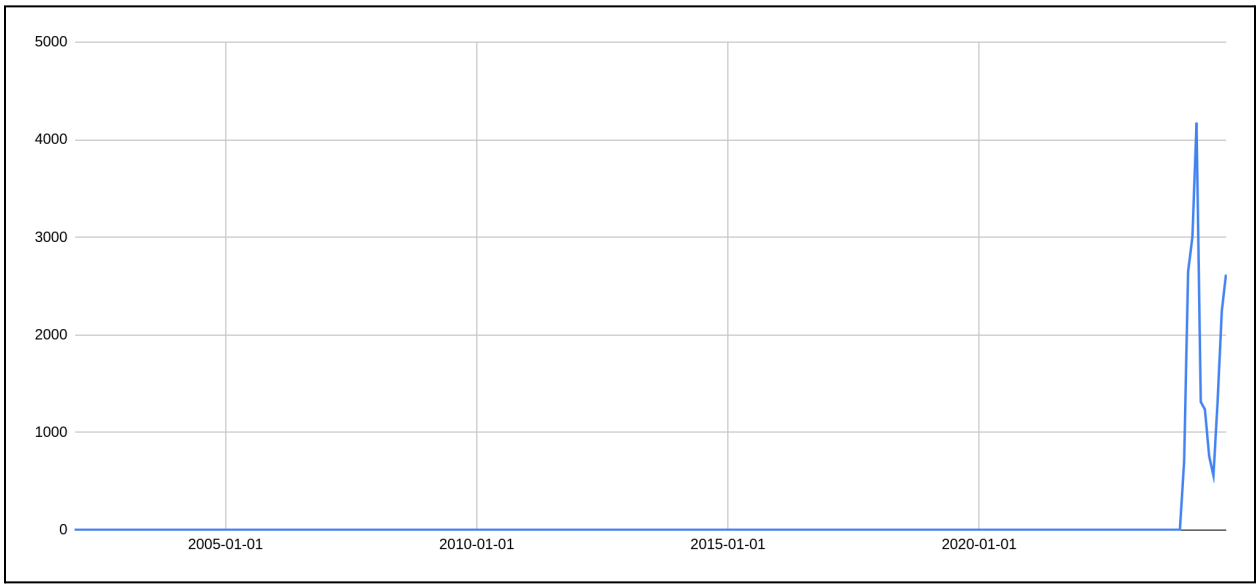
全体的な傾向としては2015年ぐらいから右肩上がりに推移しており、2024年5月には最大で5023/月となりました。これは一日平均170件ほどとなっており、既に人間の手で全ての脆弱性を追いかけるのが難しくなっている現状が伺えます。

しかし、この2024年5月の傾向はちょっと異常値な気がします。少し調べてみましょう。

1-1-2. Awaiting Analysis（2025/01時点）の動向

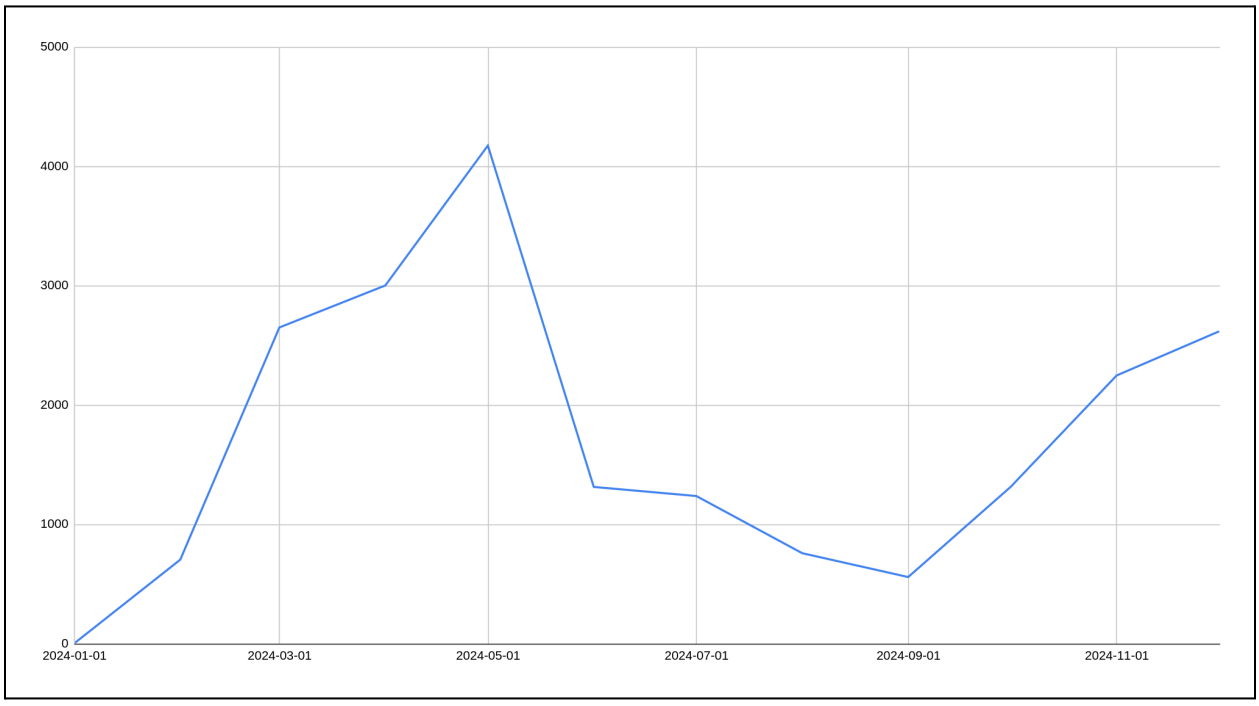
下図は「Awaiting Analysis（CVSSスコアリングの解析待ち）（2025/01時点）」の脆弱性数の推移になります。

いままでは「解析待ち」がそれほど発生していませんでしたが、2024年からいきなり発生していることがわかります。ちなみにこの「Awaiting Analysis」の状況は、2025/01時点での調査となっており、時間とともに数は減少していることを念頭に置いておく必要があります。



（Awaiting Analysis（2025/01時点）の数の状況:2002年1月～2024年12月）

さらに拡大して、2024年1月から2024年12月までの状況を見てみます。

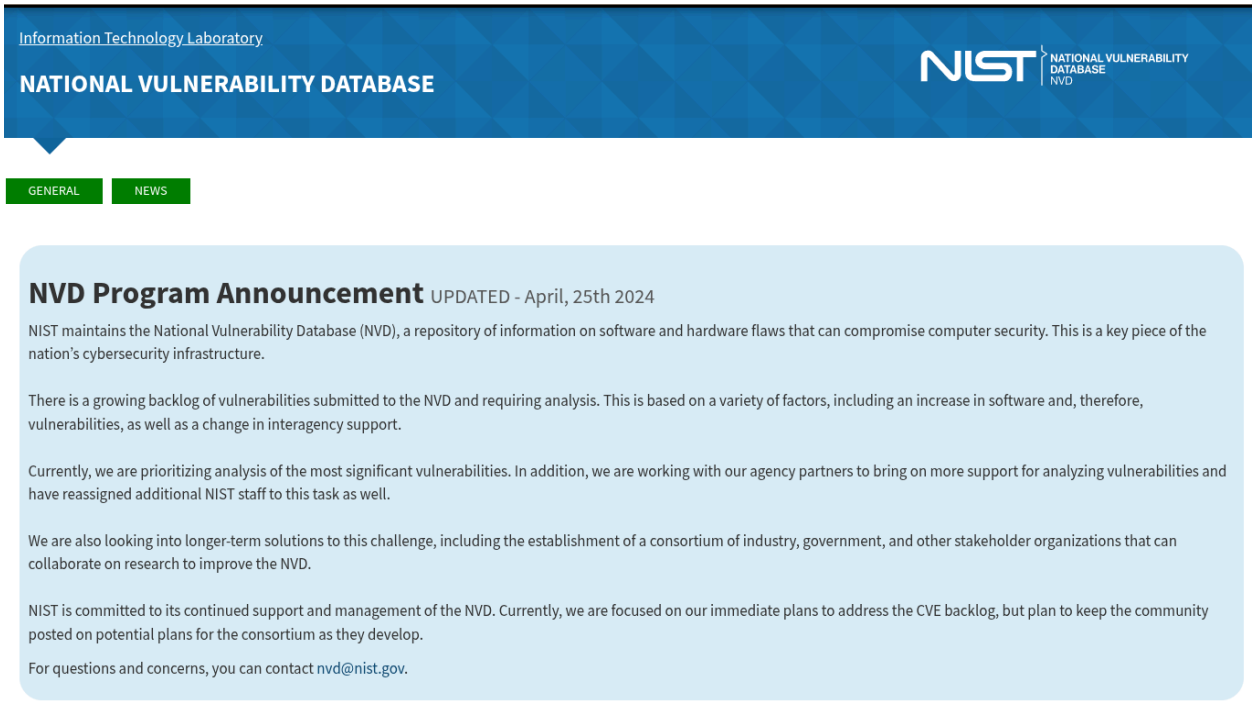


（Awaiting Analysis（2025/01時点）の数の状況:2024年1月～2024年12月）

このように、2024年5月をピークに「Awaiting Analysis」が多くなっています。

1-1-3. NISTの予算問題とbacklog(やり残し)

この「Awaiting Analysis（以下、backlog（やり残し）とも表現します」の件に関しては、NISTから声明が出ています。



（NISTのNVDでのbacklogに関するアナウンス）

NISTの発表によると、この「backlog（やり残し）」の理由としては

- 対応するべきソフトウェアの増加による脆弱性の増加、および省庁間のサポートの変更など、さまざまな要因に基づいている

とされています。

そもそも、NISTですが（全てのセキュリティ研究者はNISTの成果物に頼っているわけですが）、予算の問題に直面していました。

NextGov:「NIST's emerging tech work will be 'very difficult' without sustained funding, director says」の2024年5月時点でのニュースによると、NISTの2024年度予算が前年比10%削減されるという「壊滅的な」状況に直面しているとの事です。
その中で脆弱性の著しい増加という事があり、予算等の問題からも「さばききれない」状態が続いていた模様です。

NISTは2024年5月下旬にメリーランド州のサイバーセキュリティ企業Analygenceと86万5657ドルの業務委託を締結して、backlogの解消に努めています。

NISTはNVDの2024/11/13のNewsでbacklogについてbacklogを解消できる時期に関する当初の見積もりが楽観的だった事を認めており

- backlogにあった既知の悪用された脆弱性 (KEV) にもすべて対処しており、新たに到着するすべての KEV も処理している。
- ADPから受け取っているbacklogのデータが効率的にインポートできない形式だった為、新システムの開発を行っている。
- できる限り早く完了することに取り組んでいる。

と発表しています。

- **November 13, 2024: NVD General Update**
  This update provides information on our progress as we work to process all incoming Common Vulnerabilities and Exposures (CVEs) and to address the backlog of CVEs that built up earlier this calendar year.

  We now have a full team of analysts on board, and we are addressing all incoming CVEs as they are uploaded into our system. In addition, we have addressed all Known Exploited Vulnerabilities (KEVs) that were in the backlog, and we are processing all new KEVs as they come in.

  However, our initial estimate of when we would clear the backlog was optimistic. This is due to the fact that the data on backlogged CVEs that we are receiving from Authorized Data Providers (ADPs) are in a format that we are not currently able to efficiently import and enhance.

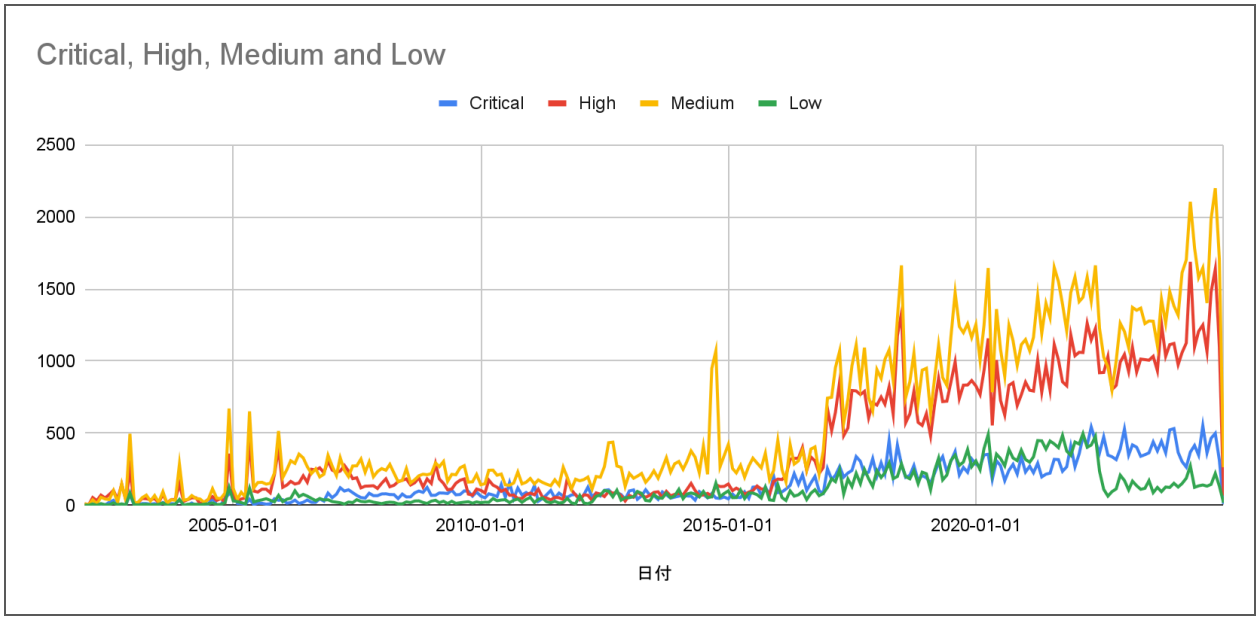
  To address this issue, we are developing new systems that will allow us to process incoming ADP data more efficiently. We are working to complete this project as quickly as possible and will continue to provide updates on our progress to this NVD Updates page.

（NISTのNVDでのbacklogに関するアップデート）

1-2. 脆弱性の重大性(Severity)動向

1-2-1. 重大性の動向

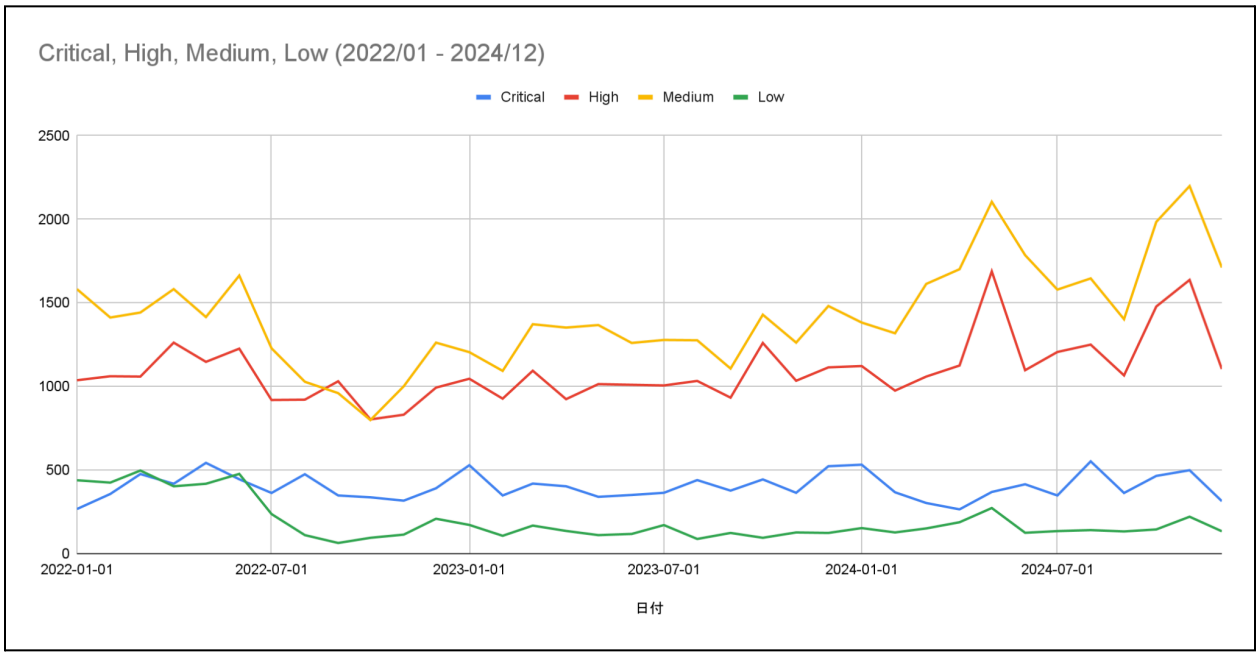
下のグラフは、重大性としてCVSSスコア（CVSS v2.0 ～v4.0）のトータルを元にCritical/High/Medium/Lowで分けたものになります。全体的な傾向としては、High, Mediumが右肩上がりのグラフとなっておりCritical/Lowはそれほど伸びがない様に見えます。



（Total Severityの動向:2002年1月～2024年12月）

1-2-2. 重大性の動向(2022-2024)

下のグラフは、重大性としてCVSSスコア（CVSS v2.0 ～v4.0）のトータルを元にCritical/High/Medium/Lowで分けたものを特に2022年1月から2024年12月までに注目したものになります。やはり傾向としては、High, Mediumが右肩上がりのグラフとなっておりCritical/Lowはほぼ横ばいの様に見えます。全体的な傾向の話をしたときに触れましたが、Awaiting Analysisが増えている辺りはMeium/Highが多くなっているように見えます。



（Total Severityの動向:2022年1月～2024年12月）

1-2-3. Awaiting Analysisの中の重大性割合

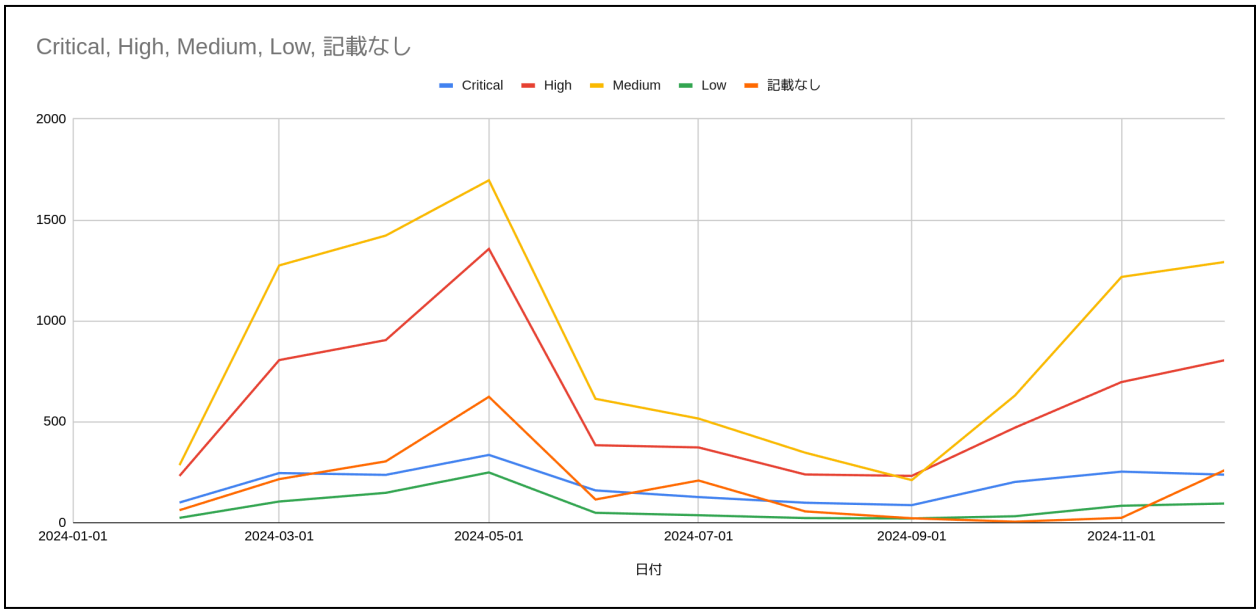
1-1-2でも解説しましたが、この「Awaiting Analysis」はあくまでも2025年1月調べのものだと認識する必要があります。

Awaiting Analysisはあくまでも

- NVDによるCVSS/CPEなどの分析待ち

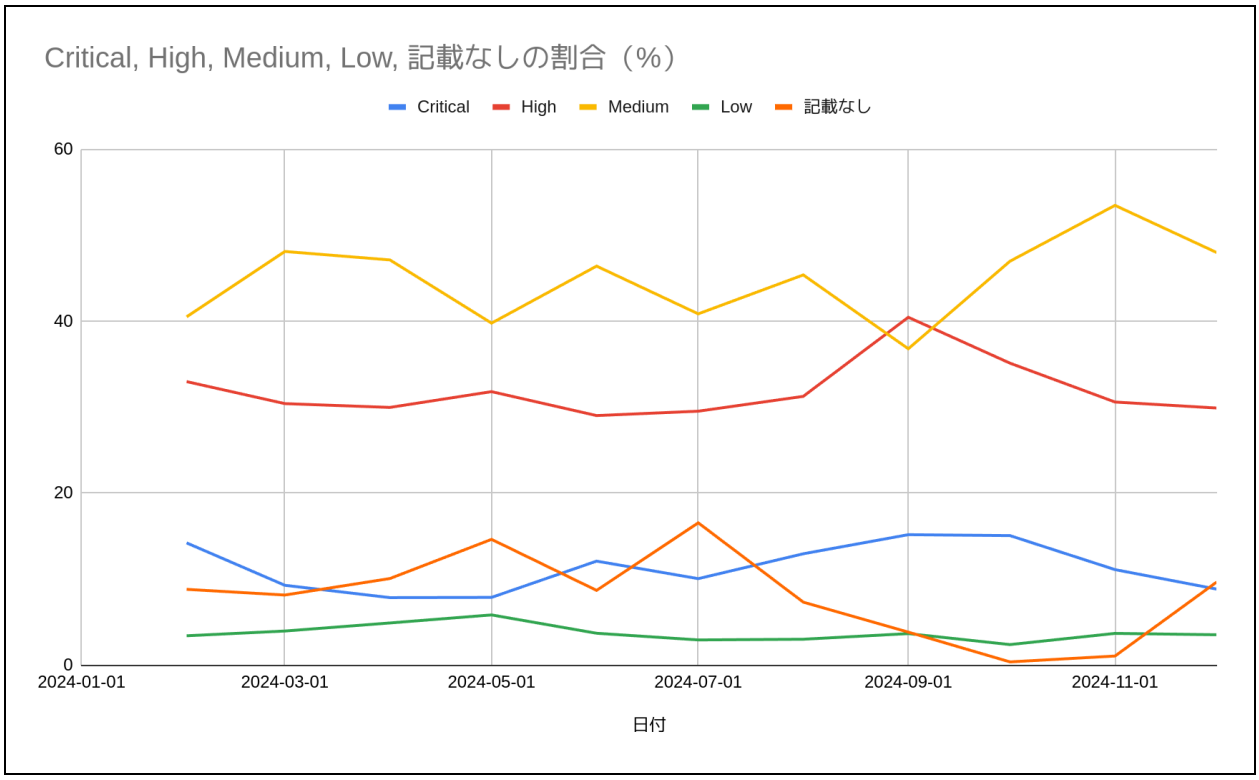
というステータスであり、（Microsoft・Ciscoなど）CNAやベンダーが付加したCVSSによるBase Scoreなどの重大性は別途付加されているものがあります。

実際に2025年1月時点での「backlog（やり残し）」扱いとなっているものの中で、どのくらいの重大性があるのかの月ごとの分布(数)を見てみましょう。



（Awaiting Analysis（2025/01時点）の数の月ごとの分布とステータスの内訳:2024年1月～2024年12月）

数では月ごとのCVEの数による出っ張り・引っ込みがあるので判然としません。そのため、実際に2025年1月時点での「backlog（やり残し）」扱いとなっているものの中で、どのくらいの重大性があるのかの月ごとの分布(%)を見てみましょう。



（Awaiting Analysis（2025/01時点）の%の月ごとの分布とステータスの内訳:2024年1月～2024年12月）

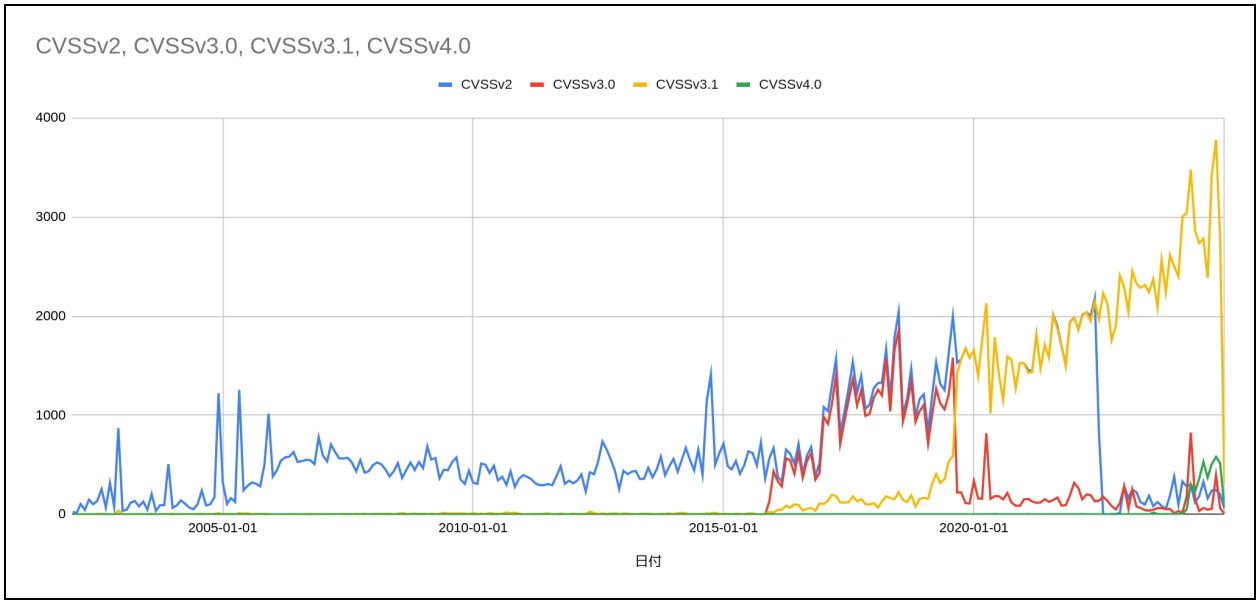
こうしてみると、上下幅はありますが内訳としてCritical/High/Medium/Lowの割合がほぼ均質になるように処理をしていっているのではないかと推定されます（あくまでも推定です）。

1-3. CVSS v4.0の動向

CVSS v4.0は2023年11月にリリースされた新しいバージョンの重大性スコアリング指標になります。

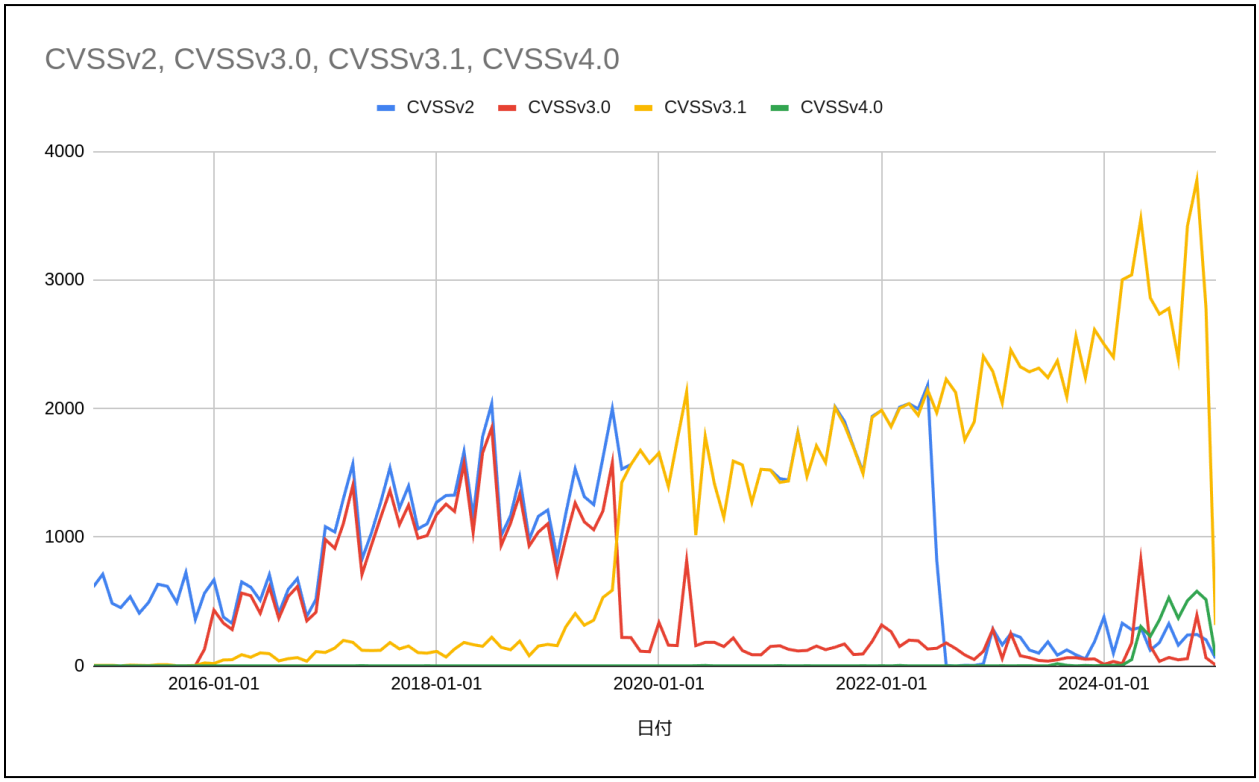
1-3-2. CVSS v4.0に着目した重大性割合

CVSS v4.0がリリースされた事を踏まえて、各CVSSのバージョンがどのように推移しているかを見てみましょう。下記のグラフは2002年1月～2024年12月までの各CVSSバージョンの占める数の推移になります。**CVSSv2, CVSSv3**など複数が記載されている**CVE**に関しては両方のバージョンでカウントしている形になります。



（各CVSSバージョンの占める数:2002年1月～2024年12月）

2015年1月～2024年12月を拡大します。

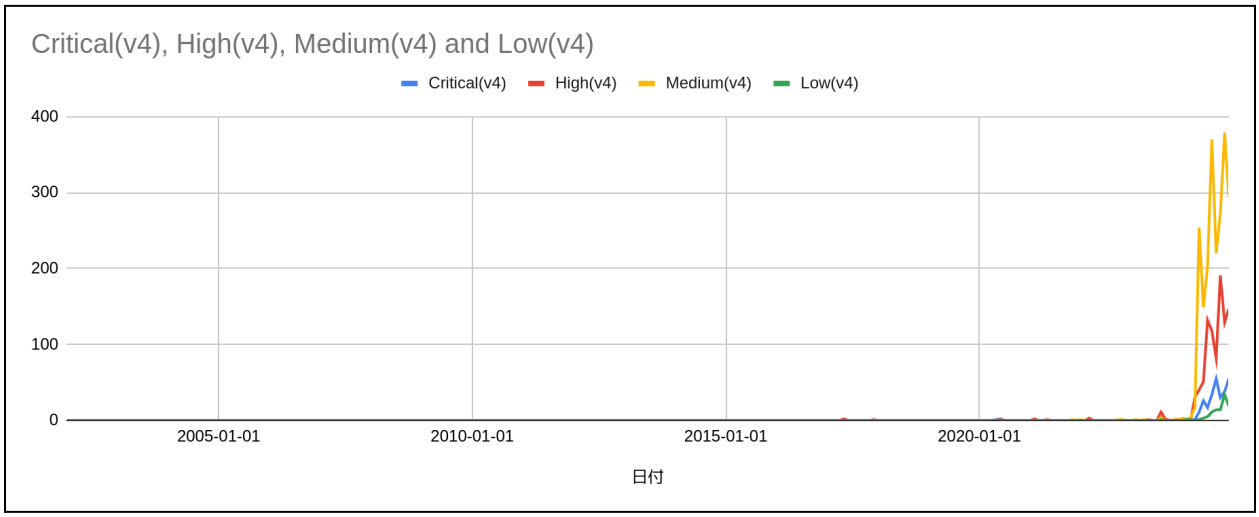


（各CVSSバージョンの占める数:2015年1月～2024年12月）

グラフから見る限り、CVSS v3.0 -> v3.1の移行が4年くらいかかっているように見えるため、CVSS v4.0への完全移行（メインがv4.0になる）までは4年くらいかかる可能性があります。実際にはメーカーでも脆弱性に関する意識が上がっているため、2026年くらいにはv4.0がメインで使われるようになる可能性があると考えられます。

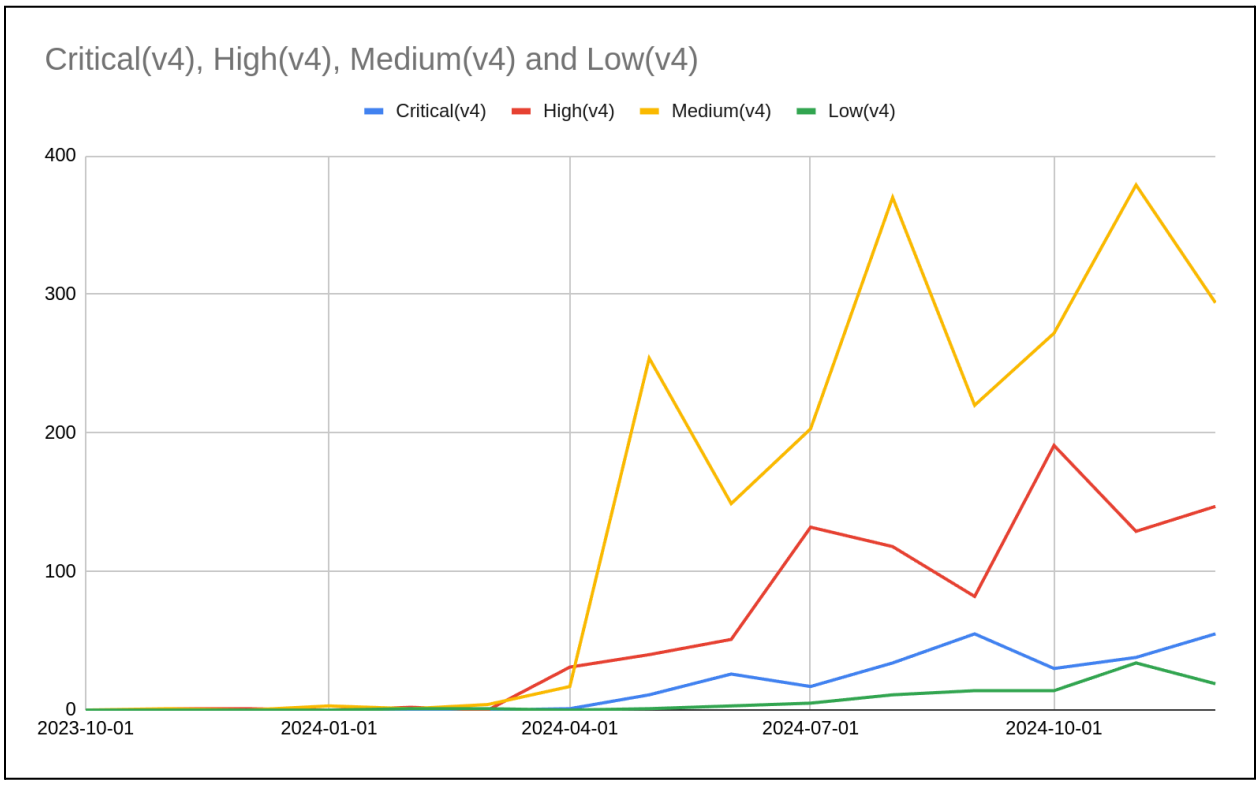
1-3-2. CVSS v4.0に着目した重大性割合

次にCVSS v4.0での脆弱性の割合を見てみましょう。



（CVSS v4.0での Severityの動向:2002年1月～2024年12月）

見えにくいので、2023年10月～2024年12月に拡大してみます。



（CVSS v4.0での Severityの動向:2023年10月～2024年12月）

2024年3月頃からCVSS v4.0が使われだしていることがわかります。また、重大度の順位は全てのバージョンTotalでの重大度の順位と同じくMedium, High, Critical, Lowの順に並んでいることがわかります。

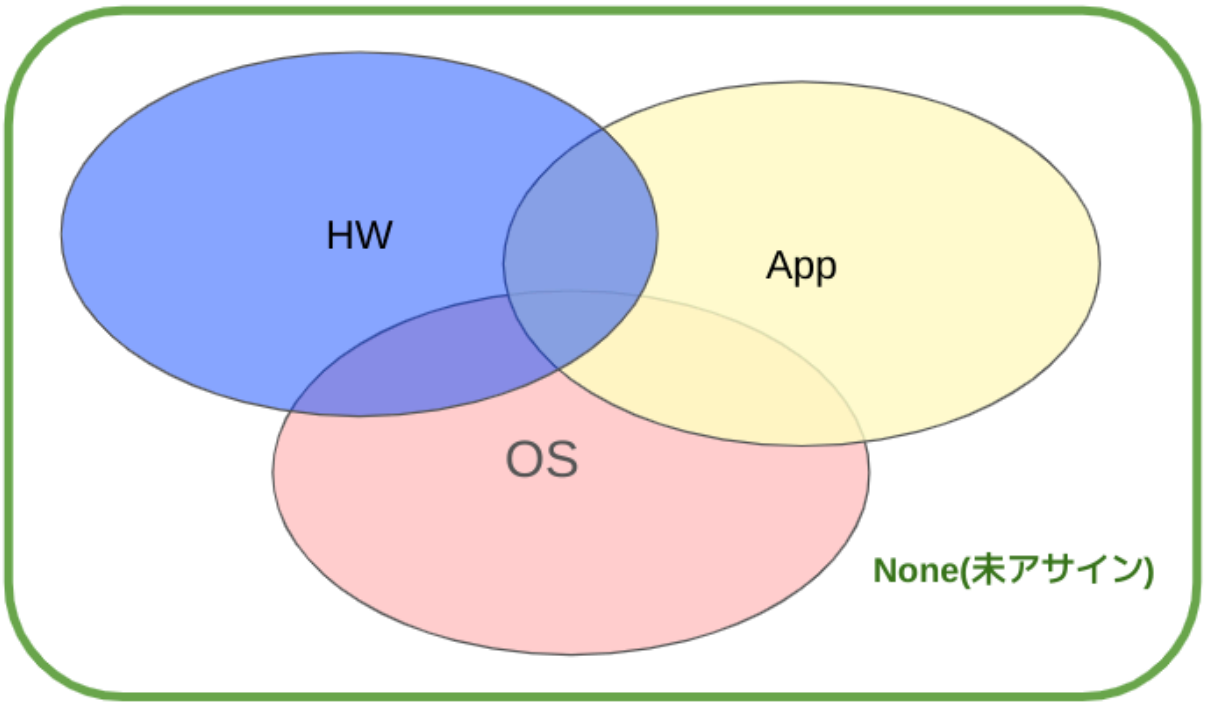
1-4. 脆弱性対象(CPE)動向

次に、CPEでHW,OS,Appに分けた際に脆弱性がどの様に推移しているかを見てみましょう。CPEは例えばPAN-OSのようにHW/OSの両方が付けられていたり、qemuのようにOS/Appの両方が付けられていたりするためはっきりと分けるのは難しい状況です。

便宜上

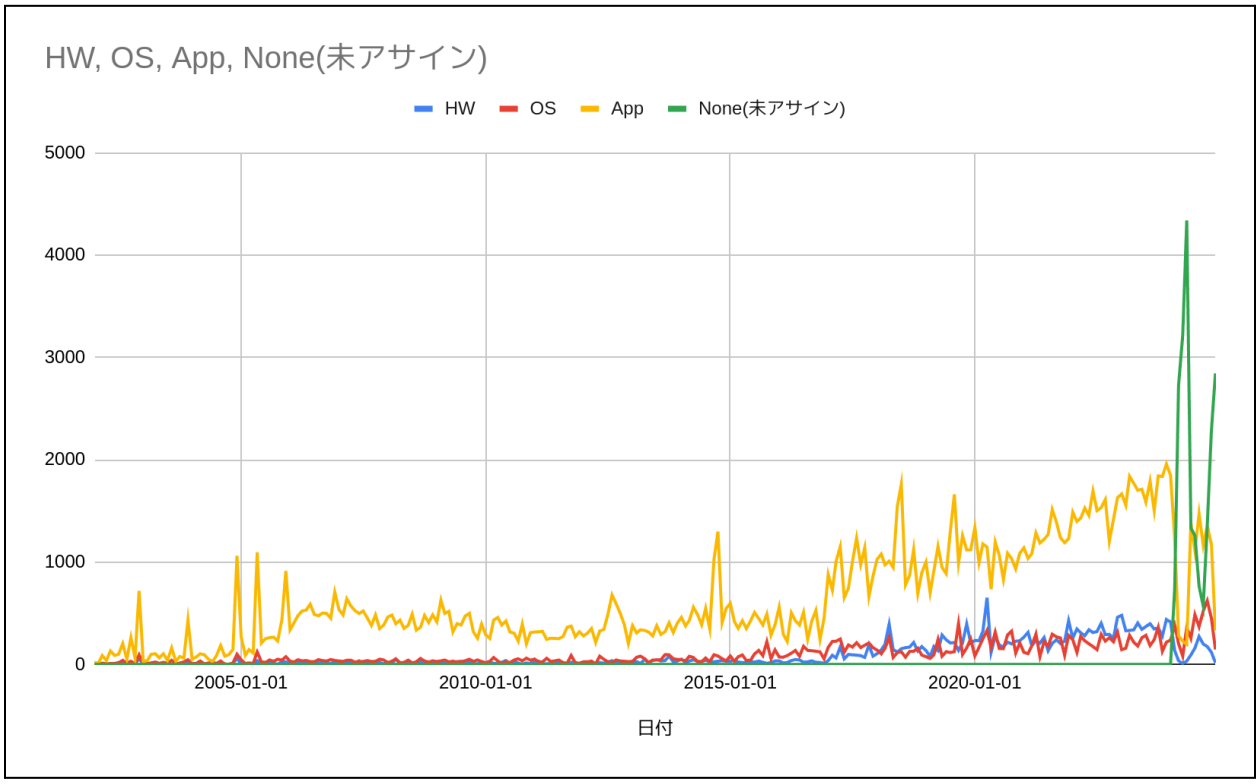
- HW
    - CPEでHW(cpe:2.3:h)が含まれるもの
- App
    - HWを除いて、CPEでApp(cpe:2.3:a)が含まれるもの
- OS
    - CPEでOS(cpe:2.3:o)が含まれるもの

に分けています。



1-4-1. HW,OS,App, None(未アサイン)でのCVE発行数の動向

下記がCPEを用いて脆弱性をHW/OS/App/None(未アサイン)で分けたものになります。



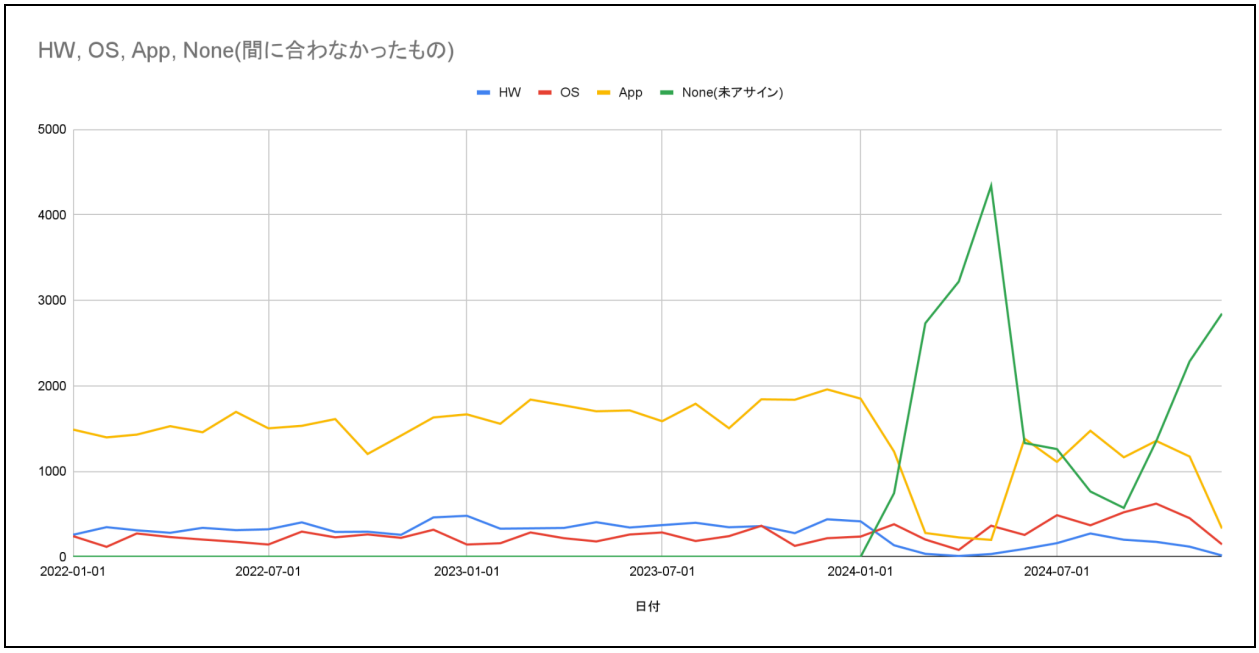
（HW/OS/App/NoneのCVE数の動向:2002年1月～2024年12月）

先述のNISTの問題で未アサインが多いところがありますが、それを考慮から外すと2002年からの全体的な傾向では

- Appは右肩上がり
- HW/OSはAppほどではないが上がっている

と言えます。

2022年1月～2024年12月を拡大したものが以下になります。



（HW/OS/App/NoneのCVE数の動向:2022年1月～2024年12月）

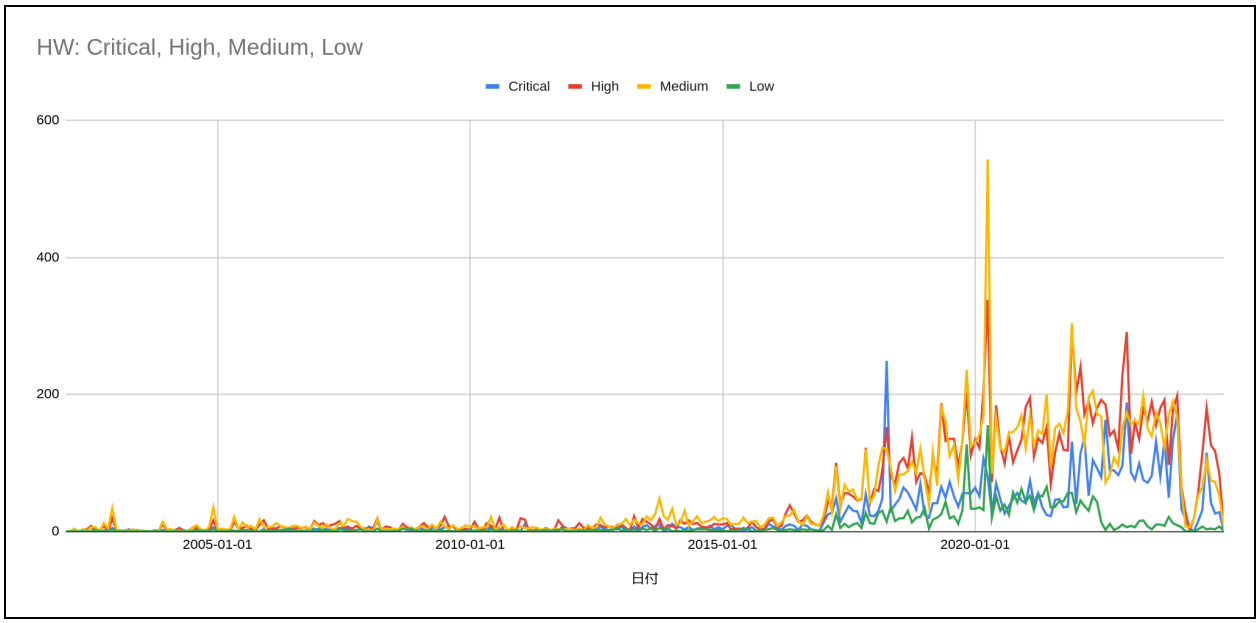
先述のNISTの問題で未アサインが多いところがありますが、それを考慮から外すと2022年からの全体的な傾向では

- Appはほぼ横ばい（下がっている部分はbacklog(積み残し)の影響が大きそう）
- HW/OSは若干の伸び

と言えます。

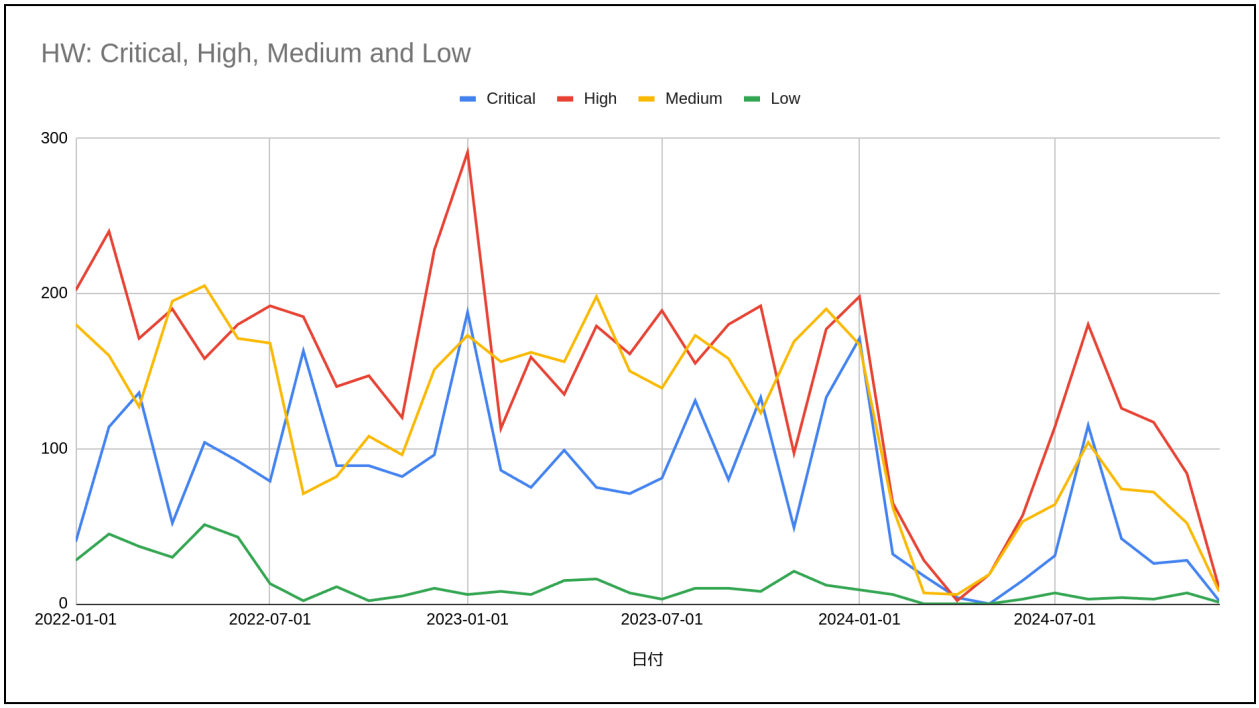
1-4-2. HWでの重大性の動向

下記がHWの中でさらに重大度ごとにCritical/High/Moderate/Lowに分けたものになります。なお、”Awaiting Analysis”のものはCPEが振られていないため、こちらのHW/OS/APPの結果からは除外されていることに注意してください（1-4冒頭の集合図参照）。



（HWでのSeverityの動向:2002年1月～2024年12月）

特に2022年1月～2024年12月を拡大したものが以下になります。

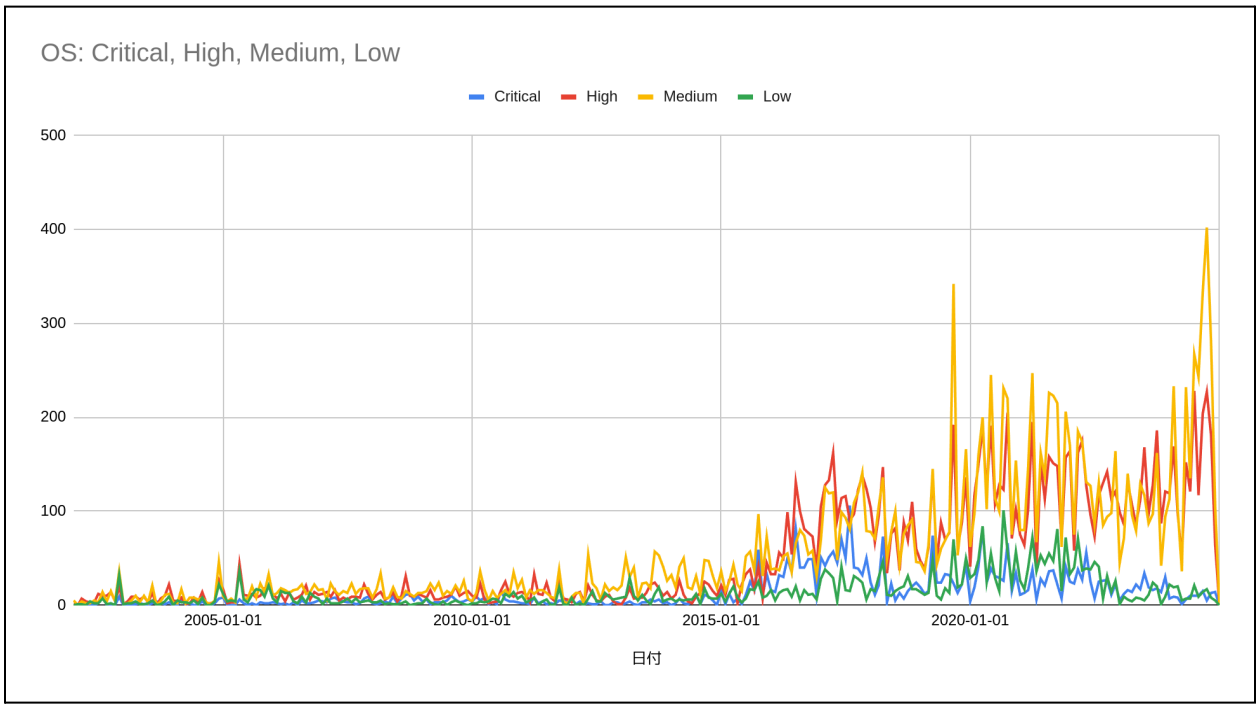


（HWでのSeverityの動向:2022年1月～2024年12月）

ばらつきはありますが全体的にLowが低くCritical/High/Mediumが均等に多くなっているように見えます。これはHW製品（ファームウェアなど）という性質上からくるものと思われます。

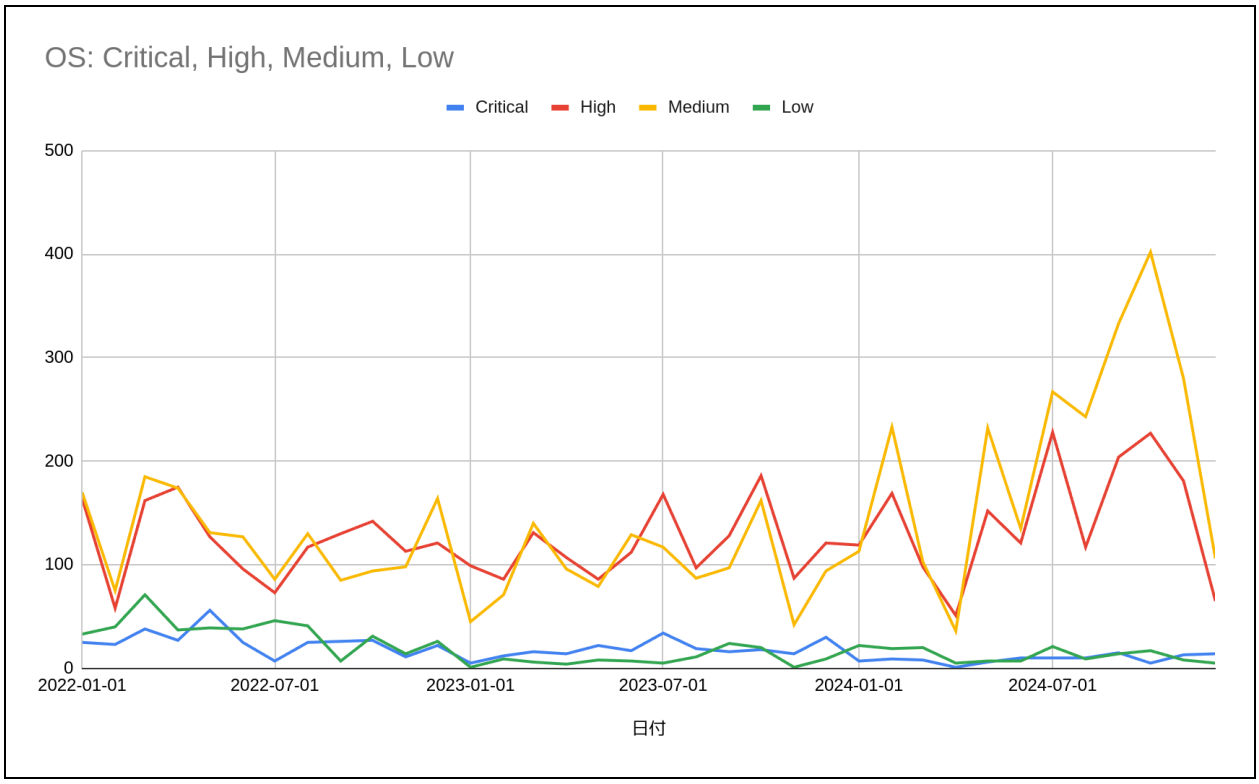
1-4-3. OSでの重大性の動向

下記がOSの中でさらに重大度ごとにCritical/High/Moderate/Lowに分けたものになります。



（OSでのSeverityの動向:2002年1月～2024年12月）

2022年1月～2024年12月を拡大したものが以下になります。



（OSでのSeverityの動向:2022年1月～2024年12月）

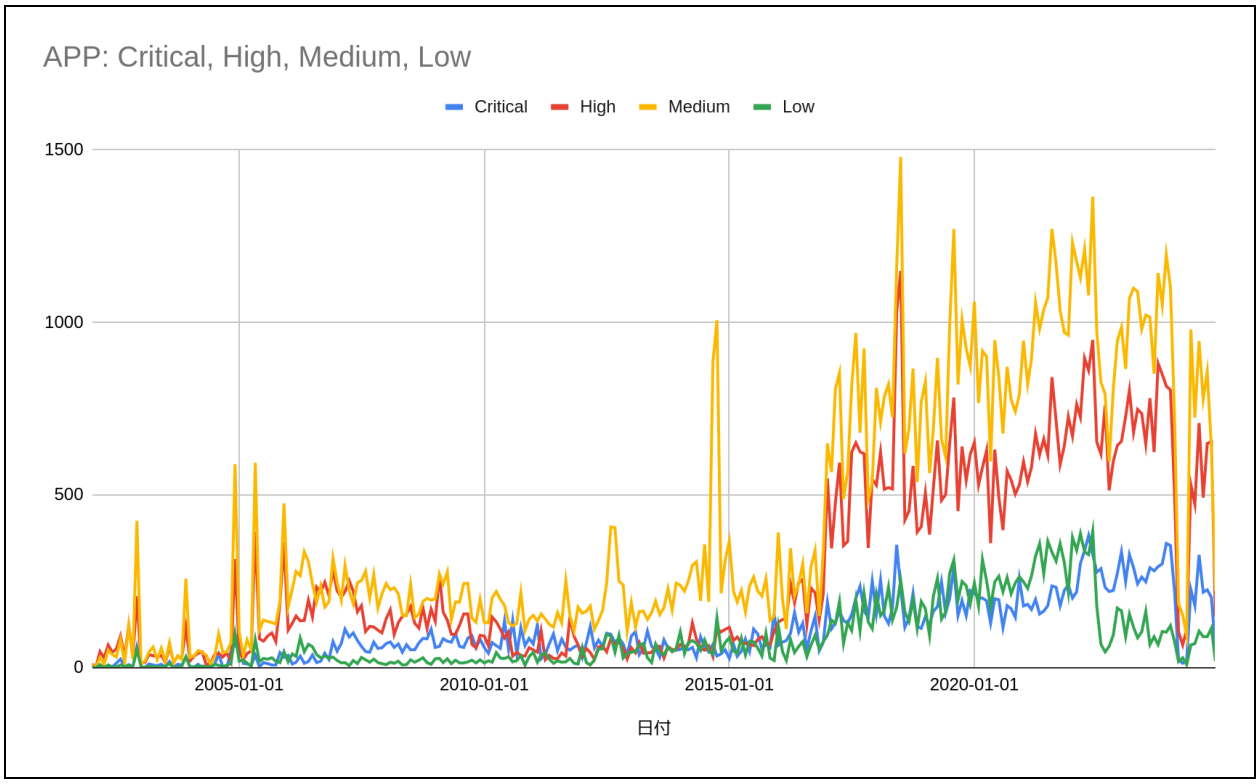
OSに関してはHigh/Mediumが右肩上がりになっているように見えます。一方でCritical/Lowはあまり変化がないように見えます。この理由としては

- OSという安定したもののためCriticalの数はそれほど多くならない
- とりあえずMedium/Highにしてしまうケースが増えているのではないか

と考えられます。

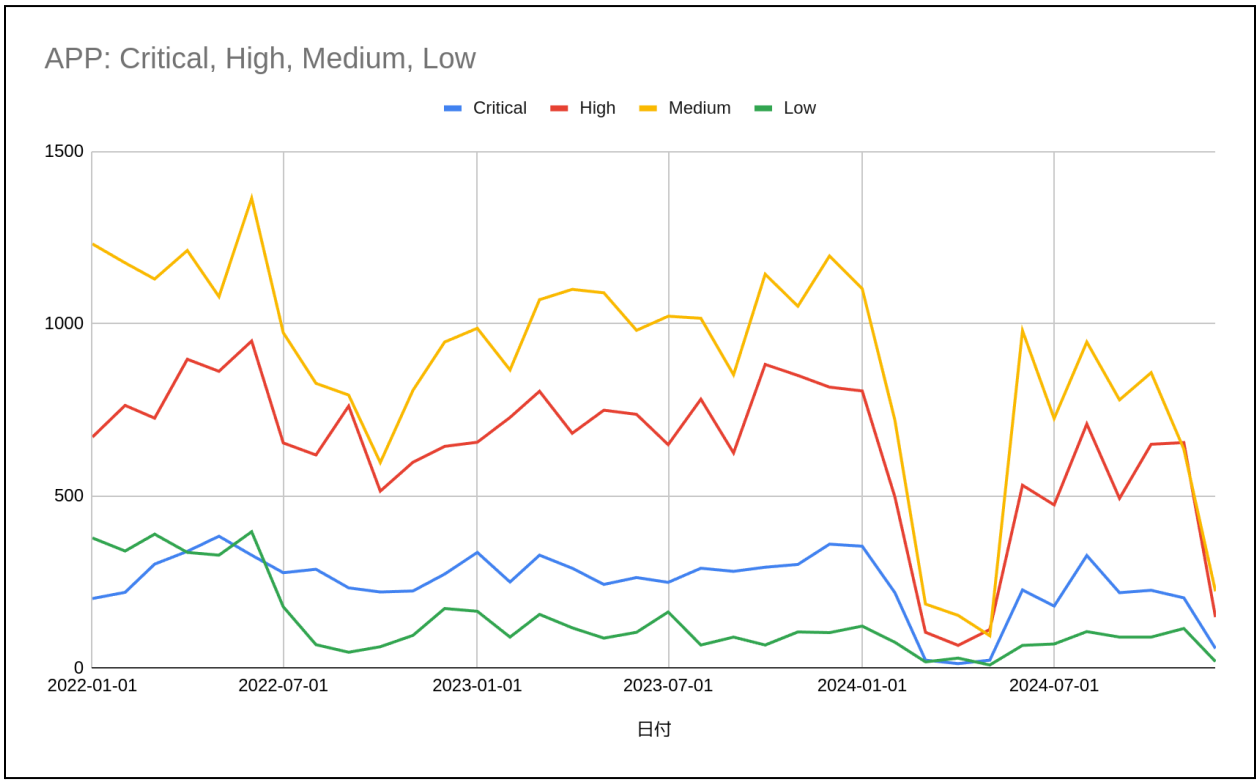
1-4-4. APPでの重大性の動向

下記がAPPの中でさらに重大度ごとにCritical/High/Moderate/Lowに分けたものになります。なお、”Awaiting Analysis”のものはCPEが振られていないため、こちらのHW/OS/APPの結果からは除外されていることに注意してください（1-4冒頭の集合図参照）。



（APPでのSeverityの動向:2002年1月～2024年12月）

2022年1月～2024年12月を拡大したものが以下になります。



（APPでのSeverityの動向:2022年1月～2024年12月）

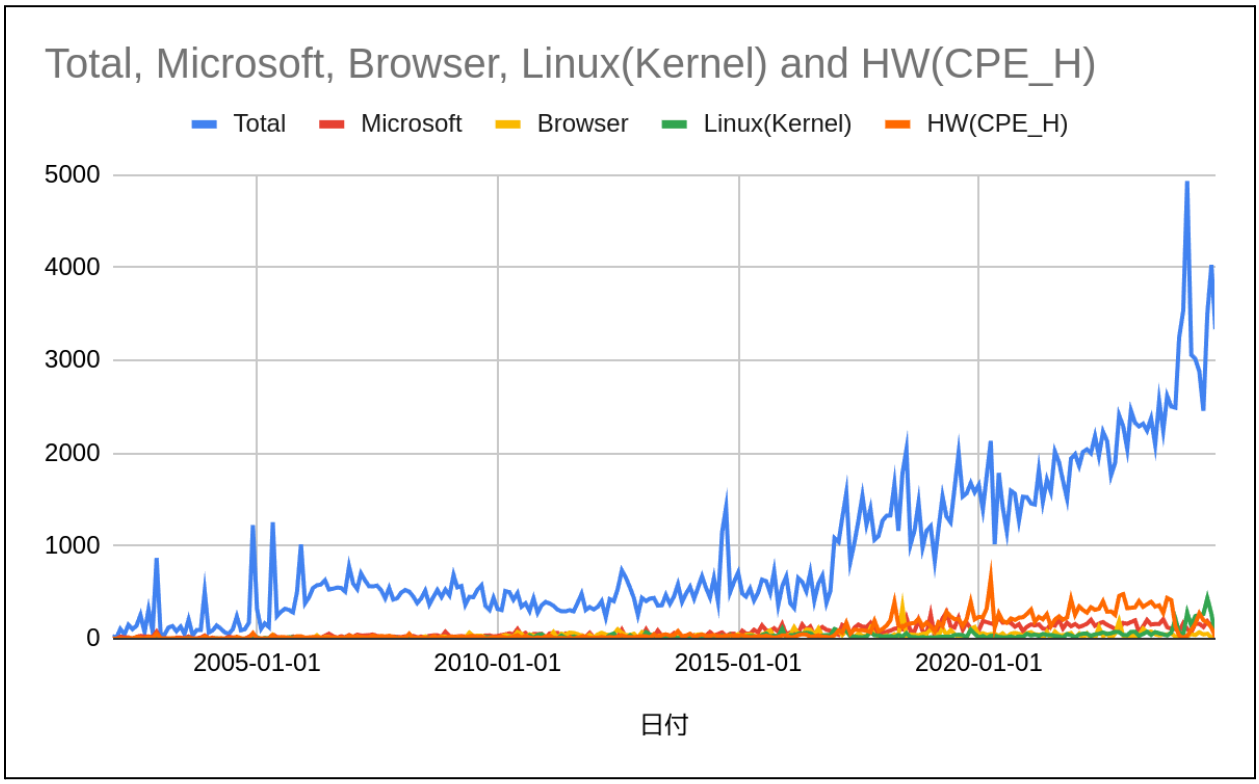
意外なことに、2024年はAPP(アプリケーション)に関してはほぼ横ばいだったことがわかります。

2. 各製品の動向

以下では代表的な製品の動向について見ていきます。

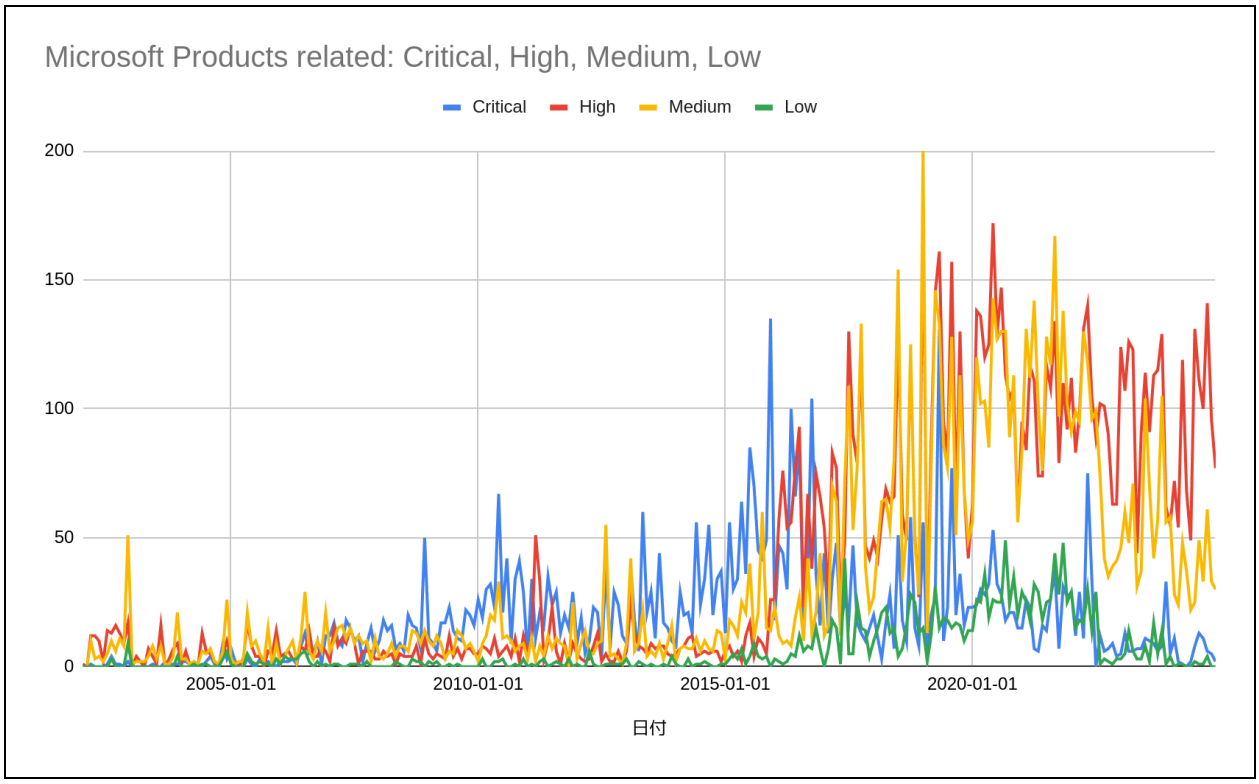
2-1. 全体の脆弱性の動向と各製品別の動向

下記は2002年1月～2024年12月までの脆弱性の動向（Total）と
Microsoft/Browser/Linux(kernel)/HW(CPE_H)の動向です。



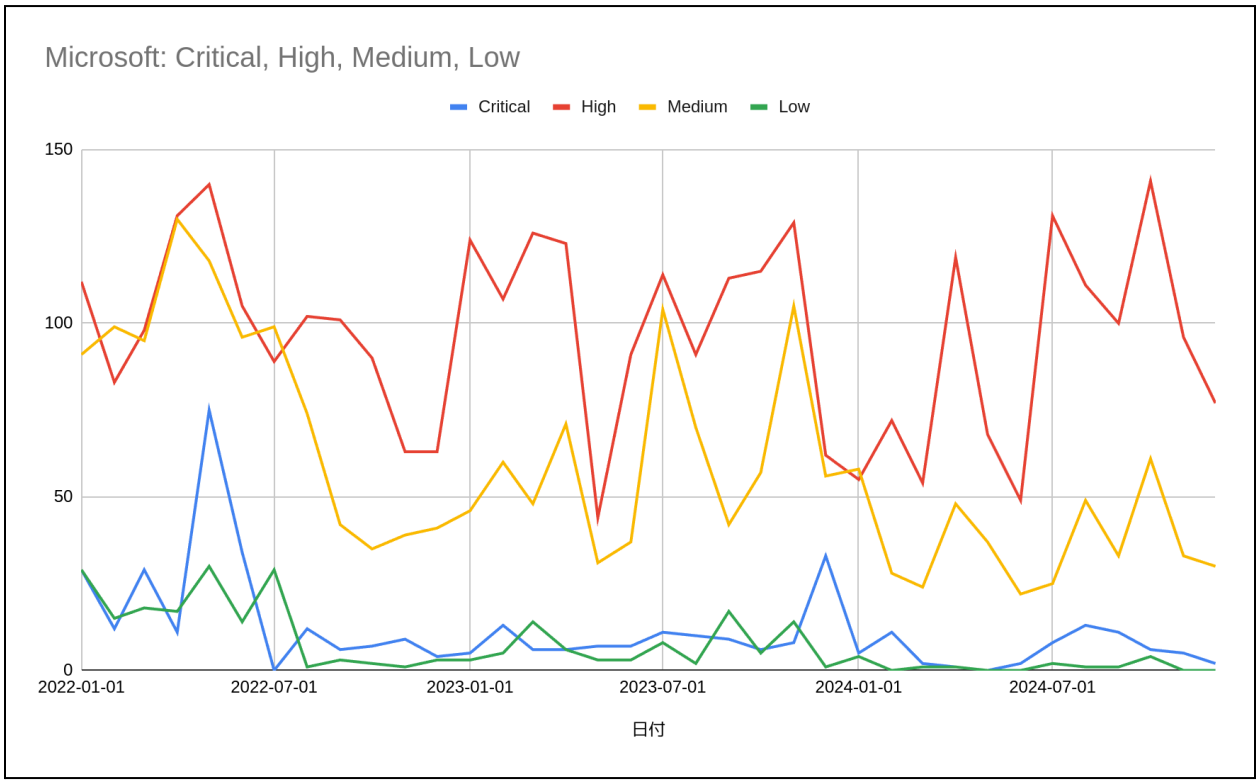
2-2. Microsoft製品の脆弱性

Microsoftの脆弱性の動向はこのようになっています。ただし、Google ChromeなどもCPEとして「microsoft」がついてしまっているため、現実にはこの数よりも割り引いて考える必要があります。



（Microsoft製品のSeverityの動向:2002年1月～2024年12月）

2022年1月～2024年12月までの動向はこのようになっています。



（Microsoft製品のSeverityの動向:2022年1月～2024年12月）

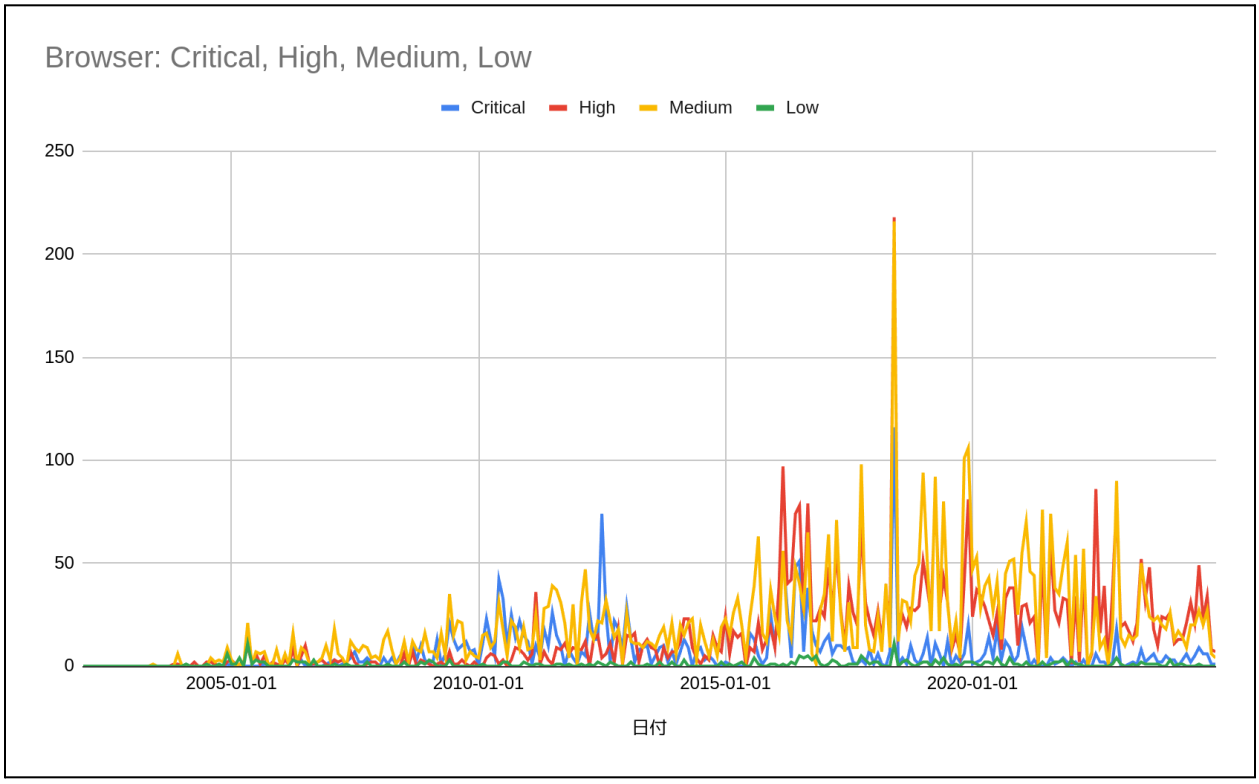
Microsoft製品に関しては、近年の動向はそれほど変化がないように見受けられます。

2-3. ブラウザ製品の脆弱性

ブラウザ製品として

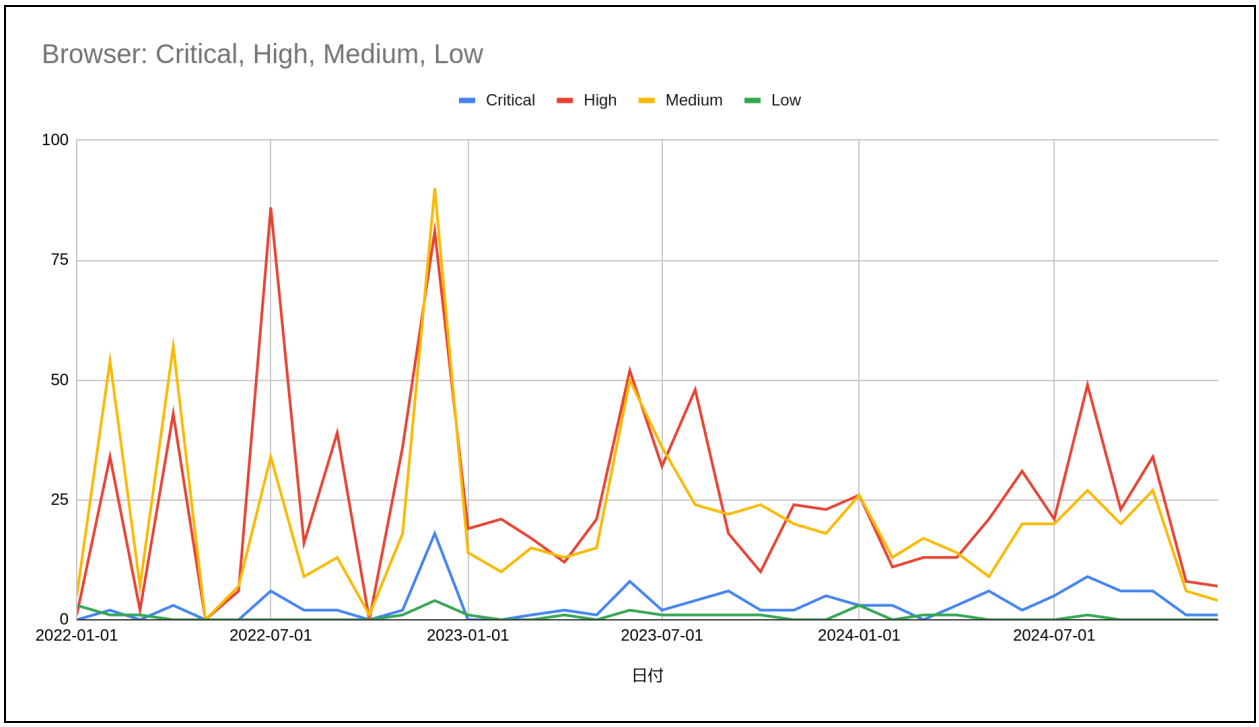
- Chrome
- Firefox
- Edge
- Safari
- Opera

をひとまとめにして脆弱性の動向を見てみます。



（ブラウザのSeverityの動向:2002年1月～2024年12月）

2022年1月～2024年12月までの動向はこのようになっています。

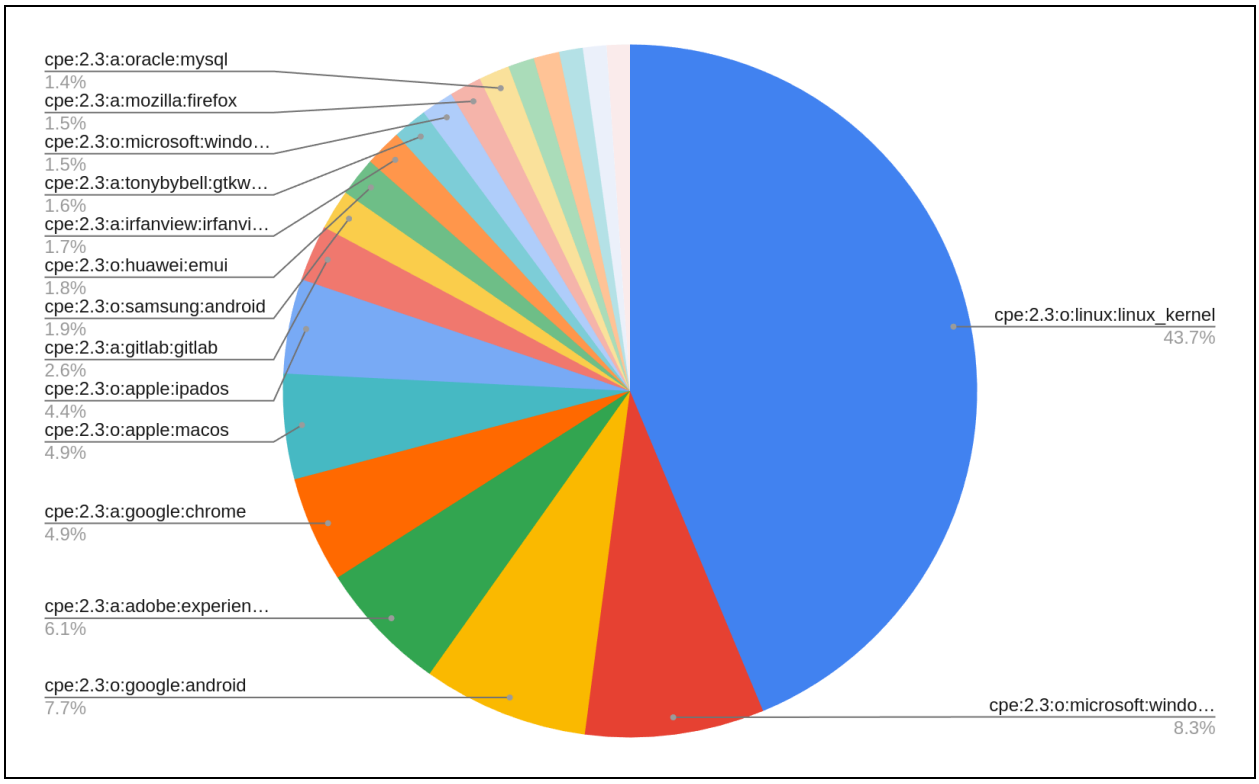


（ブラウザのSeverityの動向:2002年1月～2024年12月）

Critical, High, Mediumが多くLowが少ないため、アタックサーフェースの観点から行くとブラウザ周りの対処が重要な事が伺えます。

2-4. 2024年で脆弱性が見つかった製品のTop20

　下記は2024年で脆弱性が見つかった製品のTop20になります（CPEの一番左側に出てきたものを直接脆弱性に関係するCPEと考えてカウントしています）。



（脆弱性が見つかったCPEのTop20:2024年1月～2024年12月集計）

Linux KernelがCVEを発行するようになったため、かなりの数のLinux Kernelの脆弱性が上がっています。これは「Linux Kernelでパッチのコミットの際にきちんと脆弱性の確認と報告がなされるようになった」という意味で良い進歩と捉えて良いと思います。

3. 参考資料

1. NectGov: Can NIST get it all done?
2. NextGov: NIST’s emerging tech work will be ‘very difficult’ without sustained funding, director says
3. NIST: news updates:
4. CISA KEV: Known Exploited Vulnerabilities Catalog