

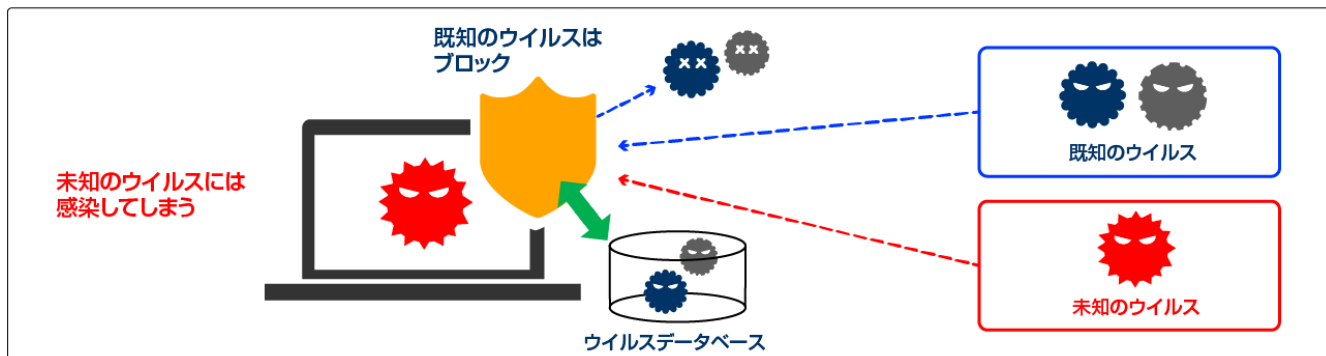
状況認識技術とは？

状況認識技術とは、周辺の状況や環境等のすべての情報を総合して認知し、その状況に最適な対応を行う技術です。

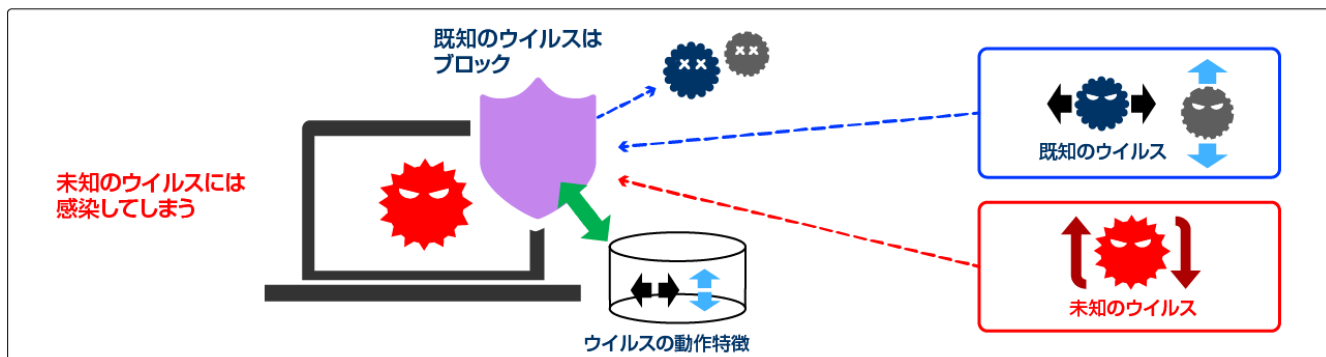
従来の対策方法ではランサムウェア自体、または、振る舞いの特徴を検出するなど、ランサムウェア自体に注目していましたが、状況認識技術では、ランサムウェアが変更・毀損する**ファイルに注目**しています。

例えば、**ファイルの変更箇所、速度、頻度などのファイルオペレーションを監視、記録**してランサムウェアの検出、および、ファイル変更箇所の復元に役立っています。

シグネチャ方式

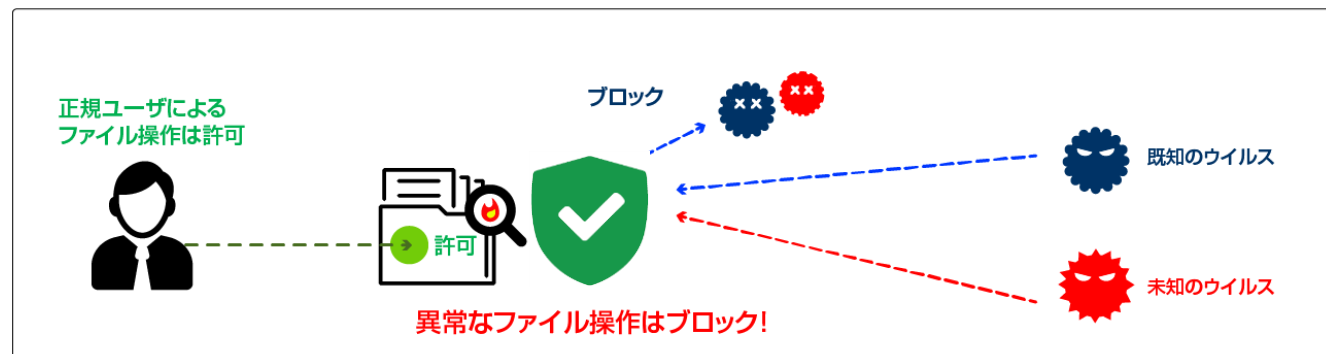


振る舞い検知方式



※シグネチャ方式も振る舞い検知方式も、未知のウイルスの場合その特徴や振る舞いを知らないため検出できない。

状況認識方式

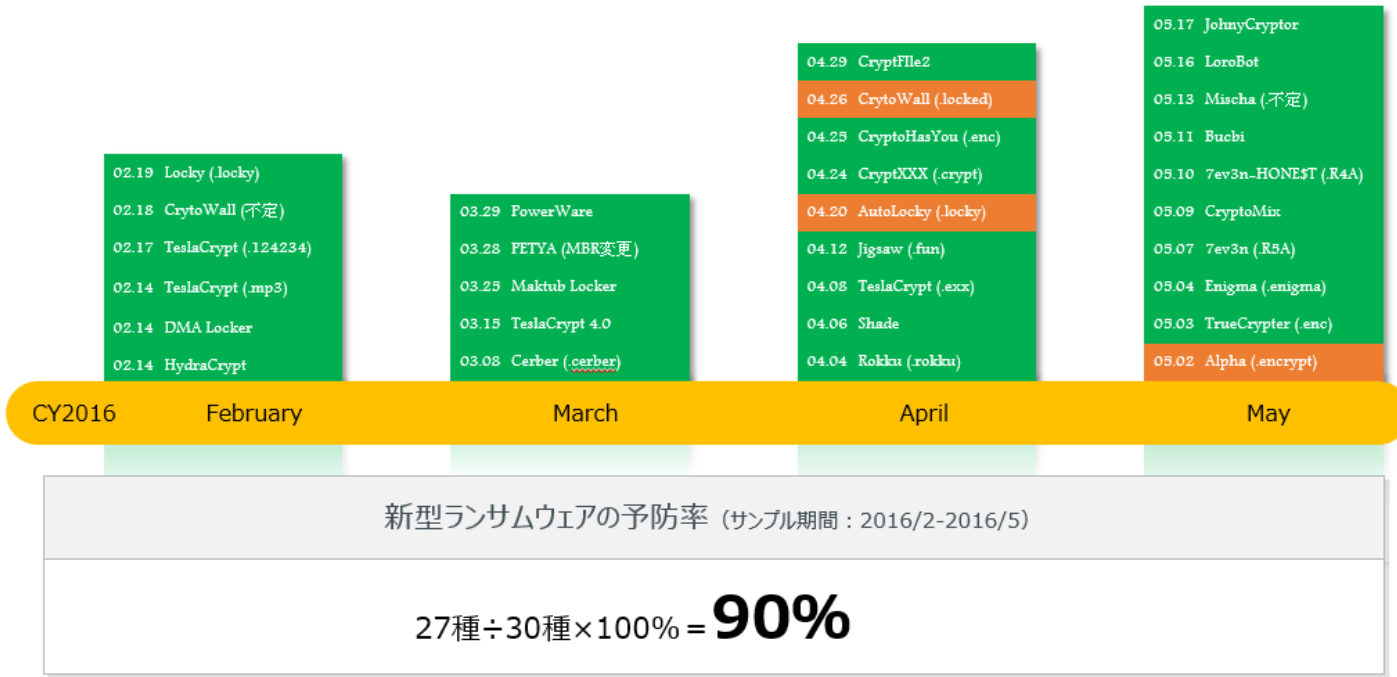


※状況認識技術の場合防御対象のファイルに注目しているため、未知のウイルスでも検出できる。

Why AppCheck? | 新型ランサムウェア予防率

AppCheckは、3ヶ月間更新することなく、30種の新種ランサムウェアのうち27個の防御に成功し90%の予防率を示しました。

一方、シグネチャ方式の場合、3か月間に更新0回ということはありません。通常、3か月あれば数百回以上の様々な更新を行っています。そして、この期間における**シグネチャ方式の防衛成功は0%**でした。(当社調べ)



Why AppCheck? | 動作が軽いわけは？

Q. AppCheckはなぜPCへの負荷が軽いのか？



A. ウイルス定義データベースを持たないからです。

※巨大になったウイルス定義データベースの問題点

1. ウイルスが増えるほどどんどんデータベースが大きくなる。
2. 照合に時間がかかる。
3. メモリ空間を圧迫する。
4. データベースのダウンロードや更新に時間がかかる。

これらの理由により、PCやネットワークへの負荷が高まります。

ウイルスデータベースを持たないAppCheckは、これらの技術を使った製品と比べてPCへの負荷が小さく、動作が軽くなっています。