

ランサムウェア対策



AppCheck

ある日突然PCをロックされたら
元に戻すために身代金を払いますか？



AppCheckとは？

パターンファイル不要。状況認識技術で新型ランサムウェアも検出できる！
ファイルのリアルタイムバックアップ・復元機能搭載で万一の場合にも安心。

シグネチャレス

シグネチャレスのため、AppCheckインストール後も、PCやサーバに負担をかけません。

また、シグネチャの更新もないため、定期的な更新作業も不要です。

リアルタイム バックアップ

ランサムウェアが侵入し不正なプロセスが実行された際、

リアルタイムで対象データをバックアップします。

ランサムウェアを削除したあと、従来のファイルを元に戻します。

ランサムウェア専用

ランサムウェア専用ソフトウェアのため、アンチウイルスソフトと

共存可能です。アンチウイルスソフトと一緒に利用することでPCおよびサーバのセキュリティを向上させることが可能です。

AppCheckの検査方式



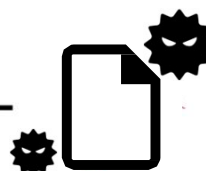
1. ファイルモニタリング

ユーザーのファイルをモニタリングして、変更時点で「正規変更」か「悪意のある変更」かを判断します



2. リアルタイムバックアップ

原本ファイルをリアルタイムにバックアップ。
ファイルを変更するプロセスについて継続モニタリング。



3. ファイル毀損プロセスの検知

断続的なファイル毀損が検出されると、そのプロセスをランサムウェアとみなして検知します。



4. プロセス遮断、削除および復旧

ランサムウェアとして検知されたプロセスを終了後、
毀損されたファイルを全て復旧します。



5. ユーザー業務の継続

別途処理なしに既存業務を継続することができます。

AppCheckはここが違う！

CARBエンジン搭載！状況認識技術で未知のランサムウェアもブロック！

CARBエンジンは、ファイルの変更状況を監視しながら複数要素からなる状況を基にユーザーによる正常な変更か、ランサムウェアによる改ざんかをリアルタイムに判断して、ランサムウェアによるファイル毀損行為をブロックします。従来のウイルス対策ソフトのようにウイルスパターンファイルを使用しないため動作が軽く、また、他社のウイルス対策ソフトとの併用が可能です。

防御

状況認識技術(特許)によりランサムウェアの毀損行為を遮断します。



ランサムウェア



脆弱性攻撃の防御



リアルタイムバックアップと復元機能

ファイル毀損時に、リアルタイムで元のファイルのバックアップを実施。



退避フォルダ



指定ファイルの自動バックアップ

指定ファイルを定期的に任意フォルダやローカルフォルダにバックアップ。



指定ファイル



状況認識技術搭載！

AppCheckはランサムウェアの特徴を調べるのではなく、状況認識技術によりファイルの変化をリアルタイムで検出し、ランサムウェアによるファイル毀損をブロックします。



指定ファイルの自動バックアップ

AppCheckは、指定したファイルを定期的にバックアップして正常なファイルを保護します。バックアップ先はネットワークフォルダにも対応しています。



リアルタイムバックアップ・復元！

AppCheckは、ファイルをリアルタイムでバックアップして正常なファイルを保護します。

(バックアップファイルは一時バックアップ後に自動的に削除されます。) また、ファイルの変更や削除などの毀損行為を記録しているので、その行為をたどることでファイルを復元することができます。



エクスプロイトガード機能

Webブラウザなど、各アプリケーションへの脆弱性攻撃を検知・遮断します。



動作が軽く、他社ウイルス対策ソフトとの共存が可能

AppCheckはパターンファイルをもたないため頻繁に発生するファイル更新が必要なく、また動作も軽いため通常業務に影響を与えません。他社ウイルス対策ソフトとの共存が可能ですので、今の環境を変えることなく追加してお使いいただけます。



中央管理(CMS) ※オプション

機能	説明
一括ポリシー設定	保護するためのポリシーを一斉に配布できるため効率的な管理、運用が可能。
アラームメール送信	AppCheck側でランサムウェア攻撃が検知された場合は、設定されたメールアドレス宛(複数設定可能)にアラームメール送信が可能。
モニタリング	ダッシュボード、ログ管理、リアルタイムでのランサムウェア検知情報の確認が可能。
レポート	期間別報告書、統計およびログデータを提供し簡単にレポートの出力が可能。

状況認識技術

AppCheckの状況認識技術！

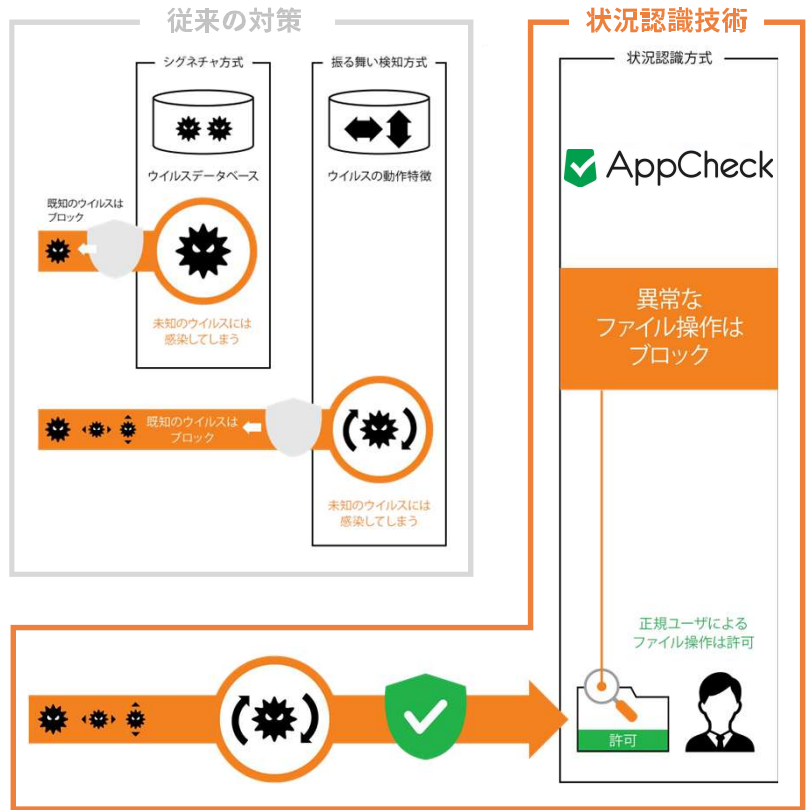
状況認識技術は、周辺の状況や環境等のすべての情報を総合して認知し、その状況に最適な対応を行う技術です。ランサムウェアが変更・毀損するターゲットであるファイル自体に注目しています。

従来のランサムウェア対策

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。

未知のウイルスには感染

ウイルスデータベースにある既存のウイルスをブロックすることしか出来ず、新しく現れるウイルスに対応することが出来ませんでした。



状況認識技術

ランサムウェア自体を見るのではなく、ファイル変更時に正常な変更か悪意のある変更かを判断。

AppCheckはファイル暗号化ランサムウェアの新種・亜種にも対応！

動作環境

AppCheck Pro	Windows7 SP1 以降 (32bit/64bit)
AppCheck Pro for Windows Server	Windows Server 2008 R2 SP1 以降
CPU	Intel 1.6GHz 以上
メモリ	1GB以上
HDD	2GB以上の空き容量
ブラウザ	<ul style="list-style-type: none"> Microsoft Edge Google Chrome Mozilla Firefox

*SHA-2認証書のMicrosoft最新パッチがインストールされていること

*ARMプロセッサは未対応となります

中央管理(CMS)提供形態

区分	クラウド
Webベース管理コンソール	○
サーバ、ストレージの用意	不要



株式会社JSecurity

東京都港区浜松町2-4-1 世界貿易センタービルディング南館17階

TEL:03-4567-2823/FAX:03-4567-2824

E-mail:sales@jsecurity.co.jp

URL:https://www.jsecurity.co.jp