2025 年 01 月 14 日

お客様各位

はじめにお読みください

AppCheck を正しく安全にお使いいただくために、以下の事項及びマニュアルを必ずお読みください。

本文書の最新版は https://www2.santec.com/app/support/download/に掲載させていただいております。

1.拡張子の登録について、AppCheck の設定でファイル拡張子を監視対象としています。

登録されていないファイルの拡張子は監視しません。

代表的なファイル拡張子は初期値として登録していますが、お使いのソフトウェアにより登録されていないファイル

拡張子を監視対象とする場合は、追加設定が必要となります。

ご注意事項

・拡張子の ini ファイルは誤検知/過検知となるため、ファイル拡張子の登録は不要です。

・exe 等の拡張子は、ランサムウェアの対象となることが少ないため、監視対象からの除外としてください。

AppCheck Pro マニュアル：ランサムガード： AppCheck Pro 拡張機能 ： 保護するファイル拡張子(区分字,または;)

AppCheck Pro CMS Cloud マニュアル：ポリシー管理:ランサムガード ・保護するファイル拡張名 (区分子,または;)

をご参照ください。

2.誤検知/過検知について、AppCheck は、暗号化ソフトウェアや大量のファイルを書き換えするソフトウェア、

スクリプト等を誤検知/過検知をする場合があります。

予め該当のソフトウェア、スクリプト等を AppCheck の信頼済みプロセス、例外設定を行ってください。

”ログモード”での試験運用を弊社では推奨しています。

ご注意事項

・ログモードは CMS Cloud(管理コンソールサービス)のみ提供している機能です。

・ログモードの運用期間は、2 週間～1か月間を弊社では推奨しています。

・ログモードの動作は、リアルタイムバックアップは実施しますが、毀損されたファイル及び攻撃プロセスの検疫、

自動復元は行いません。

AppCheck Pro CMS Cloud マニュアル：ポリシー管理:ランサムガード ・ランサムウェア検知後の動作(ログのみ残す)をご参照ください。

3.SMB サーバ保護機能の誤検知/過検知について

ランサムウェアは、共有領域（共有フォルダ等）にあるファイルを攻撃する場合があります。

AppCheck には共有領域を保護する“SMB サーバ保護機能”があります。

この機能について、上記 2.と同様に誤検知/過検知する場合があり、

PC 端末で共有領域に大量に書き換えるプログラム/スクリプト等の他、ネットワークドライブ割り当てを行っている

場合は、予め対象端末の IP アドレスの固定化と AppCheck の SMB 設定で例外設定することを弊社では推奨しています。

ログモードでのモニター監視で、上記 2.同様に試験運用後、誤検知/過検知した場合、例外設定を行います。

ご注意事項

・例外設定を行った場合、該当端末も AppCheck を導入することを弊社では推奨しています。

・例外設定を行った場合の監視対象ファイルはログとして記録はしませんが、リアルタイムバックアップは行います。

AppCheck Pro マニュアル：SMB サーバ保護

AppCheck Pro CMS Cloud マニュアル：SMB 設定 をご参照ください。

記載されている内容は、記載されております内容やアドレスが変更されている場合がございます。

ご不明な点がございましたら、以下までお問合せいただけますようよろしくお願いいたします。

【お問合せ先】

santec Japan 株式会社 ソリューショングループ

お問合せフォーム：https://www2.santec.com/app/inquiry/

メールアドレス：solution@santec.com