

日立総合計装システム EX・CyberPlantシリーズ 制御システムウイルス対策のおすすめ

制御システムを安定稼働させるために ウイルス対策をおすすめします。



お客様のニーズにあわせた
ソリューションをご用意
しております。



お気軽にご相談を!

二重のウイルス対策を実施し、 お客様制御システムの安定稼働をサポートします。

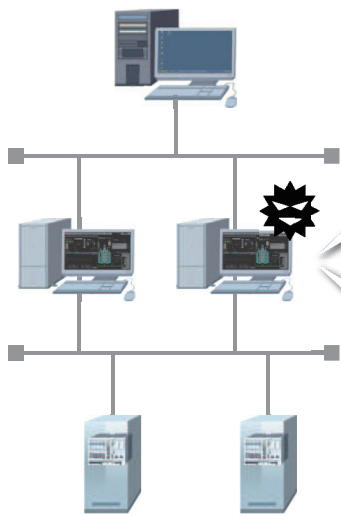
制御システムに対するウイルス攻撃を防御するため、監視操作端末へホワイトリスト方式*1、ブラックリスト方式*2のウイルス対策ソフトの導入をご提案します。

*1 あらかじめ作成した許可リストにあるプログラムのみ実行を許可する方式です。
*2 ウイルス定義パターンに合致するファイルを検索する方式です。

2種類のウイルス対策で守ります

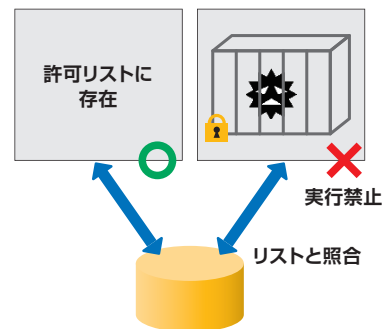
感染例

USBメモリからの侵入
外部ネットワークからの侵入



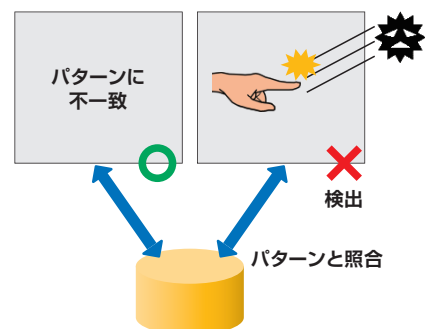
ホワイトリスト方式 (通常運用時)

許可リストにないプログラム
は実行できません。
感染しても不正プログラム
は実行できないため、脅威
を無効にします。



ブラックリスト方式 (定期点検時)

ウイルス定義パターンに合致
するファイルを検索します。
感染した不正プログラムを
駆除し脅威を無効にします。



ウイルス対策の特長

ホワイトリスト方式とブラックリスト方式のそれぞれの長所を活かして対策をします。

項目	ホワイトリスト方式	ブラックリスト方式
実施タイミング	通常運用時	定期点検時
メリット	システムへの負荷が少ない。 ウイルスは活動できない。	ウイルス発見時に駆除を行う。
リスク	ウイルスは内在する。	検査中はシステムの負荷が増加する。 ウイルス定義パターンに無いウイルスを検知できない。

※ホワイトリスト方式、ブラックリスト方式のそれぞれ個別での対応も致します。

対象システム

シリーズ	機種	OS
EX-N01	POC-N01/SOC-N01 POC-N01TS SOC-N01TC	Windows® 7 Windows Server® 2008 R2 Windows® Embedded standard 7
CyberBridge	サーバー クライアント	Windows® 7 Windows Server® 2008 R2
運転支援	サーバー クライアント	Windows® 7 Windows Server® 2008 R2
CyberPrinter	CyberPrinter	Windows® 7 Windows Server® 2008 R2
EX-8000	POC-8000/SOC-8000 POC-8000TS SOC-8000TC	Windows® XP Windows Server® 2003 R2 Windows® Embedded Standard 2009

※導入時には事前に調査が必要になります。

詳細は弊社サービスエンジニアまでお問い合わせください。

お問い合わせ

株式会社 日立ハイテクフィールドディング

計測制御部

〒105-6410

東京都港区虎ノ門一丁目17番1号 虎ノ門ヒルズ ビジネスタワー

<https://www.hitachi-hightech.com/hfd/>

お客様サポートセンター

0120-203-813



- 本資料に記載の内容は、改良のため予告なく変更することがあります。
- システム構成、ソフトウェアパッケージにより保守内容が異なります。
- システムのバージョンによっては実施できない保守メニューがあります。
- Windows および Windows Server は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

本カタログは2020年1月現在のものです。

KS1506008Rev.01