

セキュリティ対策ソフトウェア

MEIDEN

AhnLab

# WhiteShield for MEIDEN

ウイルスやワームの  
脅威から  
コントローラを  
守ります。



新しい時代を元気にします

*Empower for new days*

# ウイルスやワームの侵入防止やヒューマンエラーによる誤作動を防止します。

WhiteShieldは、強制アクセス制御によりWindowsのシステム管理者(Administrator)の権限を制限する高レベルの権限管理を提供し、ウイルスなどの脅威からコントローラを保護します。コントローラに搭載されたWhiteShieldは、フィルタドライバとしてアプリケーションとカーネルの間で動作し、

プロセス/ユーザがローカルシステムにアクセスするときに、OSの権限とは関係なくあらかじめ設定しておいた許可リスト(ホワイトリスト)を基にしてリソースのアクセス制御を行います。これによりウイルスやワームなどの侵入を防ぎ、ヒューマンエラーによる誤作動を防止できる製品です。

## WhiteShield for MEIDEN



### 特長

#### 製造現場への導入が容易

アンチウイルスソフトの導入が難しい製造現場のコントローラや産業用PCに組み込むことで、ウイルスや不正行為を防ぐことができます。

#### 現場の作業を止めることなく新種ウイルスも遮断

WhiteShieldを導入した環境では、ウイルスのパターンファイルやプログラムの更新が不要のため、生産を止める必要がなく、アンチウイルスソフトではパターン認識できない新種のウイルスも遮断可能です。

#### CPU負荷への影響なし

ウイルススキャンなどCPUに高負荷となる作業がないため、万全なセキュリティを保ちながらコントローラや産業用PCの安定した稼働を実現できます。

#### フォルダ保護機能付き

特定のフォルダに対してアクセス可能なアプリケーションを制限できるフォルダ保護機能のため、生産に関する機密データなども強固に保護します。

### 動作モードが変更可能

動作モード	機能
Enableモード	ホワイトリストが適用され、アクセス違反が発生した場合ログに保存し、違反動作を遮断します。
Disableモード	ホワイトリストが適用されず、アクセス違反が発生しても遮断せず、ログにも保存されません。WhiteShieldの機能をOFFし、通常のOSとして動作させるためのモードです。
Installモード	アプリケーションのインストール時に使用します。実行可能ファイルである場合は、自動的にホワイトリストに追加されます。
Testモード	ホワイトリストが適用され、アクセス違反が発生した場合ログに保存しますが、違反動作を遮断しません。設定したホワイトリストに問題がないかテストを行うためのモードです。

### WhiteShieldの適用範囲

- コントローラ、産業用PCのセキュリティ対策
- ウイルス/ワームの拡散防止
- 機密データの保護

### 構成

WhiteShieldは、セキュリティ機能を実現するエージェントとセキュリティポリシーの設定やエージェントの管理を行うマネージャから構成されます。

**● エージェント**  
保護対象となるコントローラにインストールされるWhiteShieldのメインプログラムです。ホワイトリストを基準にプロセス/ユーザのアクセス制御を行います。マネージャのリクエストに応じてレスポンス/処理を行う方式なので、エージェントがマネージャを呼び出すことはありません。

**● マネージャ**  
一台もしくは複数のエージェントを管理する管理プログラムです。エージェントを管理するためにエージェントに適用されるホワイトリストの作成/修正/配布機能などがあり、それぞれのエージェントのログを確認し、エージェントをグループ化して管理することができます。

	Ver.01.19以前	Ver.01.20以降 (Windows 7対応版)
<b>OS環境</b> (エージェント、マネージャ共通)	Windows Server 2003 SP2 Windows 2000 Professional SP4 Windows XP Embedded SP1/SP2/SP3 Windows XP Professional SP2/SP3 Windows Embedded Standard 2009	Windows Embedded Standard 7 32bit/64bit Windows 7 Ultimate 32bit/64bit
<b>ハードウェア環境</b> (最小仕様)	CPU: Intel Celeron M/600MHz以上 RAM: 256MB以上 HDD: 50MB以上 Network: 10BASE-T/100BASE-TX	CPU: Intel Celeron/1.86GHz以上 RAM: 2GB以上 HDD: 50MB以上 Network: 10BASE-T/100BASE-TX

※Ver.01.19以前とVer.01.20以降では、対応OS環境が異なります。

### 機能

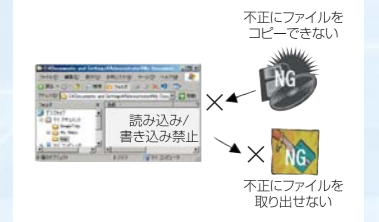
#### ホワイトリスト方式による起動プロセス制限

プロセス/ユーザなどがローカルシステムにアクセスする時、プロセス/ユーザのOSの権限と関係なく、すでに設定された許可リストを基にしてリソースへのアクセス制御を行います。この許可リストをホワイトリストと呼びます。WhiteShieldでは、ホワイトリストを採用することにより、アクセスを制御してウイルスやワームなどの侵入、ヒューマンエラーによる誤作動を防止します。



#### フォルダアクセス制御

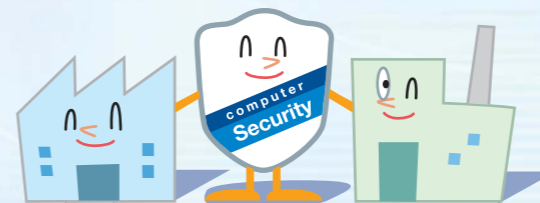
フォルダに対してアクセス可能なプロセスを設定することで、フォルダのアクセス制御を行うことが可能です。それにより、重要ファイルの保護、機密ファイルの漏えいを防ぐことが可能です。



- 書き込みが行えないため、ファイルをコピーすることができない。=ウイルスが侵入できない。
- 読み込みが行えないため、不正にファイルを取り出すことができない。=情報流出の防止

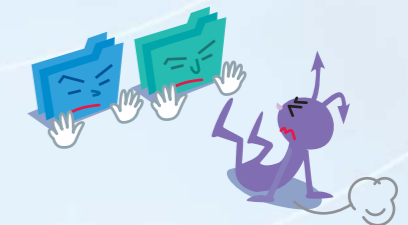
#### 低リソース

ハードウェアリソースの面で条件の厳しい産業用コントローラ向けに最適化を行い、低リソースでの稼働を実現しました。



#### 拡張子によるファイルアクセス制御

ハッキングに利用される恐れの高い拡張子を持つファイルに対し、あらかじめ利用可能なファイルを制御することにより、不正なファイルが入り込むことを防止します。



#### 監査ログ機能

設定されたホワイトリストに違反する行為が発生した場合は、違反情報が記録されます。



#### ポリシーの一斉配布

同一環境のコントローラに対して、同じホワイトリストを一斉に配布することができます。それによりセキュリティレベルを容易に統一することが可能となります。



※WhiteShieldは韓国AhnLab, Inc.の製品です。  
 ※AhnLab WhiteShieldは韓国AhnLab, Inc.の登録商標です。  
 ※Windowsは米国Microsoft Corp.の登録商標です。  
 ※Intel, Celeronは米国Intel Corp.の登録商標です。  
 その他文中の会社名、商品名は、各社の商標又は登録商標です。資料の内容はお断りなしに変更することもありますのでご了承ください。



株式会社 明電舎

本社 〒141-6029 東京都品川区大崎2-1-1 ThinkPark Tower

[www.meidensha.co.jp](http://www.meidensha.co.jp)

お問い合わせ先 コンポーネント事業部 電子機器営業部 TEL(03)6420-7610 FAX(03)5745-3058



**安全に関するご注意**

ご使用前に、「取扱説明書」又はそれに準ずる資料をよくお読みのうえ正しくお使いください。

■仕様は機能・性能向上などのため変更することがありますのでご了承ください。

この製品に関するお問い合わせは



**MB615-3089 D** 2013年11月現在  
2013-11ME (8.5L) 1.5L