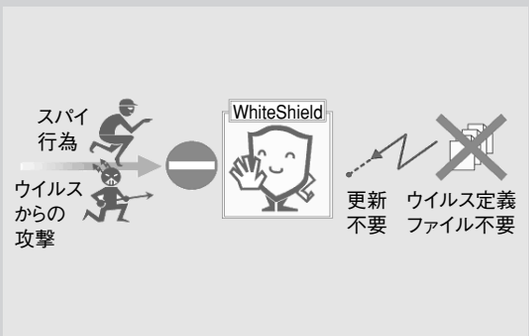
セキュリティ対策ソフトウェア　ホワイトシールド WhiteShield

セキュリティ，ホワイトリスト，ウイルス対策

＊坂上行男　Yukio Sakajo

概　　要

ホワイトシールド
WhiteShieldは，事前に許可リスト（ホワイトリスト）に登録されたプログラムしか動作できない“強制アクセス制御”により，不正プログラムの実行やデータの改ざんを防止するソフトウェアである。ウイルス定義ファイル（パターンファイル）の更新が不要なため，導入後のメンテナンスが不要なセキュリティ対策が実現できる。また，ウイルスチェックのためのコンピュータ内のファイルスキャンが不要なため，コンピュータのCPUへの負荷が低減できる。これにより製造現場で稼働している制御システムなど，CPU負荷が懸念される環境や，ウイルス定義ファイルの更新が困難な環境に適用することが可能となる。



WhiteShieldイメージ図

1. ま　え　が　き

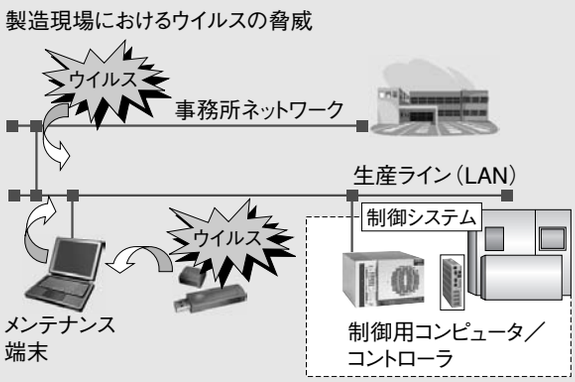
今では，ほとんどの企業で業務用コンピュータ（事務用パソコンやサーバ機）に，アンチウイルスソフトウェアなどのウイルス対策製品が実装されている。また家庭内で使用されている多くのパソコンにも，アンチウイルスソフトウェアが実装されており，一般にウイルス対策が必要であるという考えが浸透している。

これに対して製造現場などのシステムの制御用に使用されているコンピュータは，以下の理由によりアンチウイルスソフトウェアを容易に導入できない状況にある。

⑴ コンピュータがインターネットに接続されていないため，ウイルス定義ファイル（パターンファイル）の更新ができない。

⑵ ウイルスチェックによるコンピュータのCPU負荷がシステムへの悪影響を及ぼす可能性がある。

一方，**第 1 図**に示すように，製造現場においても以下の理由によりウイルスの感染，情報の流出



第 1 図　製造現場におけるウイルスの脅威
製造現場においても外部からの持ち込みパソコンやUSBメディアなどからウイルスに感染する危険がある。

＊製品開発企画室

の危険にさらされているため何らかの対策が必要である。

⑴ 外部からウイルスが侵入する可能性　　外部からウイルスが侵入した場合，工場内のネットワークを通じて制御用コンピュータに感染する。

⑵ 持ち込みメディアによる感染の可能性　　フロッピーディスクや，MO，USBメモリ，CD－ROMなどの持込データがウイルスに感染していた場合，持ち込んだメディアから感染する。

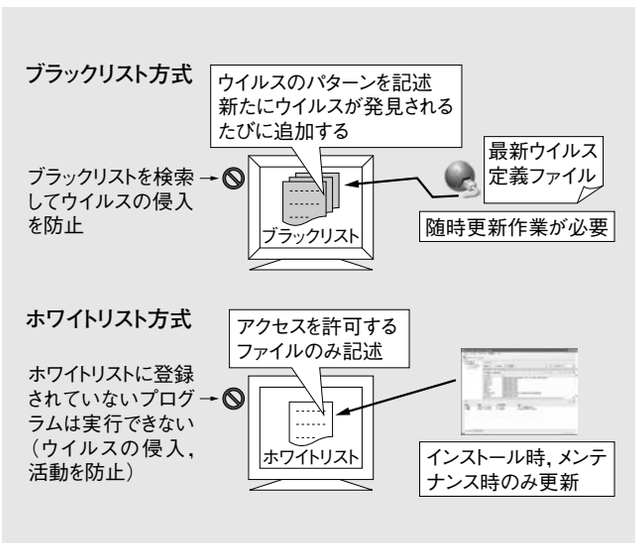
⑶ 持ち込んだコンピュータによる感染の可能性　　メンテナンスなどで持ち込んだノートパソコンなどがウイルスに感染していた場合，ネットワークを通じて感染する。

WhiteShield（ホワイトシールド）は，一般の事務用途ではなく製造現場などで使用されている制御用コンピュータへの導入を目的とし，既存のアンチウイルスソフトウェアの問題点を解決した製品である。

本稿では，WhiteShieldの概要について紹介する。

2.　WhiteShieldの特長

WhiteShieldは，制御用コンピュータのセキュリティ対策を目的とした製品である。そのためブラックリスト方式ではなく，ウイルス定義ファイルの更新が不要なホワイトリスト方式を採用し，強制アクセス制御を実現した。これによりコンピュータのCPUに負荷がかからない，且つウイルス定義ファイルの更新が不要な環境を実現している。**第 2 図**にブラックリスト方式とホワイトリスト方式を示す。



第 2 図　ブラックリスト方式とホワイトリスト方式
ブラックリスト方式は，ブラックリストを検索してウイルスの侵入を防止する。ホワイトリスト方式は，ホワイトリストに登録されていないプログラムは実行できない。

⑴ ブラックリスト方式　　既知のウイルスを解析してウイルスのパターンをブラックリストに登録する。対象ファイルとブラックリストと照合することにより，ウイルス感染の有無を確認する。新たなウイルスが発見される度にウイルスの解析とブラックリストの更新が必要になる。

⑵ ホワイトリスト方式　　動作を許可するプログラムをあらかじめホワイトリストに登録しておく。対象ファイルとホワイトリストを照合することにより，動作の許可／拒否を確認する。

⑶ 強制アクセス制御（MAC：Mandatory Access Control）　　プロセスやファイルへのアクセス権限をOSの管理とは別にWhiteShieldが強制的に管理する。

制御システムでは，動作するプログラムが決められているため，リストの更新が不要なホワイトリスト方式が有効である。また，ホワイトリスト方式を採用することにより不正プログラムの侵入を防止することができ，データの改ざん及び流出を防止することができる。

ホワイトリストの登録は，WhiteShieldをコンピュータにインストールする時に自動登録される。そのため，専門の知識が不要で容易に導入することができる。また管理を行うマネージャを使用することで，画面上の簡単な操作でホワイトリストの更新作業が行える。

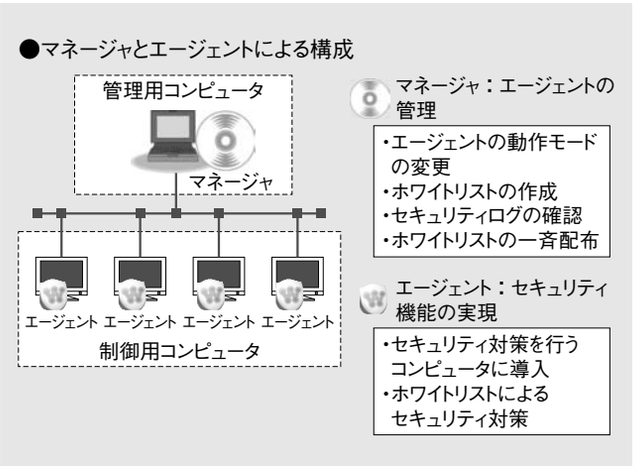
以下にWhiteShieldの特長を示す。

⑴ ウイルス情報（ウイルス定義ファイル）の更新が不要　　強制アクセス制御により最新のウイルス情報を取得する必要がない。

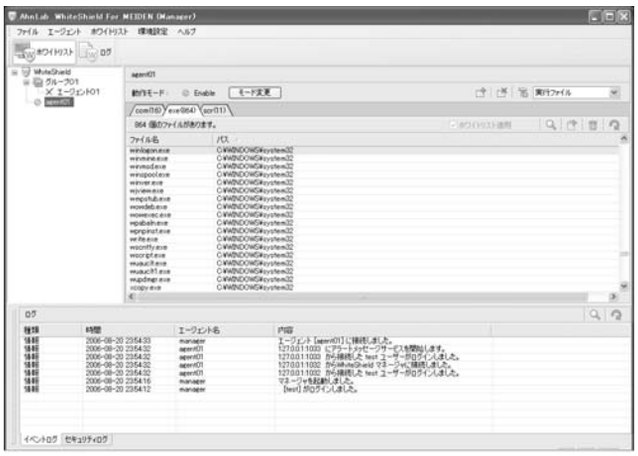
⑵ ファイルの作成／更新の時でもCPU負荷無しウイルス情報を検索する必要がないため，CPU負荷がかからない。

⑶ 未知のウイルスに対応可能　　ホワイトリストに登録されたプログラムしか動作できないため，未知のウイルスも活動できない。

⑷ ホワイトリストの自動登録　　ホワイトリストは，WhiteShieldインストール時に自動登録されるためインストール後，すぐにシステムの動作確認が行える。また，後からホワイトリストを編集する場合も専門の知識が不要なため，短時間で編集作業が行える。



第 3 図　WhiteShield構成図
ホワイトリスト方式によるアクセス制御を行うエージェントとエージェントの管理を行うマネージャで構成される。



第 4 図　マネージャ画面
ホワイトリストの追加・削除など，エージェントの管理を容易に行えるユーザインタフェースである。

3. 製 品 の 構 成

WhiteShieldは，ホワイトリストによるアクセス制御を実現する「エージェント」とエージェントの管理を行う「マネージャ」で構成される。**第 3 図**にWhiteShieldの構成図を示す。

マネージャは，エージェントの管理を行う時に使用するため，通常の運用時は必須ではない。コンピュータにエージェントのみ実装されていればセキュリティ対策が行える。なお，マネージャ1台で最大128台のエージェントを同時に管理することができる。

3.1　エージェント

エージェントは，定義されたホワイトリストに従って制御を行い，OSのファイルシステムが提供するアクセス権限より高いレベルで動作し，「強制アクセス制御」を実現する。

3.2　マネージャ

マネージャは，**第 4 図**に示すユーザインタフェースで容易にエージェントの管理を行うことができる。以下にマネージャの機能を示す。

⑴ エージェントのグループ管理　　複数のエージェントを管理するため，グループ別にエージェントを登録することが可能。

⑵ エージェントのホワイトリスト修正機能　　登録されたエージェントから特定のエージェントのホワイトリストを読み込み修正する機能。

⑶ エージェントのホワイトリストバックアップ／復元（一括配布）機能　　エージェントのホワイトリストをバックアップして，再びエージェントに復元する機能。ホワイトリストを同時に複数のエージェントに配布する一括配布機能も装備。

⑷ エージェントのログ確認機能　　1台もしくは複数のエージェントで発生したログをマネージャで確認及び保存することが可能。

4. 機　能　概　要

以下にWhiteShieldがサポートする機能を紹介する。

4.1　ホワイトリスト

プロセス／ユーザなどがシステムにアクセスする時，プロセス／ユーザのOS権限と関係なく，すでに設定されている許可リストを基にしてリソースへのアクセス制御を行う。この許可リストをホワイトリストと呼ぶ。ホワイトリストには以下の4種類がある。

⑴ 実行ファイルホワイトリスト　　実行ファイルホワイトリストは，レジストリとファイルに対してアクセス権限を持つ実行ファイルのリストを意味する。単独で起動できる拡張子がこのホワイトリストに登録される。エージェントのインストール時にローカルシステムのすべての実行ファイル（exe，com，scr）を読み込み，ホワイトリストを生成する。

⑵ 基本拡張子ホワイトリスト　　基本拡張子ホワイトリストは，悪用される恐れが高い拡張子のアクセス制御を行う機能。これらの拡張子は，bat，pif，cmd，cpl，ocx，vbs，jsがある。これらの対

第 1 表　動作モード
エージェントの動作モード一覧を示す。

動作モード	説明
Enable	セキュリティ機能有効 通常運用時のモード
Disable	セキュリティ機能無効 但し, WhiteShield自身のセルフプロテクト機能は有効
Install	アプリケーションのインストール時に使用 ホワイトリストの追加自動生成を行う
Test	アプリケーションの稼働試験に使用 セキュリティ機能は無効で違反ログのみ残す 違反ログを参考にホワイトリストの設定を調整する

象となるファイルはエージェントのインストール時に基本拡張子ホワイトリストに自動登録される。

⑶ ユーザ定義拡張子ホワイトリスト　　実行ファイルホワイトリスト，基本拡張子ホワイトリストに含まれない拡張子に対して，アクセス制御を追加するための機能。

⑷ フォルダホワイトリスト　　フォルダホワイトリストは，特定のフォルダを保護するため，許可された実行ファイルのみアクセスが可能となる機能。これによりデータの改ざん及び不正持ち出しを防止する。

4.2　動作モード

動作モードは，メンテナンスなどを考慮し，**第 1 表**にある4種類のモードを実装している。

4.3　オプション機能

ホワイトリストでは定義できない特殊な機能に対して，以下のオプション機能を実装している。

⑴ Internet ExplorerでのJava Scriptファイル実行許可　　HTMLに含まれているJava Scriptファイルの実行／遮断を指定する機能。Java Scriptは悪用されることがあるため，ユーザが制御できるようにする機能。

⑵ Internet ExplorerでのVB Scriptファイル実行許可　　HTMLに含まれているvbsファイルの実行／遮断を指定する機能。VB Scriptは悪用されることがあるため，ユーザが制御できるようにする機能。

⑶ プロセス強制終了許可　　実行中のプロセスに対して他のプロセスが強制終了することを「許可する／許可しない」を設定する機能。

⑷ システムアカウントのcmd.exeコマンド実行許可　　システムアカウント（System，Local Service，Network Service）でcmd.exeの実行の許可／拒否を指定する機能。ワームやハッカーによりシステムアカウントが奪われて，cmd.exeが実行されて悪用されることを防止する機能。

第 2 表　動作環境
マネージャ，エージェントの動作環境を示す。

エージェント	対応OS	Windows XP Embedded Service Pack1 Windows XP Embedded Service Pack2 Windows XP Professional Service Pack2 Windows XP Professional Service Pack3 Windows 2000 Professional Service Pack4 Windows Server 2003 Standard Service Pack2 Windows Server 2003 Enterprise Service Pack2
	CPU	Celeron M 600MHz以上
	メモリ	256MB以上（256MB時空き50～60MB想定）
	HDD	50MB以上（インストール可能な最小容量は5MB）
マネージャ	対応OS	Windows XP Embedded Service Pack1 Windows XP Embedded Service Pack2 Windows XP Professional Service Pack2 Windows XP Professional Service Pack3 Windows 2000 Professional Service Pack4 Windows Server 2003 Standard Service Pack2 Windows Server 2003 Enterprise Service Pack2
	CPU	Celeron M 600MHz以上
	メモリ	256MB以上（256MB時空き50～60MB想定）
	HDD	50MB以上

5.　動　作　環　境

第 2 表にエージェントとマネージャの動作環境を示す。エージェントとマネージャとも，対応OSはWindows XP EmbeddedとWindows XP Professionalである。

6.　む　　す　　び

当社のセキュリティ対策ソフトウェアWhiteShieldを紹介した。制御用コンピュータにWhiteShieldを実装することにより，システム性能に悪影響を及ぼすことなくセキュリティ対策が実現できる。今後もお客様の要望を取り入れ，機能追加及び対応OSの拡充を図り，よりよい製品を提供していく所存である。

《執筆者紹介》

坂上行男　Yukio Sakajo
開発・企画業務に従事