情報漏洩対策ソフトウェア

Port Security

ポートセキュリティ シリーズ Ⅳ

ご紹介資料

エムコマース株式会社

電子データを取巻く環境と脅威

M-Commerce

危険なソフトウェアの
無断インストール

ウィルス侵入による
データ破壊 / 漏洩

PC の紛失 / 盗難

USB デバイスや
CD-R 等による
重要データの持ち出し

持ち出した外部記憶媒体を
不注意で紛失 / 盗難

不注意

情報漏洩事故の約7割が内部要因だといわれています

不正アクセス

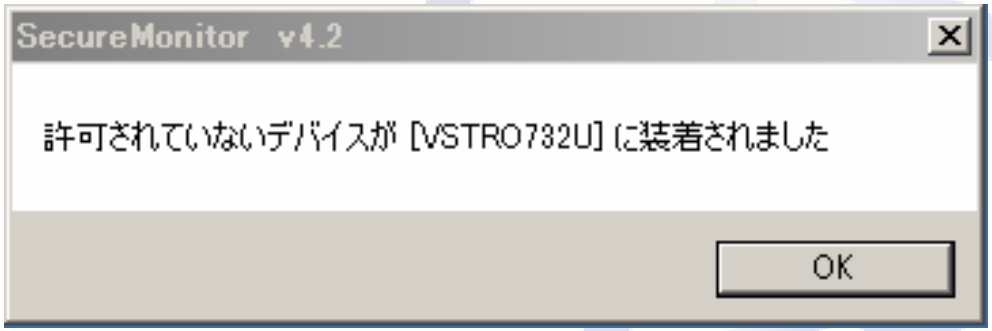
「ポートセキュリティシリーズⅣ」は

M-Commerce

ポートセキュリティ シリーズⅣは、使用（装着）が許可されていないUSBデバイスがPCに接続された際に瞬時にマシンロック等の保護動作を実行。

強制的に作業を中断させることで、不正なUSBデバイスや内蔵デバイス（CD-RW等）を使った重要データの流出を未然に防ぎます。

また、管理者が認知しない不要なソフトウェアのインストールや、USBワームによるウィルス侵入の脅威からPCを保護します。



ポートセキュリティ シリーズⅣは
不正なUSBデバイスや内蔵デバイスの使用を制御するソフトウェアです

ポートセキュリティシリーズIVが導入されている環境では

M-Commerce

USBデバイスや内蔵デバイスの
不正使用をシャットアウト

管理サーバー一切不要

PCへ直接インストールし
初期設定するだけですぐに制御開始

低コスト＆短時間で導入

■　不正なUSBデバイスや内蔵デバイスの使用をシャットアウト

USBデバイスの使用（装着）制御に加え、内蔵のCD、DVD、FD、Windowsポータルデバイスへの書込み禁止や使用禁止設定が可能です。

■　Windows8にいち早く対応！64ビット版にも対応し最新の環境で運用可

ネットワーク上にWindows XP、7、8のPCが混在している場合でも、全てのPCに運用が可能です。

■　msi形式のインストーラに対応

導入の規模やネットワークに応じて、インストール方法を選択できます。クライアントPCへ直接インストールや、ネットワーク配信ツールを利用してリモートインストールやサイレントインストールが可能です。

■　使用許可デバイスは機器を接続してワンクリックでホワイトリストに登録

USBデバイスは、機器個体で持っているデバイスインスタンス（ベンダーID、プロダクトIDおよびシリアル番号）が自動取得され、ワンクリックでホワイトリストに登録されます。また、ひとつのUSBポートに対して複数のUSB機器を登録できるため、柔軟な運用形態に対応します。デバイスインスタンス全てを識別するので、同一製品であっても個別にアクセス制御が可能です。

■　USBデバイスをクラスで分類、フィルタ設定

使用許可デバイスをクラス毎（ヒューマンインターフェースデバイスクラス、大容量ストレージクラス、プリンタクラスなど）に、チェック方式で簡単に設定できるオプション機能を持っています。

■　設定情報エクスポート・インポート機能

設定ファイル（ホワイトリストや保護動作設定など設定情報）のエクスポートとインポートが可能。この機能により、簡単に複数のPCに複製設定する事ができます。

■　運用環境に応じて保護動作を選択

イベント発生時の保護動作は、Windowsのログオフ、シャットダウン、再起動、電源オフ、マシンロック、無視の6つから選択できます。強制的に作業を中断させることで不正なUSBデバイスを使った重要データの流出を未然に防ぎます。

■　遠隔地にあるPCへの設定も可能

1台のPCで作成したホワイトリストとセキュリティ設定をActive Directoryのグループポリシーで複数の端末へ配信できます。また、お客様ごとの遠隔操作ツールを利用したリモートPCへの設定も可能です。運用管理負荷がさらに低減、TCO削減を実現します。

■　保護動作の発生履歴を記録、サーバPC上で集中管理可能

許可されていないUSBデバイスの不正使用により、PC上で保護動作が実行された際には、ワーニングメッセージを表示すると共に、発生日時、対象PC、保護動作種別、対象デバイス、デバイスインスタンスの情報をロギングし、保護動作の発生ログとして記録・管理することが可能です。
ログファイルの保存先にはクライアントPC又はネットワーク内の管理端末を指定でき、複数PCのログを集中・一元管理できます。
また、このログ一覧からホワイトリストの自動生成も可能です。

■　設定ユーティリティの使用制限（管理者機能）

ポートセキュリティの設定変更を特定の管理者のみ許可する事ができます。ローカルの管理者権限でPCを利用している環境で使用者による不正な設定変更を防ぐ事ができます。

■　使用許可デバイスの利用状況をリアルタイムで監視（資産管理）

情報セキュリティマネジメントに関する認証制度である「ISMS適合性評価制度(ISO27001：2005)」や「プライバシーマーク」などの導入・取得を行っている各企業では、内部におけるIT統制への対応が強く要望されるため、使用が認められているUSBデバイス等の使用履歴を取得し、所定の場所で正しく使用されているかモニタリングする事で、自社のIT資産の利用状況の正確な把握が可能です。

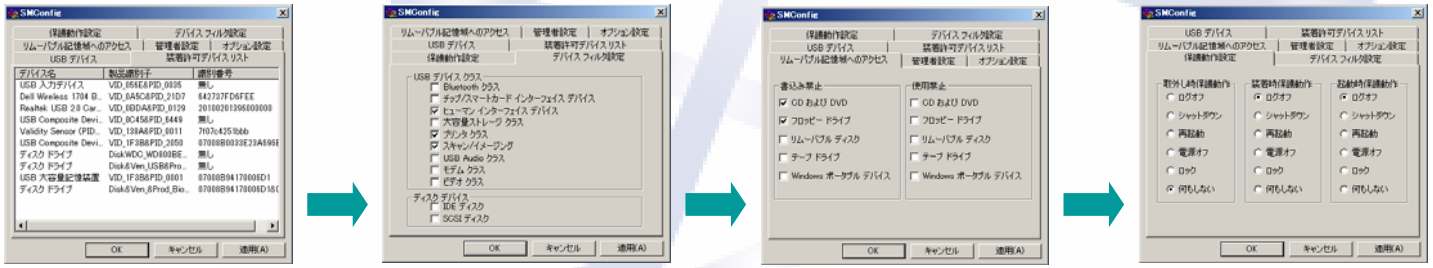
≪　クライアントPCへの導入イメージ　≫

【 Step 1 】対象のクライアントPCへソフトウェアインストール

【 Step 2 】使用許可USBデバイスをPCへ接続（キーボード、マウス等）

【 Step 3 】PC上でワンクリックで簡単設定

ホワイトリスト登録　デバイスフィルタ設定　内蔵デバイス制限設定　保護動作設定



【 セットアップ完了！】

≪　ＡＤサーバのグループポリシー配信機能を使った導入イメージ　≫

まずはマスターＰＣで設定ファイルを作成

＊マスターPCでの作業＊

【Step 1】マスターPCへソフトウェアインストール

【Step 2】使用許可USBデバイスをPCへ接続（キーボード、マウス等）

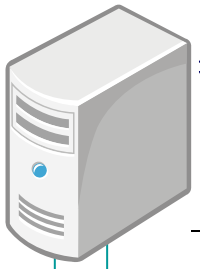
【Step 3】使用（装着）許可デバイスのホワイトリストを作成

例:　社内認定のUSBメモリ50台を
ホワイトリスト登録

【Step 4】設定ファイルをエクスポート

ポートセキュリティシリーズⅣ　導入イメージ②

M-Commerce

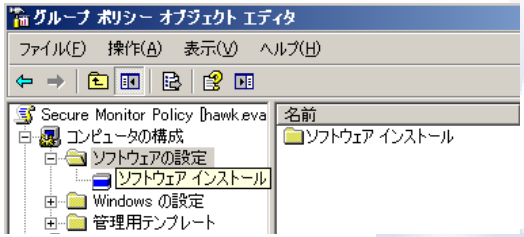


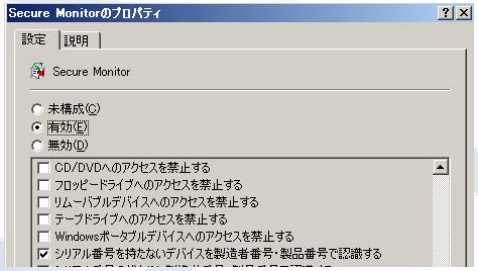
アプリケーション&設定ファイルを配信

＊ＡＤサーバでの作業＊

【Step 5】ADサーバへ、インストールパッケージ（msiインストーラ）と
Step 4でエクスポートした設定ファイルをコピー

【Step 6】グループごとのセキュリティポリシーの設定





【Step 7】対象のクライアントPC へ msiインストーラのリモートインストール

【Step 8】セキュリティポリシーの配信

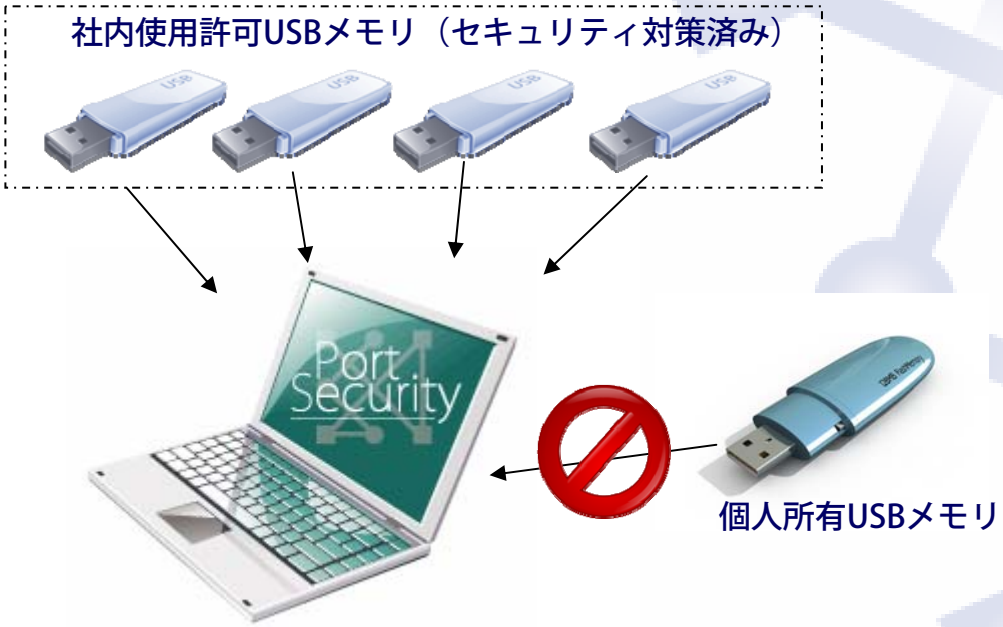
【Step 9】サービスの開始

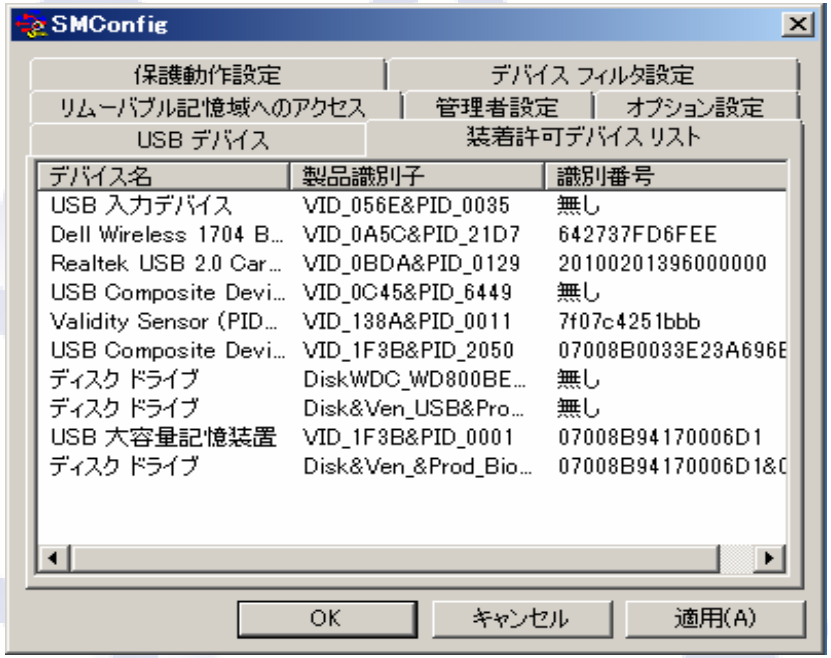
【セットアップ完了！】

使用許可デバイスのホワイトリスト登録

使用許可するUSBデバイスをPCへ装着し「適用」することでホワイトリストに登録されます。
デバイスインスタンス（ベンダーID、プロダクトID、シリアル番号）による固体識別が可能で、運用方針に適した制限設定を実現します。

例） 現存する社内USBメモリ50個はOK、個人所有メモリはNG





全ての固体識別情報を判別するので、同じ製品でもそれぞれに異なった制御設定が可能です。

ポートセキュリティシリーズIV導入　基本機能②

M-Commerce

USBデバイスをクラスで分類、フィルタ設定

USBデバイスクラス毎にフィルタリング設定が可能

例） ヒューマンインターフェースデバイス（キーボード、マウス等）は監視対象デバイスから除外する場合、ヒューマンインタフェースデバイスにチェックをするだけで設定完了。

○ ヒューマンインターフェイスデバイスは使用可


× その他のデバイスは使用不可

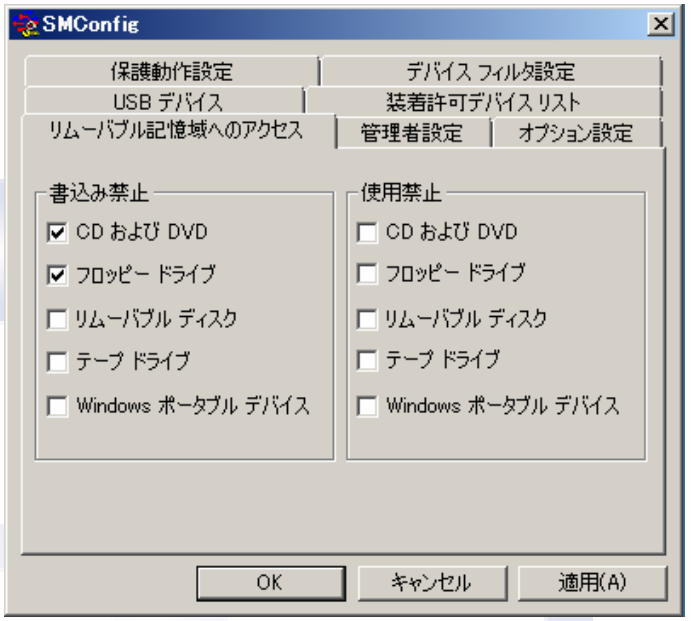


運用環境に応じて保護動作を選択

保護動作は、Windowsのログオフ/
シャットダウン/電源オフ/マシンロック
など6種類から選択

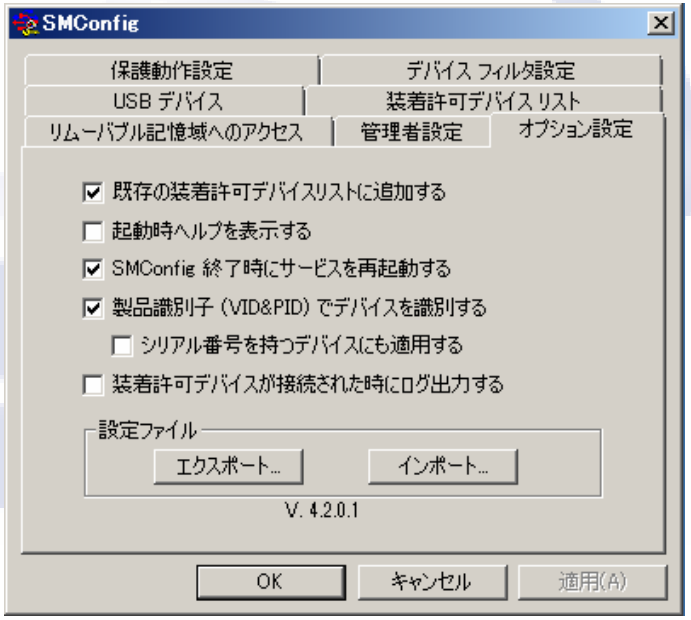
PC内蔵デバイスの使用制限

内蔵CD、DVD、FD、リムーバブルディスクやポータブルデバイスへの書込み禁止・使用禁止設定が可能。



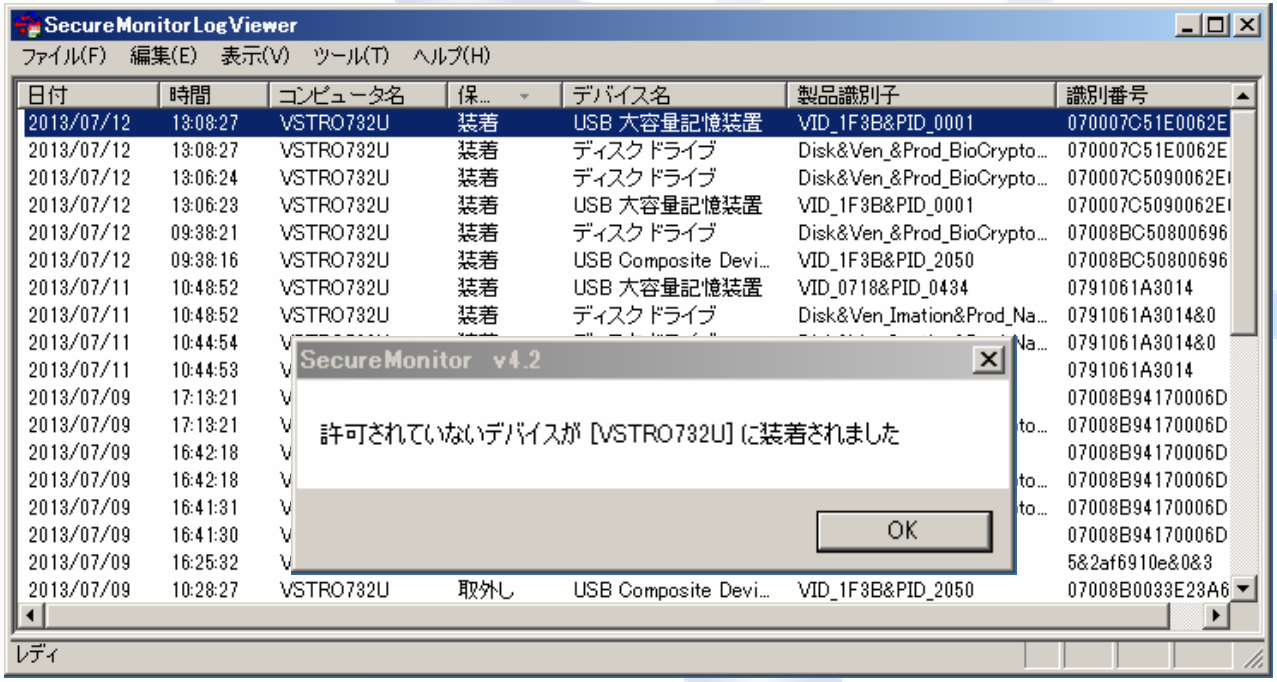
設定情報エクスポート・インポート機能

設定情報（ホワイトリストや保護動作設定など）のエクスポートとインポートが可能。
この機能により、簡単に複数のPCに設定できます。



保護動作発生履歴を記録、サーバPC上で集中管理を実現

許可されていないUSBデバイスが不正使用された際には、警告メッセージを表示すると共に、発生日時、対象コンピュータ名、デバイス名などの情報をログファイルに記録します。ログはそれぞれにPCに記録する設定と管理PCに集中管理する設定が選択できます。
このログからホワイトリストの自動生成も可能です。



管理PCは、クライアントPC（Windows XP等）で併用可能、サーバOSやSQLは必要ありません。

ポートセキュリティシリーズⅣ　配信機能

M-Commerce

msi形式のインストーラに対応

導入の規模やネットワーク構成に応じてインストール方法を選択できます。
「PCへ直接インストール」や「ネットワーク配信ツールを利用して、リモートインストール（サイレントインストール）」が可能です。

ADサーバグループポリシーで配信可能

1台のPCで作成したセキュリティポリシー設定を
Active Directoryのグループポリシーで複数の端末へ
配信可能です。

※配信機能を利用する場合、 Active Directory環境または、ネットワーク配信ツールが必要です。

ポートセキュリティシリーズⅣ　機能一覧①

M-Commerce

導入	サーバ構築	不要 クライアントOSで稼動
	SQLサーバ構築	一切不要
デバイス制御 （PC内蔵デバイス）	フロッピー	○ 対応
	CD/DVD	○ 対応
	MO	○ 対応
	テープ	○ 対応
	リムーバブルディスク	○ 対応
	Windowsポータブルデバイス	○ 対応
デバイス制御 （USBデバイス）	フロッピー	○ 対応
	CD/DVD	○ 対応
	MO	○ 対応
	HDD	○ 対応
	フラッシュメモリ	○ 対応
	PCカード	○ 対応
	テープ	○ 対応
	Buletooth	○ 対応
	プリンタ	○ 対応
	スキャナ	○ 対応
	Windowsポータブルデバイス	○ 対応
	ヒューマンインタフェースデバイス	○ 対応

ポートセキュリティシリーズⅣ　機能一覧②

M-Commerce

デバイス制御 （USBデバイス）	USB　Audio	○　対応
	モデム	○　対応
	ビデオ	○　対応
	その他（USBインタフェースに準拠する機器）	○　対応
デバイス制御 （ディスクデバイス）	IDEディスク	○　対応
	SCSIディスク	○　対応
その他	装着許可デバイス ホワイトリスト登録	○
	デバイスクラス設定（フィルタリング機能）	○
	USBデバイス取外し制限	○
	不正操作時保護動作（ロック/シャットダウンなど）	○
	監査ログ	○
	装着許可デバイス使用時ログ	○
	警告メッセージ表示	○
	装着許可デバイスリストエディタ機能	○
	USBデバイス　フィルタリング機能	○
	設定情報エクスポート・インポート機能	○
	装着許可デバイスリストインポート機能	○
	管理者機能（設定変更制限）	○
	Active Directory連携	○

製品名称　　情報漏洩対策ソフトウェア「ポートセキュリティシリーズIV」
製品型番　　SLUSB-LK-4　(JANコード: 4582420182000)
動作環境　　Windows 8 / 7 / Vista / XP

■　無償30日間評価用ダウンロード
「ポートセキュリティ　シリーズIV」ダウンロードページ
http://www.m-commercekk.jp/usbps/ps4trial404.html

＊関連製品＊
製品名称　　「ポートセキュリティシリーズIV　年間サポート」
製品型番　　SLUSB-LE-U　(JANコード: 4582420182017)

製品名称　　「ポートセキュリティシリーズIV　インストールCD-ROM」
製品型番　　SLUSB-CD-4　(JANコード: 4582420182024)