Universal Shield 技術ノート

Rev. 1.0 更新 2007 年 11 月 15 日

株式会社ネクステッジテクノロジー

http://www.nextEDGEtech.com

はじめに

本ドキュメントは、データ保護ソフトウェア Universal Shield をより適切な環境で効果的にご利用して頂くために必要な技術情報、利用用途例について高度な技術者を対象に解説しています。製品に関する基本的な機能や操作方法に関しては、製品カタログやユーザガイドを参照してください。

目次

nextEDGE TECHNOLOGY

製品概要

「Universal Shield」は、ファイルやプログラムなどを OS 上から完全に隠す「非可視化」を中心とした独自のアクセス制御と暗号化機能により、重要なデータを確実に保護する「データ非可視化＆暗号化」ソフトウェアです。

保護対象としたデータは、システムレベルで隠され完全に見えなくなるため、通常のユーザはもちろん、Windows の管理者権限を持つユーザやローレベルで活動する悪意あるプログラムであっても、保護対象へアクセスすることはできません。

保護対象へのアクセス許可は、ユーザ/グループの ALC 設定、およびアプリケーションファイアウォール(プログラム ホワイトリストの設定、)による制御できます。これにより保護対象へのアクセスも必要なマルウェア対策ソフト、バックアップソフトなどとの併用も可能です。

著作権

商標

nextEDGE TECHNOLOGY

保護対象と保護の指定方法

Universal Shield は、インストールされた環境下の全ローカルデバイス（ネットワークドライブ、UNCPATH などには対象外）を保護対象とすることができます。
保護対象への指定は、プログラムが持つリストへの PATH 登録により行ないます。
登録できる種類は次のとおり。

ドライブ:

保護対象をドライブ単位で指定できます。OS の仕様上、非可視化したドライブも、マイコンピュータにはリストされますが、これ以下の PATH にアクセスすることはできません。

フォルダ:

保護対象をフォルダ単位で指定できます。対象は、指定したフォルダを含めたフォルダ内に存在する全サブフォルダとファイル。

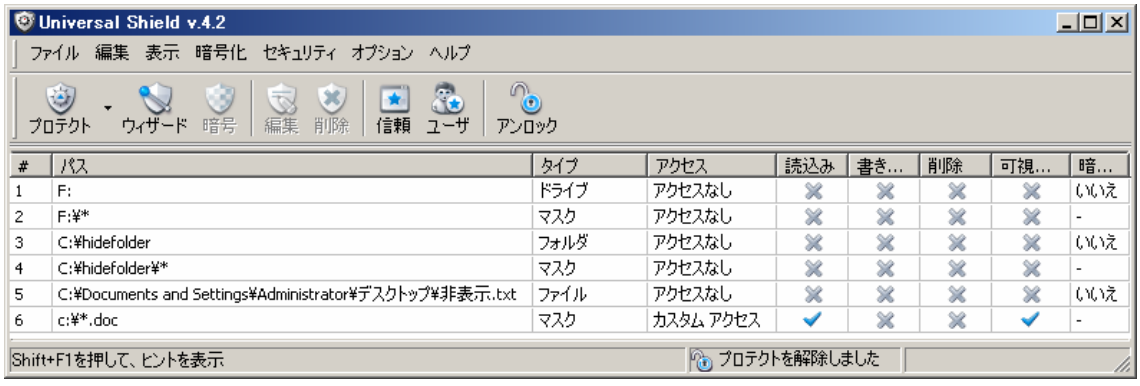
ファイル:

保護対象をファイル単位で指定できます。一番オーソドックスな指定方法。

マスク:

ワイルドカード[*]、[?] を用い対象ファイル、フォルダを指定できます。ファイルの種類（拡張子）単位での保護指定や、特定文字、特定書式での保護指定に適しています。

例： c:¥*.txt , c:¥*重要*.doc, c:¥重要?.xls



保護対象指定時の注意点

- 保護指定は PATH で行なわれている為、デバイスに割り当てられるレターが変更された場合、保護設定が無効化されてしまう危険があります。
- OS の仕様上、Autorun の実行アクセスを Universal Shield で抑制することはできません。必要に応じ、グループポリシーなどでこの実行を無効化してください。

nextEDGE TECHNOLOGY

・ 不用意に、システムファイルやシステムフォルダを非可視化しないでください。それらファイル、フォルダが非可視化すると、ご使用のコンピュータが不安定になり、データの損傷や喪失を引き起こす可能性があります。(¥¥windows や¥¥WinNT 内のサブフォルダやファイルに限ったことではありません。)

アクセス権限の優先順序

Universal Shield のアクセス権は NTFS の上位に位置するもので、仮に共有フォルダ内のファイルに保護設定を行った場合、ネットワーク経由でアクセスするユーザは、共有設定→NTFS→Universal Shield の順でアクセス権が適用されます。
また、Universal Shield には、リスト上に登録された各保護対象単位でのアクセス権指定他に、Windows(ドメインを含む)のユーザ/グループを用いた権限の設定、さらにプロセス単位による保護機能からの無効化設定が用意されており、これら機能によりユーザ毎に異なるセキュリティレベルの提供や、バックアップソフト、ウィルス対策ソフト等の併用性などを確保しています。

アクセス権＝「保護対象リストの許可」＋「ユーザ/グループ単位での許可」

(”拒否”は非動作)」

なお、保護リストは、様々な単位で登録が行える関係上、リスト上の保護設定の重複が発生するケースもありますが、その場合、許可側のアクセス権が優先されます。

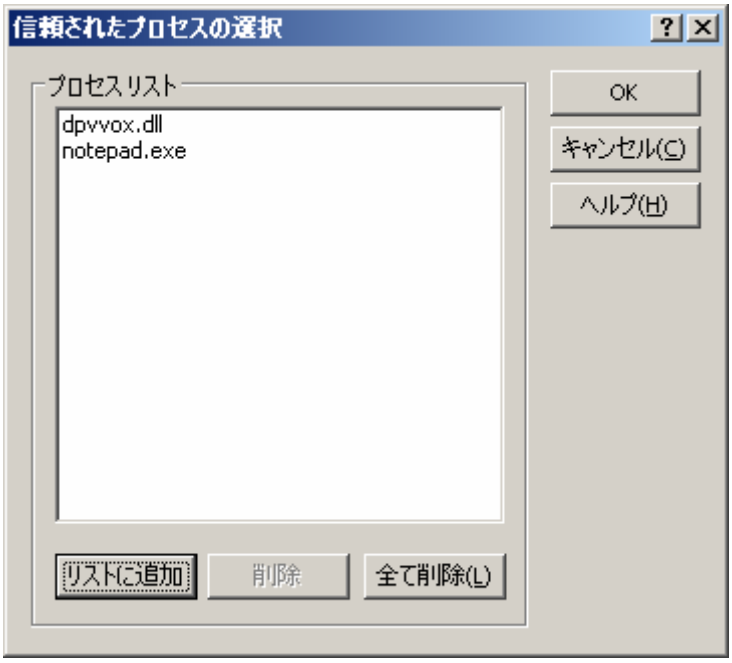
例:リストに以下の順序で保護リストに登録されていた場合、C ドライブ上のテキスト.txt 以外の txt が非可視化されます。

パス	タイプ	アクセス
C:¥*.txt	マスク	アクセスなし
C:¥テキスト.txt	ファイル	フルアクセス

nextEDGE TECHNOLOGY

信頼されたプロセスの設定

信頼されたプロセスに登録されたアプリケーションは、Universal Shield の設定を問わず、保護対象に対し通常のアクセスが行なえるようになります。なお、画面上では EXE のみの登録、且つファイル名のみが表示されますが、直接指定（若しくは参照画面で*.*と入力）することで、EXE 以外の登録も可能となっており、また動作についてもフル PATH で設計されています。

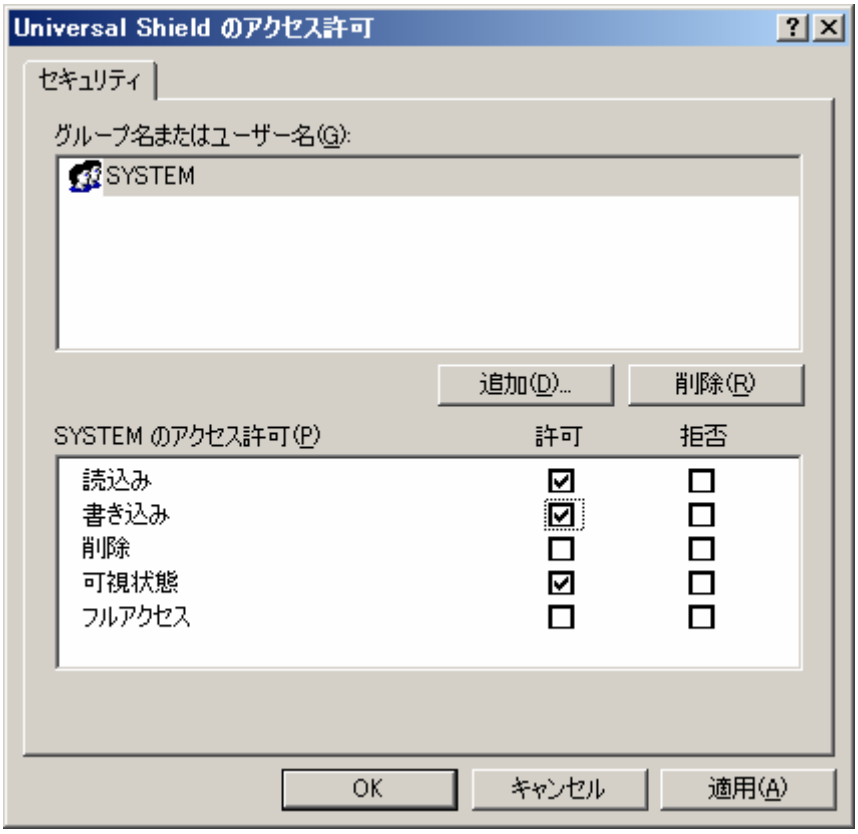


秘文などディスク暗号化ソフトとの併用

「秘文」のようなディスク暗号化システムと併用することでさらにセキュリティレベルを向上することができます。通常これらの暗号化システムでは、ユーザのログインと共に、ディスク上の暗号化されているデータはすべて自動的に複合化されアクセスが可能になります。Universal Shield を併用することで、この環境下においても、重要なデータへのアクセスを保護することが可能です。

Universal Shield をデフォルト設定のまま「秘文」と共に稼動すると、暗号化/複合化が正しくおこなわれなくなります。問題を回避するために、メインメニューの［セキュリティ］→[ユーザ］から SYSTEM アカウントへの[書き込み許可]を追加してください。（設定変更後、システムの再起動が必要です。）

nextEDGE TECHNOLOGY

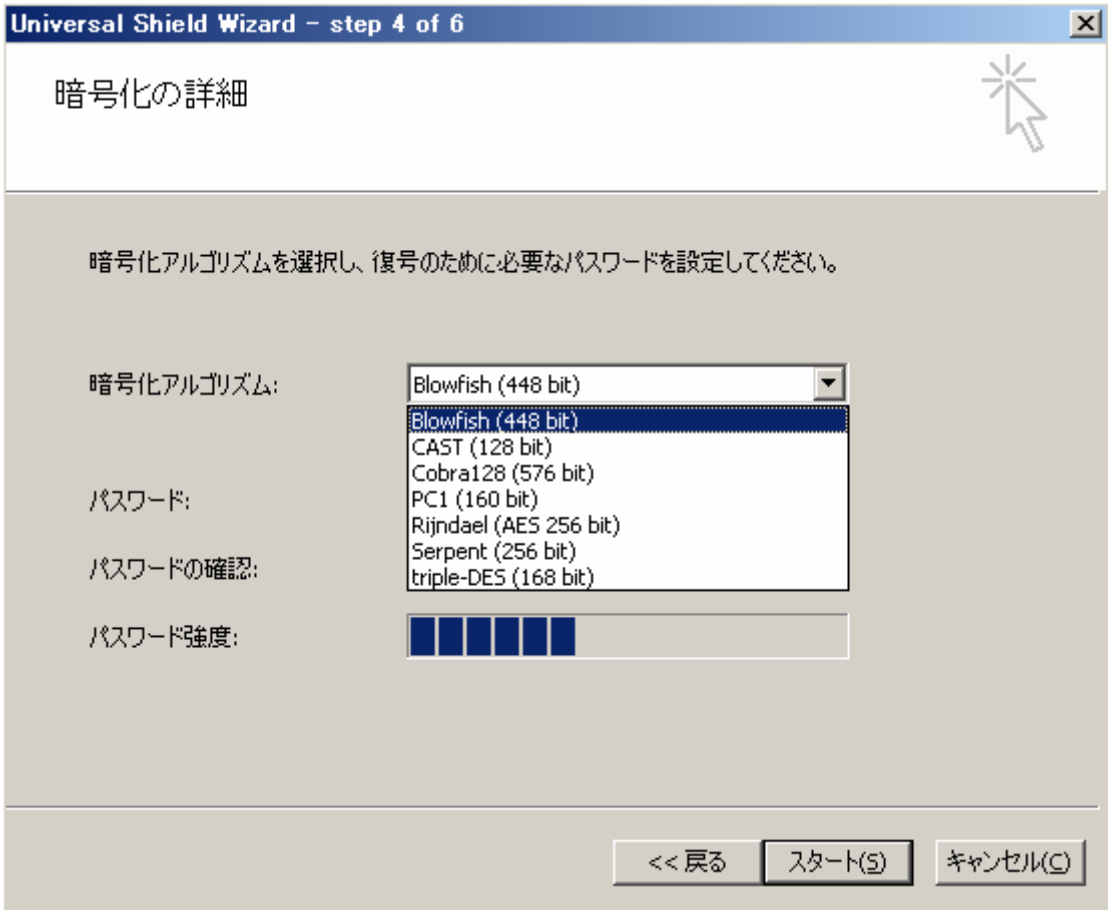


暗号化機能

Universal Shield は、保護対象への暗号化機能も用意しており、これを外付けハードディスク上のファイルに適用することで、他環境に接続した際の情報漏えいを防ぎます。
ただし、復号化に際しUniversal Shieldでの作業が必要となる関係上、ステルス モードで運用している場合や、Universal Shield がインストールされていない環境でも利用するファイルに対しては、暗号化機能は利用できませんので、必要に応じ「秘文」や「PrivateDisk」などと併用し、外へ持ち出すファイルの暗号化を行なってください。

補足: これらの暗号化アルゴリズムは、一般的な暗号化アルゴリズムであるため、復号化は Universal Shield に限らず同じ復号化アルゴリズムを持ったツールを利用して復号化が可能です。

nextEDGE TECHNOLOGY



仮想暗号化ソフト「PrivateDisk」との併用

仮想暗号化ソフト「PrivateDisk」により、外付けデバイス内に仮想暗号化ディスクと呼ばれる暗号化領域（ファイル）を作成し、その領域内にファイルを保存することで、他環境でもファイルを保護します。

仮想暗号化ディスクを利用するためのソフトウェアを外付けハードディスクにインストールできる為、利用環境を選びません。

また、PrivateDisk には、「アプリケーションファイアウォール」と呼ばれる、プロセス単位でのアクセス制御機能が用意されており、これを用いることで不正アクセスやウィルス混入を防ぐことも可能です。

Private Diskに関する情報は、シェアエッジ http://www.shareEDGE.comを参照してください。

nextEDGE TECHNOLOGY

運用例

以下では、Universal Shield の運用例について、より具体的に紹介しています。

Web コンテンツの不正アクセスによる改ざんからの保護

＜目的＞
インターネットに接続した Web サーバは常に危険にさらされています。悪意のある外部や内部ユーザにより Web サーバ内のコンテンツが改ざんされてしまうと、企業によっては大きなダメージとなります。
こうした重要なサーバやコンテンツをルートキットなどのマルウェアや内部からの不正な改竄から守るために Universal Shield は役立ちます。

〈設定方法〉
Universal Shield を Web サーバにインスールします。保護したい Web コンテンツを含んだフォルダを保護リストに追加します。Web サービス（IIS や Apache)プログラムを信頼されたプロセスリストに追加します。

Universal Shield を起動後、保護をオンにした状態では、Web サービス以外の一切のユーザやプログラムからのコンテンツへのアクセスがブロックされます。

メンテナンス時にのみ保護をオフにしてコンテンツの変更を行います。

「ステルスモード」の利用例

＜目的＞
JSOX 法、人材の流動化などセキュリティニーズの複雑化に対し、その対策が追いつかず、利便性の低下、トラブル発生など、組織レベルでのセキュリティ運用が行なえていなかった。ユーザへの教育が不要で、かつ重要ファイルを確実に保護できるようなシステムを簡単に構築できないだろうかと考え、「Universal Shield」の導入を決定した。

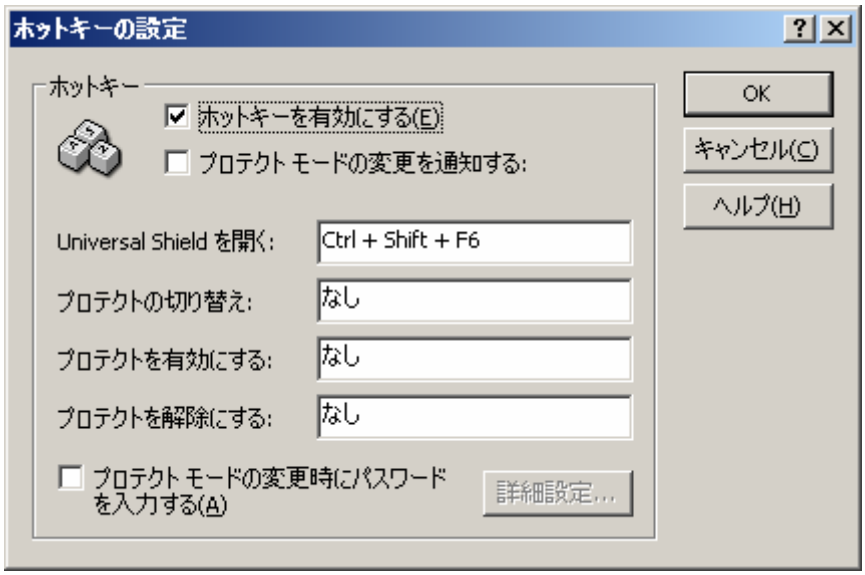
＜導入後の効果＞
「Universal Shield」自体を見せない設定により、ユーザにセキュリティを意識させない運用を実現。管理者のみが簡単な操作でセキュリティをオンオフできる点も、トラブルシューティングの際に役立っている。また、「ローカル以外の Office からはファイルを参照できなくする」など、共有、ユーザアカウントなどとは完全に独立したセキュリティ機能により、情報漏洩対策および切り分けを行なえるようになった。

nextEDGE TECHNOLOGY

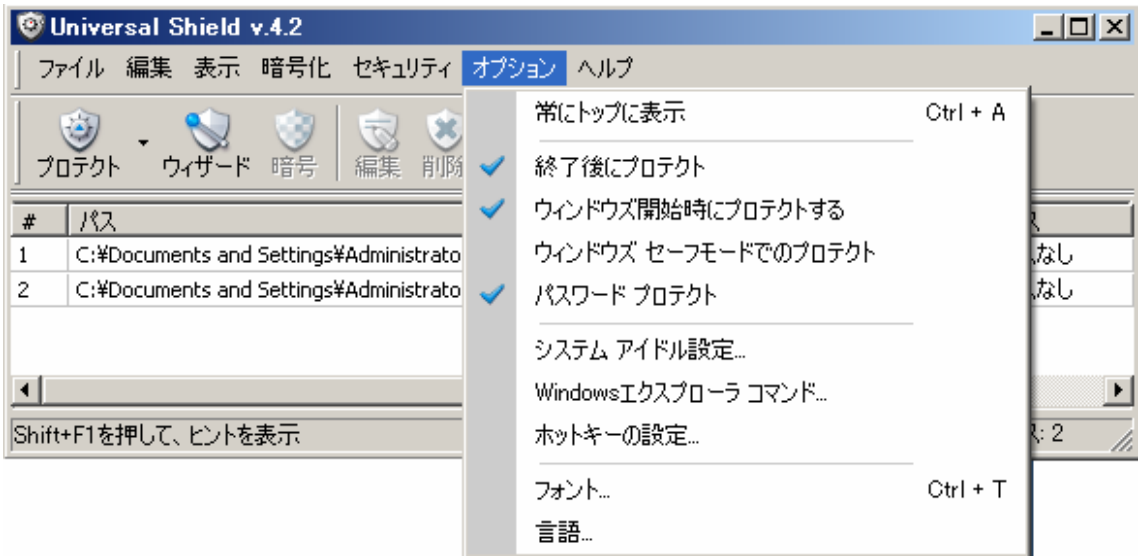
〈設定方法〉

1、 保護対象をリストに登録する。

2、 オプション→ホットキーの設定から、Universal Shield 起動用のホットキーを設定する。（その他ホットキーは任意）

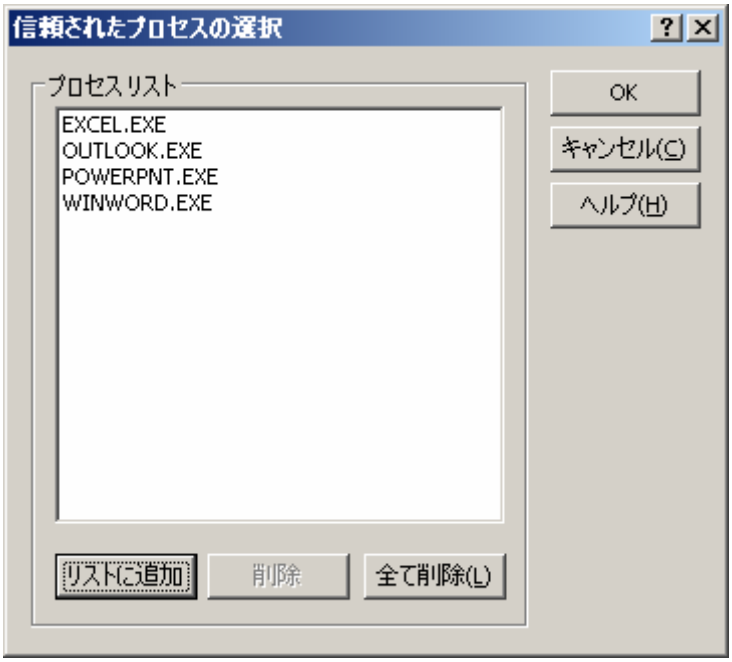


3、 オプションの[終了時にプロテクト]、[Windows 開始時にプロテクトする]、[パスワード プロテクト]が有効になっていることを確認する。

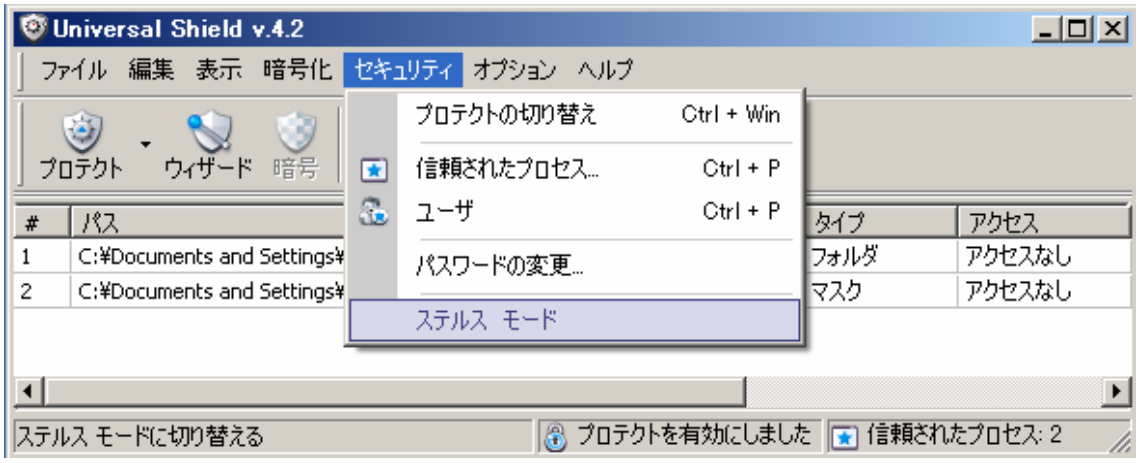


nextEDGE TECHNOLOGY

4、 オプション→信頼されたプロセスから、Office のアプリケーションを登録する。



5、 セキュリティ→ステル スモードを有効にする。



備考：さらにセキュリティを高めるために

ステルス モードを有効にすることで、一般ユーザからUniversal Shieldを隠したセキュリティ運用が可能となりますが、デフォルト設定では、管理者が Universal Shield を使用するためのホットキー用のサービスが常駐する為、他ユーザが偶然、設定したホットキーを押した場合にも、Universal Shield は動作しますので、万が一に備え、必ずパスワード保護の設定を行った上運用してください。また、さらに高度なオプションとして、登録されている「US30Service」のサービスを無効化する方法もあります。

nextEDGE TECHNOLOGY

セキュリティトリックの利用例

学校の授業で使用するPCや共用PCなどは、利便性や可用性を考慮したセキュリティを設定する必要があり、ユーザレベルやグループポリシーなどでの対応では不十分と言わざるを得ません。それらに加え、Universal Shieldのセキュリティトリックを用いることで、本当に必要なセキュリティ環境を構築することが可能となります。

セキュリティトリックとは保護リストのプリセットであり、これを利用することで、ユーザは簡単に特定の機能を抑制することができますが、これ以外にも、OSで利用する各機能用のファイルを個別に登録（可視化のみ許可する）することで、グループポリシーなどでも実現できない、特殊なセキュリティを構築することができます。

なお、Universal Shieldの保護機能は、簡単にオンオフが行える為、メンテナンス対応にも優れています。

XPで利用される各機能用のファイル例

Windows ファイアーウォール	%WinDir%¥System32¥firewall.cpl
インターネットオプション	%WinDir%¥System32¥inetcpl.cpl
キーボード	%WinDir%¥System32¥main.cpl
ゲームコントローラ	%WinDir%¥System32¥joy.cpl
システム	%WinDir%¥system32¥sysdm.cpl
セキュリティセンター	%WinDir%¥System32¥wscui.cpl
ネットワーク接続	%WinDir%¥system32¥ncpa.cpl
ハードウェアの追加と削除	%WinDir%¥System32¥hdwwiz.cpl
プログラムの追加と削除	%WinDir%¥system32¥appwiz.cpl
マウス	%WinDir%¥System32¥main.cpl
ユーザアカウント	%WinDir%¥system32¥nusrmgr.cpl
ユーザ補助のオプション	%WinDir%¥system32¥access.cpl
ワイヤレスネットワークセット	%WinDir%¥system32¥netsetup.cpl
アップウィザード	
画面	%WinDir%¥system32¥desk.cpl
自動更新	%WinDir%¥system32¥wuaucpl.cpl
地域と言語のオプション	%WinDir%¥System32¥intl.cpl
電源オプション	%WinDir%¥system32¥powercfg.cpl
電話とモデムのオプション	%WinDir%¥System32¥telephon.cpl
日付と時刻	%WinDir%¥System32¥timedate.cpl
各種管理用マネージャ	%WinDir%¥System32¥*.msc
MSCONFIG	%WinDir¥pchealth¥helpctr¥binaries¥msconfig.exe

nextEDGE TECHNOLOGY

ローカルデータベースの保護

例えば、個人情報を含んだ重要なデータベースをノートブックで持ち運ぶ必要がある場合、データベースファイルへのアクセスをアプリケーションが管理していてもデータベースファイルそのものが不正にコピーや改竄される危険があります。
Universal Shieldを導入することでデータベースファイルへのアクセスをロックし、専用のアプリケーションにのみ許可することでデータベースファイルの存在を隠すことができます。
不正なデータベースのコピーを防ぐことになります。

システム監視ログの保護

ユーザPCのアクティビティを監視するシステムを導入している場合に残されるセキュリティの問題として、アクティビティログの保護があります。アクティビティログが完全に保護されない以上、監視システムは無能化される可能性があります。
例えば、監視ログが一旦ローカルドライブに保存される場合、このログファイルが悪意のあるユーザにより削除されると、データの持ち出し、不正コピーを監視するシステムは全く無効化されることになります。
Universal Shieldを導入し、監視ログや監視Agentの存在を隠すことで、より完全なセキュリティシステムを構築できます。

システム管理ツールとの連携

Universal Shield(USPro.exe)をスイッチ付きで実行することで、保護の有効/無効を切り替えることができます。これらの機能を利用してリモートの管理コンソールからクライアントの保護設定を変更、ロック/ロック解除が可能になります。

保護の有効化

C:¥Program Files¥Universal Shield 4.2¥USPro.exe -E

保護の無効化

C:¥Program Files¥Universal Shield 4.2¥USPro.exe -D

注意: ステルスモードが有効な場合、管理プログラム(Agent)を、「信頼されたプロセス」に登録しておく必要がありますので注意してください。

nextEDGE TECHNOLOGY

付録

販売経歴(日本国内)

2004 年 8 月　www.shareEDGE.com　WebサイトからESD販売を開始。

2005 年 8 月　“PC プライバシー”としてパッケージ販売開始（発売元:サイバーリンクトランスデジタル社）

2007　年 7 月　大手建設会社による全社システムへの展開

対象 OS

クライアント向け:

Windows 2000 Professional、Windows XP　全 Edition、Windows Vista　全 Edition　※1 (x64 版を含む)

サーバ向け:

Windows 2000 Server、Storage Server Edition　以外の　Windows Server 2003、R2(x64 版を含む)

NAS 向け

Windows Powered NAS、Windows Storage Server 2003

※1Windows Vista には、2008 年初頭対応予定

nextEDGE TECHNOLOGY