Universal Shieldによるデスクトップ PC のシンクライアント化

～Windows のアキレス腱「デスクトップ」を書き込み禁止に～

株式会社ネクステッジテクノロジー

2008/5/20

はじめに

本ドキュメントは、データ非可視化&暗号化ソフトウェア「Universal Shield」を用いたセキュリティ環境についてまとめた管理者向けのドキュメントです。製品に関する詳細な仕様、操作方法については、製品カタログ、ユーザガイド等を参照してください。

目次

１、セキュリティ・バックアップ運用の理想と現実

セキュリティやバックアップ運用が見直されつつある今日において、重要なデータを各コンピュータのデスクトップやマイ ドキュメントなどのローカルハードディスクにデータを保存させず、ネットワーク上のNASなどに保存させ、管理者がこれを一元管理するといった運用が重宝されつつある。

これを実現するのにもっとも適した方法としては、やはりシンクライアントを用いた運用だろう。ただし、シンクライアントでは、容量やスペック的な制限により利用できるアプリケーションが限られてしまったり、また導入コストや既存のIT資産を有効活用できないといった点からも万能な対策とは言えない。

現状においては、ローカルハードディスク全体を暗号化することで盗難、紛失時におけるセキュリティを強化し、バックアップについては、保存先となる可能性のある場所全体をバックアップするという、ある種妥協案的な対策が取られているのが実情だ。

２、管理者を悩ませるWindowsの仕様「ユーザー プロファイル」

Windowsは、アクティブディレクトリのグループ ポリシーなどを用いることで、ほとんどすべての機能を抑制できるよう設計されているが、基本的にデスクトップやテンポラリなど、ユーザー プロファイルのパス変更は行えない。

そして、それらはシステムドライブ:¥Document and Settings¥各ユーザ名のフォルダ以下となり、自分のフォルダに対しそれぞれフルアクセス権が割り当てられる。

理想のセキュリティ・バックアップ運用の妨げとなるのは、まさにこのWindowsの仕様で、逆にここへの書き込みを抑制することで、理想のセキュリティ・バックアップ運用が可能となる。

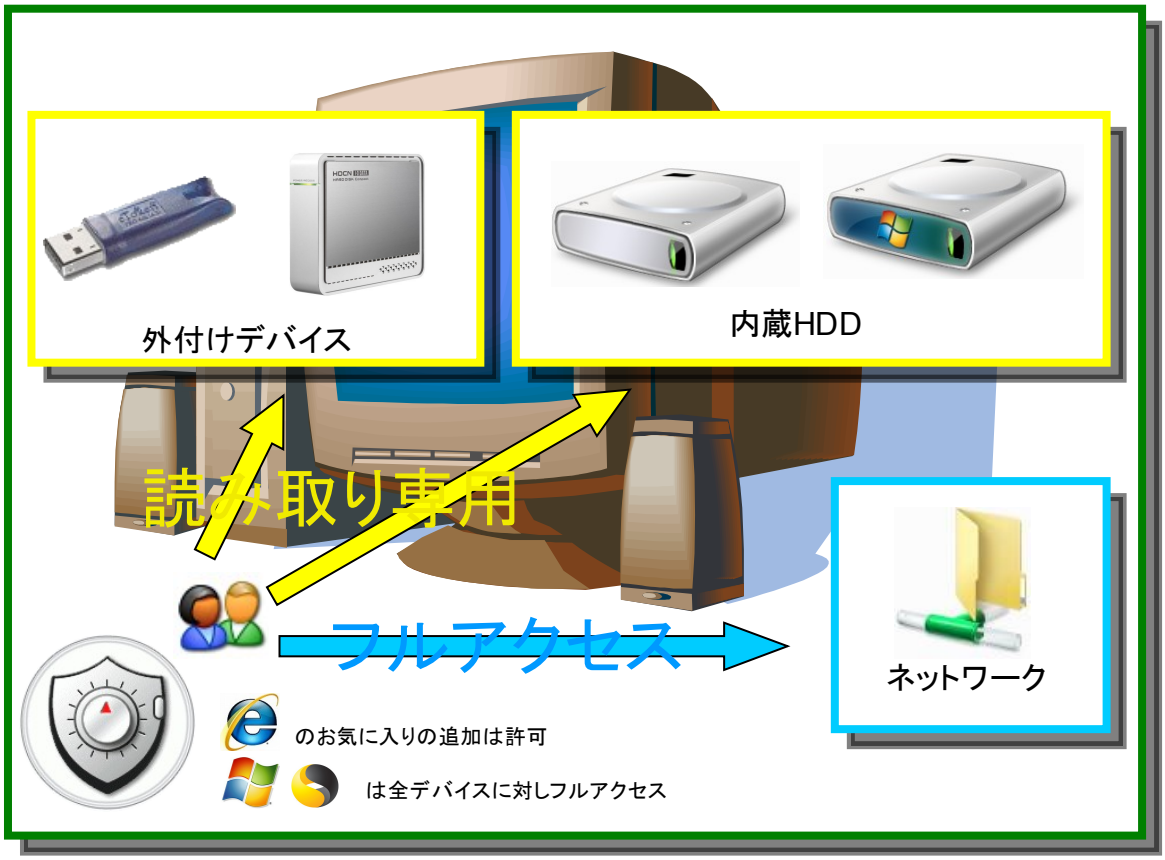
※正確には上記パスの変更も可能だが、変更に伴い運用の変更が必要となったり、その他Windowsの安定性、汎用性が失われる危険があるなど、非常にリスクが高いことから、それらを変更するケースはほとんどない。

３、シンクライアント化を実現可能とするUniversal Shield

Universal Shieldは、非可視化（OSから存在を隠す）を始めとするNTFSより上位の独自アクセス権により、対象を如何なる権限のプロセスからも確実に保護できるセキュリティソフトである。今回はこれをグループ ポリシーと併用し、デスクトップ、マイ ドキュメントなどにデータを保存させず、かつ管理性や併用性に富む理想的な環境の構築法を紹介する。

構築する環境

- ユーザデータをデスクトップ、マイ ドキュメントなどのローカルハードディスクに保存させない。
- アンチウィルスソフトは常時、ドライブ全体を常駐監視。
- お気に入りの追加のみ許可（履歴、Cookieの利用は禁止）。
- 外付けデバイスは、読み取り専用とする。
- Universal Shieldの存在をユーザから隠す。



４、Universal Shield の主な特徴

デスクトップ PC のシンクライアント化を実現可能とする Universal Shield の主な特徴を紹介する。

・ 柔軟な保護対象の指定方法
保護対象となるファイル、フォルダなどをワイルドカード付きのパスで指定することができる。また、ユーザ／グループ単位でのアクセス権指定も可能で、これらによりユーザー名など、環境独自の名称に捕らわれない汎用的な保護指定が可能となる。

・ 併用性の確保
プロセス単位での除外指定が可能で、これによりすべてのファイルにアクセスが必要となるアンチウィルスソフトやバックアップソフトなどの併用も可能となる。

・ メンテナンス性の確保
NTFS のアクセス権などと異なり、独自セキュリティ設定の有効／無効をコマンドレベルやボタンで簡単に切り替えることが可能で、これによりシステムのシステム環境のアップグレードなどにも柔軟に対応できる。

・ 最上位のセキュリティ
たとえ Domain Admins に所属するユーザであっても、UniversalShield のセキュリティ設定を変更することはできない。また、これはセーフモードの状態においても同様である。

・ ユーザに存在を隠した状態でのセキュリティ運用
ステルス モードを有効にすることで、Universal Shield の存在を全ユーザから完全に隠すことができる。

５、環境シナリオ

- ユーザが利用するPCは、ActiveDirectoryに参加したWindowsXP ProSP2。
- ユーザは、DomainUsersに所属する専用のドメインアカウントにてログオンする。
- ローカルハードディスクに用意されたパーティションはCドライブのみ。
- アンチウィルスソフトが常駐監視
- グループ ポリシーにて、マイ ドキュメントのパス変更および自動実行機能は禁止

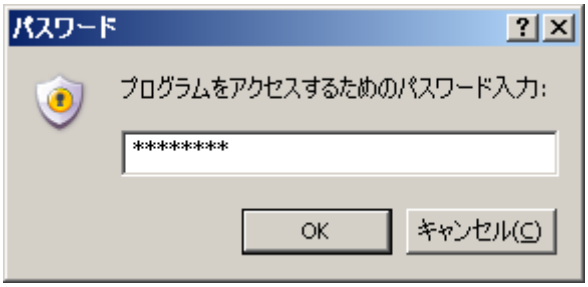
６、構築手順

Universal Shieldのインストール＆設定

1、 管理者権限を持つユーザにてログオン後、パラメータ -var:"InstallIcons=0" 付きでUniversal Shieldのインストーラを実行し、C:¥US42フォルダへインストールを行ないます。

```
ushield42_jpn.exe -var:"InstallIcons=0"
```

2、 システム再起動後、C:¥US42¥USPro.exeを実行し、Universal Shieldを起動します。なお、起動に際し、インストール時に設定した起動用パスワードを求められます。



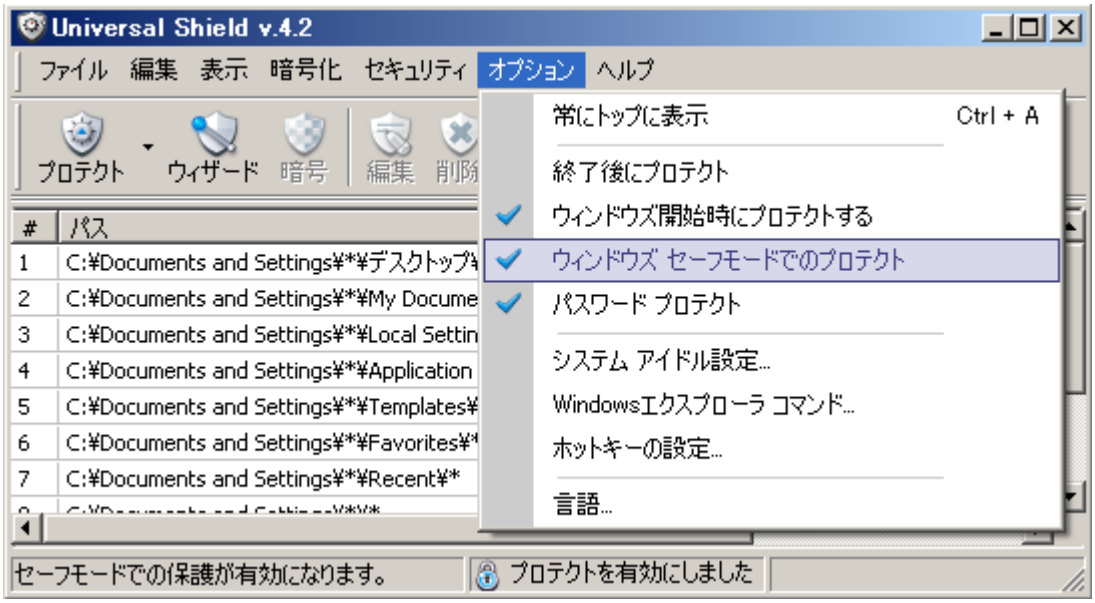
3、 メニューの[ファイル]>[オブジェクトのプロテクト]>[マスク]を選択し、次のプロテクト設定をそれぞれ登録します。

パス	読込み	書込み	削除	可視状態
C:¥Documents and Settings¥*¥Local Settings¥*	○	○	○	○
C:¥Documents and Settings¥*¥Application Data¥*	○	○	○	○
C:¥Documents and Settings¥*¥Templates¥*	○	○	○	○
C:¥Documents and Settings¥*¥デスクトップ¥*	○	×	×	○
C:¥Documents and Settings¥*¥My Documents¥*	○	×	×	○
C:¥Documents and Settings¥*¥Favorites¥*	×	×	×	×
C:¥Documents and Settings¥*¥Favorites¥*.url	○	○	○	○
C:¥Documents and Settings¥*¥Recent¥*	×	×	×	×
C:¥Documents and Settings¥*¥Cookies¥*	×	×	×	×
C:¥Documents and Settings¥*¥NetHood¥*	○	×	×	○
C:¥Documents and Settings¥*¥PrintHood¥*	○	×	×	○
C:¥Documents and Settings¥*¥SendTo¥*	○	×	×	○
C:¥Documents and Settings¥*¥スタート メニュー¥*	○	×	×	○
C:¥Documents and Settings¥*¥Local Settings¥History¥*	×	×	×	×
C:¥Documents and Settings¥*¥*	○	×	×	○
D:¥*	○	×	×	○
E:¥*	○	×	×	○
F:¥*	○	×	×	○

G:¥*	○	×	×	○
H:¥*	○	×	×	○
I:¥*	○	×	×	○
J:¥*	○	×	×	○
K:¥*	○	×	×	○
L:¥*	○	×	×	○
M:¥*	○	×	×	○
N:¥*	○	×	×	○
O:¥*	○	×	×	○
P:¥*	○	×	×	○
Q:¥*	○	×	×	○
R:¥*	○	×	×	○
S:¥*	○	×	×	○
T:¥*	○	×	×	○
U:¥*	○	×	×	○
V:¥*	○	×	×	○
W:¥*	○	×	×	○
X:¥*	○	×	×	○
Y:¥*	○	×	×	○
Z:¥*	○	×	×	○

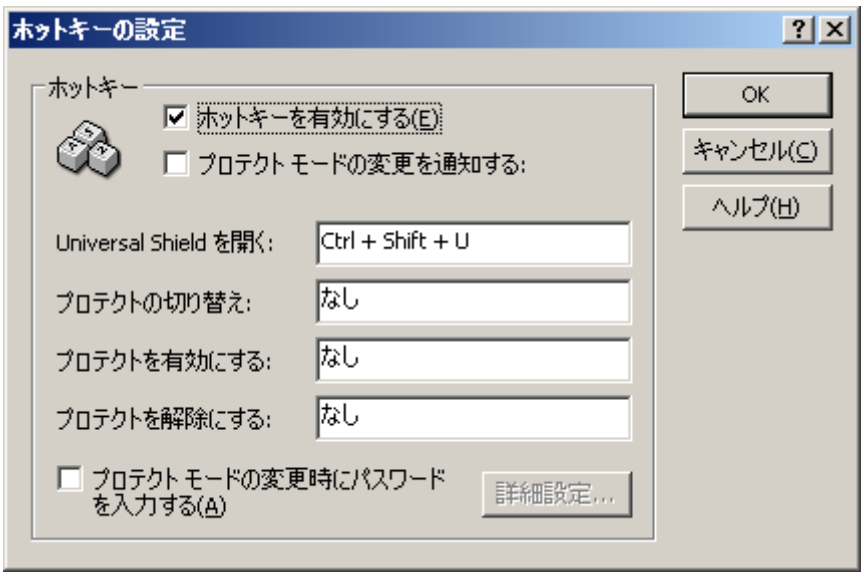
※環境や運用方針により、登録リストの内容は異なります。

4、 メニューの[オプション]>[ウィンドウズ セーフモードでのプロテクト]を選択し、オプションを有効化します。（チェックマークがつく）



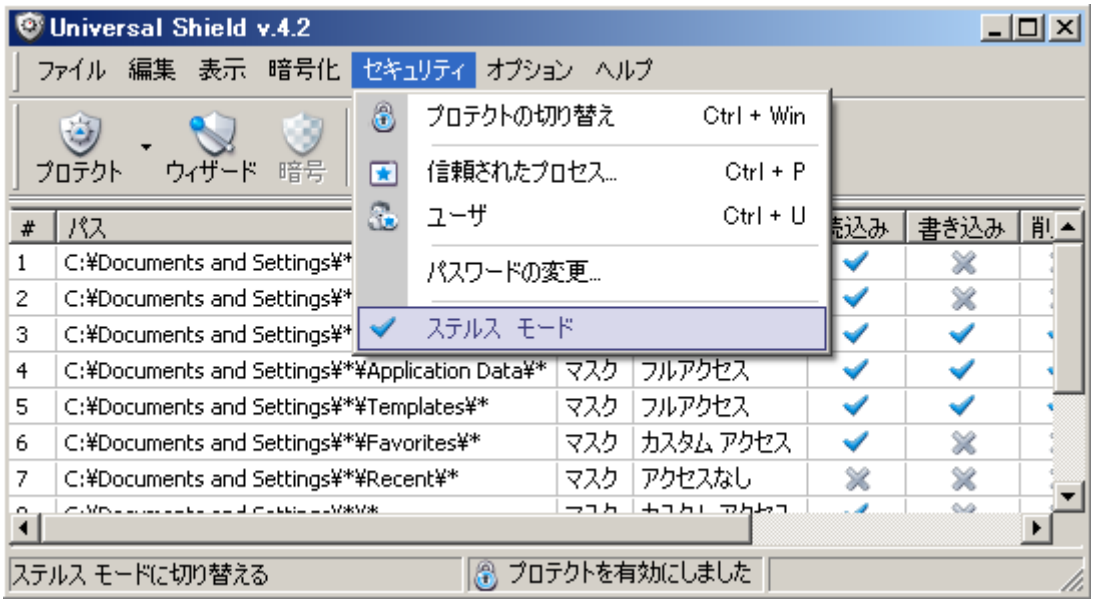
5、 メニューの[オプション]>[ホットキーの設定]を選択し、ホットキーの有効化、並びに

Universal Shield 起動用のホットキーを設定します。



6、 メニューの[セキュリティ]>[信頼されたプロセス]を選択し、[リストに追加]ボタンから、アンチウィルスソフトのプロセスを除外登録します。

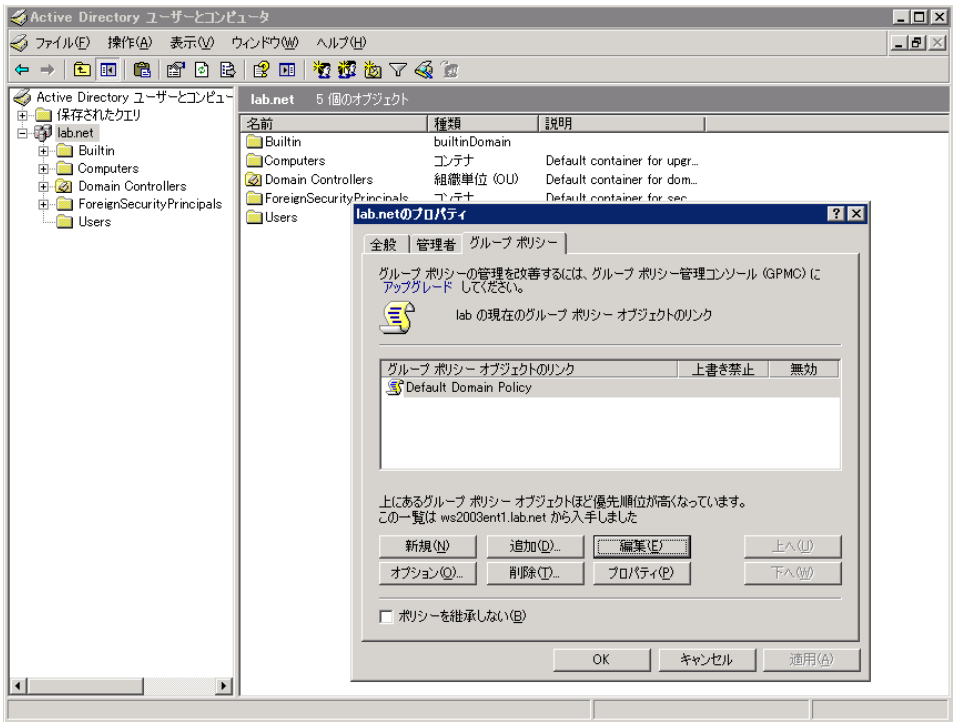
7、 メニューの[セキュリティ]>[ステルス モード]を選択し、オプションを有効化します。（チェックマークがつく）



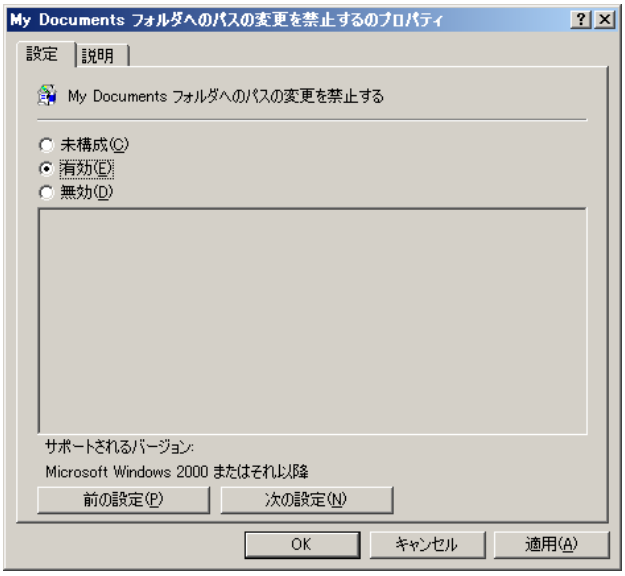
グループ ポリシーの設定

1、 ドメインコントローラのサーバーへ管理者権限でログオンし、[スタート]メニューから[ActiveDirectory ユーザーとコンピュータ]を選択します。

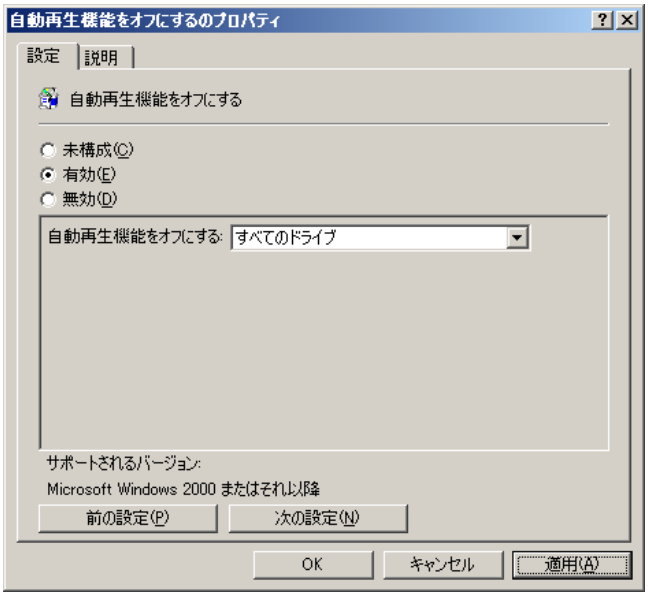
2、 ドメイン名を右クリック>[プロパティ]>[グループ ポリシー]タブからdefault Domain Policyを選択し、[編集]ボタンをクリックします。



3、 [ユーザーの構成]>[管理用テンプレート]>[デスクトップ]>[My Documents フォルダへのパスの変更を禁止する]を選択し有効化します。



4、［コンピュータの構成］>［管理用テンプレート］>［システム］>［自動再生機能をオフにする］を選択し、［有効］、［すべてのドライブ］を選択します。



７、スムーズな導入、管理の為に

初期導入時においては、Universal Shield導入済みのコンピュータをクローニングすることで、容易に複数台への導入も可能となるが、既存環境への導入においては、管理ツールなどを用いた一斉展開がもっとも有効な導入手段となる。
もちろん、ドメインのスクリプト機能などを用いた導入も可能ではあるが、運用後のシステムメンテナンス（プログラムの追加、大規模なアップデートなど）を考慮した場合、ネットワーク上から保護の有効／無効を指示できる管理ツールとの併用がもっとも望ましい。

なお、ネットワーク上からステルス モードで運用するUniversal Shieldの有効／無効を切り替えるには、専用ツールが必要となる。

８、お問い合わせ

株式会社ネクステッジテクノロジー　　担当：坂本、杉田
Tel:　029(858)1126
Web:　https://www.shareedge.com/modules/cs/index.php?c_lid=20040617-001