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
- 2. <u>管理者を悩ませる Windows の仕様「ユーザー プロファイル」</u>
- 3. シンクライアント化を実現可能とする Universal Shield
- 4. <u>Universal Shieldの主な特徴</u>
- 5. <u>環境シナリオ</u>
- 6. <u>構築手順</u>
- 7. スムーズな導入、管理の為に
- 8. <u>お問い合わせ</u>

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
 MTFS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



- ・ 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。



NTFSアクセス権の上位アクセス権で保護

5、環境シナリオ

- ・ ユーザが利用する PC は、ActiveDirectory に参加した Windows XP 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

 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"

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。

パスワー	۶ <u>؟</u> ×
٢	プログラムをアクセスするためのパスワード入力:

	OK キャンセル(C)

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¥*	0	0	0	0
C:¥Documents and Settings¥*¥Application	0	0	0	0
Data¥*				
C:\Documents and Settings*\Templates*	0	0	0	0
C:¥Documents and Settings¥*¥デスクトップ¥*	0	×	×	0
C:\Documents and Settings*\My Documents*	0	×	\times	0
C:\Documents and Settings*\Favorites*	×	×	\times	×
C:¥Documents and Settings¥*¥Favorites¥*.url	0	0	0	0
C:\Documents and Settings*\Recent*	X	×	\times	X
C:¥Documents and Settings¥*¥Cookies¥*	×	×	X	×
C:\Documents and Settings*\NetHood*	0	×	X	0
C:¥Documents and Settings¥*¥PrintHood¥*	0	×	X	0
C:\Documents and Settings*\SendTo*	0	×	X	0
C:¥Documents and Settings¥*¥スタート メニュ	0	×	×	0
¥*				
C:¥Documents and Settings¥*¥Local	×	×	×	×
Settings¥History¥*				
C:¥Documents and Settings¥*¥*	0	×	X	0
D:¥*	0	×	X	0
E:¥*	0	×	×	0
F:¥*	0	×	×	0

G:¥*	0	×	×	0
H:¥*	0	×	×	0
I:¥*	0	×	×	0
J:¥*	0	×	×	0
K:¥*	0	×	×	0
L:¥*	0	×	X	0
M:¥*	0	×	X	0
N:¥*	0	×	X	0
0:¥*	0	×	\times	0
P:¥*	0	×	X	0
Q:¥*	0	×	X	0
R:¥*	0	×	X	0
S:¥*	0	×	X	0
T:¥*	0	×	\times	0
U:¥*	0	×	\times	0
V:¥*	0	×	X	0
W:¥*	0	×	X	0
X:¥*	0	×	X	0
Y:¥*	0	×	X	0
Z:¥*	0	×	×	0

※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。

ホットキーの設定	? ×
ホットキー ホットキー ホットキーを有効にする(E)	ок キャンセル(<u>C</u>) ヘルプ(出)
Universal Shield を開く: Ctrl + Shift + U	
プロテクトの切り替え: なし	
プロテクトを有効にする: なし	
プロテクトを解除にする: なし	
□ プロテクトモードの変更時にパスワード を入力する(A) 詳細設定	

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。

信頼されたフロセスの選択	? ×
プロセスリスト DefWatch.exe Rtvscan.exe	ок キャンセル(С) ヘルプ(Н)
「リストに追加」前除 全て削除(し)	

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)

0	🞯 Universal Shield v.4.2							
7	ファイル 編集 表示 暗号化 セキュリティ オブション ヘルプ							
Ī	🕲 _ 😒 🎯	3	プロテクトの切	り替え	Ctrl + Win			
J	ロテクト ウィザード 暗号	*	信頼されたプロ	コセス	Ctrl + P			
#	パス	3	ユーザ		Ctrl + U	記み	書き込み	削▲
1	C:¥Documents and Settings¥*		パスワードの愛	5更		 Image: A set of the set of the	×	
2	C:¥Documents and Settings¥*					 Image: A second s	×	
3	C:¥Documents and Settings¥*	~	ステルス モー	ĸ		~	 Image: A set of the set of the	•
4	C:¥Documents and Settings¥*	¥Appli	ication Data¥*	マスク	フルアクセス	~	 Image: A set of the set of the	•
5	C:¥Documents and Settings¥*	¥Temp	plates¥*	マスク	フルアクセス	-	~	
6	C:¥Documents and Settings¥*	¥Favo	orites¥*	マスク	カスタム アクセス	-	×	1
7	C:¥Documents and Settings¥*	¥Rece	ent¥*	マスク	アクセスなし	*	×	
Î	C.VD	/*				1	0.0	₽
ステルス モードに切り替える								

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 Domai
 n Policyを選択し、[編集]ボタンをクリックします。

🥌 Active Directory ユーザーとコンピ	ደ - አ				_ 🗆 X
≪ ファイル(E) 操作(A) 表示(V) 「	フィンドウ(型) ヘルプ(世)				_ 8 ×
	🖻 💷 🦉 🖉 🐌 🖓 🍕	§ 🗑			
🎻 Active Directory ユーザーとコンピュー	lab.net 5 個のオブジェクト				
Idente University 1 y Local Identet Identet Computers Domain Controllers Domain Controllers Users	Addinet Of BUDS プリセンド 名前 Builtin Computers ② Domain Controllers □ Foreign-Security Principals □ Users Iso net 07 ② Def ⑦ルーフ ⑦ルーフ ⑦ルーフ ⑦ルーフ ⑦ルーフ ⑦ルー ⑦ルー ⑦ルー ⑦レー ⑦ルー ⑦ルー ⑦ルー ⑦ルー ⑦ルー ⑦ルー ⑦ルー ⑦ル	種類 しいitinDomain コンテナ 組織単位(OU) マ・テキ ロメティ ロメラット ロメラット ロメラット ロメラット ロメラット ロメロシー ロシー ロシー	説明 Default container for upgr Default container for see シー にするには、グループ ポリシー 管理 パープ ポリシー オブジェクトのリン のリンク 上 ジェクトほど優先順位が高くなって センクトほどした 型 フロパティ(空) OK キャン	マンソール (GPMC) (こ ク 書を禁止 無効 こ(います。 上へ(<u>い</u>) 下へ(<u>い</u>) ンセル 通用(<u>A</u>)	
	,				

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。

My Documents フォルダへのパスの変更を禁止するのプロパティ	<u>?</u> ×
設定 説明	
My Documents フォルダへのパスの変更を禁止する	
○ 未構成© ○ <u></u> ○ <u></u> 一 一 一 一 一 一 一 一 一 一 一 一 一	
	—
サポートされるバージョン:	
Microsoft Windows 2000 またほそれ以及降	
前の設定(P)次の設定(N)	
OK キャンセル 適用	

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。

自動再生機能をオフにするのブロパティ	<u>?</u> ×
設定 説明	
🗿 自動再生機能をオフにする	
 C 未構成(©)	
● 有効(E)	
○ 無効(D)	
自動再生機能をオフにする: すべてのドライブ ▼	
Microsoft Windows 2000 またはそれ以降	
前の設定(P) 次の設定(N)	
OK キャンセル 通用	(<u>A</u>)

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: <u>https://www.shareedge.com/modules/cs/index.php?c_lid=20040617-001</u>