VSSはユーザデータを守らない

2.1 はじめに

VSSはVolume Shadow Copy Serviceの略で、Windows XP/ Windows Server 2003以降に搭載されているバックアップ 関連の機能です。

VSSはスナップショットを作成することができ、ある時点のボ リュームの状態を保存することができます。ユーザはスナップ ショットを参照することで、スナップショットを作成した時点 のボリュームのデータにアクセスすることができます。これに は削除したファイルやデータが変更されたファイルも含まれ ます。また、スナップショット上のデータはリードオンリーで あるため更新されません。更にボリューム上でファイルがロッ クされていても、スナップショット上のファイルはロックされ ません。これらの特性を利用するとデータの完全なバックアッ プを行うことができます。 Windows 7/10のファイルやフォルダのプロパティに表示 される「以前のバージョン」タブから復元できるファイルもス ナップショットを利用しています(図-1)。ランサムウェアが流 行した際にスナップショットからファイルを復元する方法が 紹介されていたことを記憶している人も少なくないでしょう。

スナップショットは攻撃者が使用した攻撃ツールや一時ファイ ル、改ざんされたファイルなどの復元に利用できるため、デジタ ルフォレンジックにおいても非常に重要なデータの1つとして、 解析者たちに認識されています。しかし今回、デジタルフォレン ジックの技術調査を行う中で、VSSを有効にしていてもユー ザのデータがスナップショットに正常に保存されない事象を Windows 8.1/10で確認したため、その原因と影響範囲を調査し ました。また、事象の対処方法についても紹介します。



図-1「以前のバージョン」タブ

図-3 スナップショットアクセスの仕組み



2.2 VSSスナップショットの仕組み

前述したように、スナップショットはある時点のボリュームの 状態を保存しますが、ファイル単位でデータの保存を行ってい るわけではありません。例えば、1GBのファイルの内、1MBを変 更した際にファイル全体を保存するのは、ボリュームの使用効 率が悪い上にOS全体のパフォーマンスも低下してしまいます。



図-4 スナップショットはユーザアクセスから保護されている

そのため、スナップショットには差分データのみが保存され ます。ボリューム全体を16KBごとのデータブロックに分割し、 スナップショット作成後に変更が発生したデータブロックの データをそのオフセットと共に保存したものが差分データと なります(図-2)。スナップショット上のファイルにアクセスす る際には、現在のボリュームデータにスナップショットの差分 データを透過的に統合して、スナップショット作成時のデータ を再構築します(図-3)。

2.3 VSSスナップショットのファイル構成

スナップショット関連のファイルはボリュームのルートフォ ルダ直下の「System Volume Information」フォルダに保存 されていますが、通常はエクスプローラなどではアクセスする ことができません(図-4)。図-5ではFTK Imager*1を使用して ファイルを表示しています。

Evidence Tree	\times	File List			×
D. NONAME [NTFS]	^	Name	Size	Туре	Date Modified
🗄 🛅 [orphan]		SPP	1	Directory	10/20/2017 5:4
[root]		SystemRestore	1	Directory	10/20/2017 5:2
G SBadClus		Windows Backup	1	Directory	10/20/2017 5:3
		SI30	4	NTFS Index All	10/20/2017 5:3
Secure		lndexerVolumeGuid	1	Regular File	10/16/2017 10:
		MountPointManagerRemoteDatabase	0	Regular File	10/16/2017 10:
Documents and Settings		Tracking.log	20	Regular File	10/16/2017 10:
PerfLogs		UVcifs.md リタロク	1	Regular File	10/16/2017 8:1
🕀 🗁 Program Files		WDSettings dat	1	Regular File	10/16/2017 6:5
😟 🧰 Program Files (x86)		{3808876b-c176-4e48-b7ae-04046e6cc752}	64	Regular File	10/19/2017 12:
🕀 👘 Program Data		[] {95e1f108-b4c4-11e7-a9a4-7c7a91d0d869}{3808876b-c176-4e48-b7ae-04046e6cc752}	139,312	Regular File	10/20/2017 5:2
		[] {95e1f57d-b4c4-11e7-a9a4-7c7a91d0d869}{3808876b-c176-4e48-b7ae-04046e6cc752}	327,680	Regular File	10/20/2017 5:2
Upor		フトマ			
E Windows		ストア			
Free [unallocated space]	~				
	_	0000 65 87 08 38 76 CI 48 4E-57 AE 04 04 6E 6C C7 52 K ·· 8VARN ·8· · 11	Çκ ···		^
Properties	×	0020 00 C0 7E 0A 00 00 00 00-00 00 7F 0A 00 00 00 ·À~······			
2↓		0030 00 00 00 00 00 00 00 00 00 00 00 00	•••		
8					
Name (2000076h c176 4c40 h7					
100000100-C110-4640-D1	•	0070 00 00 00 00 00 00 00 00 00 00 00 00			
File Class Regular File		0080 02 00 00 00 00 00 00 00-00 00 A0 E0 09 00 00 00 ······ à··			
File Size 65,536		0090 08 F1 E1 95 C4 B4 E7 11-A9 A4 7C 7A 91 D0 D8 69 ·ñá·Ä′ç·©¤ z·Đ	Øi		
Physical Size 65,536		00a0 01 00 00 00 00 00 00 00-40 04 00 00 00 00 00 00 00			
Start Cluster 42,988					
Date Accessed 10/19/2017 12:18:23 PM		00d0 00 00 00 00 00 00 00 00 00 00 00 00	• •		
Date Created 10/19/2017 12:18:23 PM		00e0 00 00 00 00 00 00 00 00-00 00 00 00 00	• •		
Date Modified 10/19/2017 12:18:23 PM		0100 03 00 00 00 00 00 00 00 00 00 00 00 0			
	-	0110 08 F1 E1 95 C4 B4 E7 11-A9 A4 7C 7A 91 D0 D8 69 .ñá.Ä´ç.@¤ z.Đ	Øi		
		0120 00 00 50 F0 04 00 00 00-00 80 50 F0 04 00 00 00 ··Pð·····Pð··			
		0130 00 00 52 F0 04 00 00 00-DA 00 00 00 00 00 04 00 ··Rð····Ú·····	•••		~
Properties Hex Value Inter., Custom Con	tel	Cursor pos = 0; dus = 42988; log sec = 343904			•
- ropenes - rick value internit Custom Con	1	Cursor pos = 0, cus = 12500, log sec = 010501			

図-5 「System Volume Information」フォルダ内のファイル構成

*1 FTK Imager(https://accessdata.com/product-download)。

スナップショットは「カタログ」と「ストア」という2種類のファ イルから構成されています。カタログは「{*カタログGUID*}」と いうファイル名で、スナップショットの生成日時やストアの GUIDといったメタ情報を記録しています。ストアは「{*ストア GUID*}{*カタログGUID*}」というファイル名でスナップショット のデータ本体になります^{*2}。

2.4 VSS有効化とスナップショットの操作

VSSは「システムのプロパティ」で有効か否か確認することがで きます(図-6)。無効になっている場合は「構成(Configure)」ボ タンをクリックして、「システム保護対象」ダイアログを表示し ます。そして、「システムの保護を有効にする(Turn on system protection)」を選択し、「ディスク領域の使用量(Disk Space Usage)」を設定後、「OK」ボタンをクリックします(図-7)。ス ナップショットを手動で作成する場合、図-6の「作成(Create)」 ボタンをクリックします。 なお、同一のボリューム内にスナップショットを複数作成する ことができますが、図-7で設定した「ディスク領域の使用量」を 超える場合、もっとも古いスナップショットが削除されます。

作成したスナップショットのリストの確認や削除などは、 vssadmin.exeで行うことができます。管理者権限のコマンドプ ロンプトから、「vssadmin.exe list shadows」を実行するとス ナップショットのリストを取得することができます(図-8)。そ の他、WMIやPowerShellからスナップショットを操作するこ とも可能です。

2.5 ファイル復元テスト

ユーザが作成したファイルがスナップショットに正常に保存 されるか検証するために、スナップショットに保存されたファ イルを復元するテストを行います。ユーザデータとして、弊社 のWebページで公開しているIIR Vol.26からVol.35の10個の

ystem Properties			×	🏪 System Protect	tion for Local Disk (C:)	×
Computer Name Hard Use system p System Restore — You can undo system your computer to a pr	Iware Advanced protection to undo un n changes by reverti revious restore point	System Protection nwanted system chan- ing System R	Remote ges. estore	Restore Settings - By enabling system reverting your con Turn on sys Disable system	m protection, you can undo undes mputer to a previous point in time. tem protection tem protection	ired changes by
Protection Settings Available Drives New Volume (E Local Disk (C:) Configure restore se and delete restore poin have system protect	E:)) (System) ettings, manage disk points. nt right now for the o tion turned on.	Protection On Space, Config drives tha Crea	gure	Disk Space Usage · · You can adjust th space fills up, olde ones. Current Usage: Max Usage: Delete all restore	e maximum disk space used for sy er restore points will be deleted to 248.91 MB 10% (3.95 GB) points for this drive.	stem protection. As make room for new
	OK	Cancel	Apply		OK Car	Apply
図-6	「システムのプロ	パティュダイアログ		1	図-7「システム保護対象」ダイ	アログ

*2 今回はスナップショットのファイル構成やデータ構造については取り扱わない。詳細について知りたい場合、Volume Shadow Snapshot(VSS) (https://github. com/libyal/libvshadow/blob/master/documentation/Volume%20Shadow%20Snapshot%20(VSS)%20format.asciidoc)が非常に参考になる。



PDFファイルをデスクトップの「PDF」フォルダに保存し、ス ナップショットを作成しました。

ファイル削除ツールであるSDelete^{*3}を使ってPDFフォルダ 内のファイルを削除し、その後、ShadowExplorer^{*4}を使用し てスナップショットからデータを復元します。 Windows 7 SP1とWindows 10 1703の環境でこの作業を 行い、それぞれのスナップショットから復元したPDFのMD5 ハッシュ値^{*5}を表-1にまとめました。Windows 7ではすべて のファイルが正常に復元できたのに対して、Windows 10で はすべてのファイルが破損していました。

G Administrator: Command Prompt	-	×
C:\Windows\system3 vssadmin 1.1 - Vol ume Shadow Copy Scivice a dministrative command-line tool (C) Copyright 2001-2013 Microsoft Corp.		^
Contents of shadow copy set ID: {0628d116-4d3a-4135-8bc1-4f3dcd9bd177} Contained 2 shadow copies at creation time: 10/19/2017 9:18:25 PM Shadow Copy ID: {d8e0e408-e086-421e-b6c1-48dec6b15c9d} Original Volume: (E:)\\?\Volume{e73eeadf-0000-0000-1000000000000}\ Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2 Originating Machine: WIN10 Service Machine: WIN10 Provider: 'Microsoft Software Shadow Copy provider 1.0' Type: ClientAccessibleWriters Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered		
<pre>Shadow Copy ID: {c0a46b95-a6eb-41b4-8bde-546df26b762c} Original Volume: (C:)\\?\Volume{6a7fcfc8-0000-0000-501f00000000}\ Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1 Originating Machine: WIN10 Service Machine: WIN10 Provider: 'Microsoft Software Shadow Copy provider 1.0' Type: ClientAccessibleWriters Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered</pre>		
Contents of shadow copy set ID: {29b8e867-ce5d-4a6c-9a94-ab38e5e5f724} Contained 2 shadow copies at creation time: 10/20/2017 2:29:30 PM Shadow Copy ID: {9a87ca60-c6bc-4803-b074-5ad905dbc8de} Original Volume: (E:)\\?\Volume{e73eeadf-0000-0000-0000-100000000000}\ Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4		~

図-8 スナップショット一覧

フラノリタ		Windows 7 SP1	Windows 10 1703		
ノアイル名		復元したファイルのMD5 -		復元したファイルのMD5	一致
iir_vol26_EN.pdf	a3002c631ca894034b594ec4e1a7c285	a3002c631ca894034b594ec4e1a7c285	0	42b4ac3f7e2f349ed8a0d3e240db35a6	×
iir_vol27_EN.pdf	09339fc3375988f8f769ccfa7ac75d4f	09339fc3375988f8f769ccfa7ac75d4f	0	e4986e8866435b7273f16a7f8fe60a14	×
iir_vol28_EN.pdf	89fee5ffccfb5be9749639e7e65a218e	89fee5ffccfb5be9749639e7e65a218e	0	86ff8c095a5b116e1ff34e12d6999053	×
iir_vol29_EN.pdf	42edeccedd51eecc20d0d9c123329b9a	42edeccedd51eecc20d0d9c123329b9a	0	5a8a530c084e5ee8ec129c62afa5ab0e	×
iir_vol30_EN.pdf	25df11281a2b1fb72a3f6d48d697c6b4	25df11281a2b1fb72a3f6d48d697c6b4	0	a4a68b122007b80a24ca2457e69b0902	×
iir_vol31_EN.pdf	79eac7926477141397f179654d307473	79eac7926477141397f179654d307473	0	b8cac677d7cf6bf15594a477c4b1b104	×
iir_vol32_EN.pdf	a99869ea8ea3cbda032d36ba000cdd26	a99869ea8ea3cbda032d36ba000cdd26	0	1bd79719c9c91c52e1de214a16572f90	×
iir_vol33_EN.pdf	a246c3f7ef836a141eb9c181899003f3	a246c3f7ef836a141eb9c181899003f3	0	17b820ab7f61a6de25cfcc89a1f49e62	×
iir_vol34_EN.pdf	093f3757b7a9269655d9fa6816b6dc72	093f3757b7a9269655d9fa6816b6dc72	0	b3c354a635ec62d747ae20aa71f46ab0	×
iir_vol35_EN.pdf	256dd74e71e1080170ddf59d0757e230	256dd74e71e1080170ddf59d0757e230	0	6220ce0b3df16961123438bd524568ce	×

表-1 復元ファイルの比較

- $* 3 \quad {\tt SDelete(https://technet.microsoft.com/ja-jp/sysinternals/sdelete.aspx)}_{\circ}$
- *4 ShadowExplorer.com(http://www.shadowexplorer.com/)。
- *5 MD5ハッシュが衝突しやすいことは知られているが、特定ファイルの同一性の比較であること、また、紙面の広さの制限から採用した。

2.6 ファイル破損の原因と対策

破損しているファイルを正常なファイルとバイナリエディタ で見比べると、ファイルの一部がNullバイト(0x00)で置き換 わってしまっていることが分かります(図-9)。左がオリジナル のファイルで右がWindows 10から復元したファイルです。 赤い箇所がデータの異なっている部分になります。ファイルに よって、Nullバイトに置き換わっている箇所は異なります。

調査の結果、スナップショットのユーザデータが破損する原因 はWindows 8から導入された「ScopeSnapshots^{*6}」という機 能であることが分かりました^{*7}。この機能が有効になっている 場合、スナップショットに保存する対象のデータがWindows のシステムに関連するファイルのみに限定されるため、ユーザ データはスナップショットに保存されなくなります^{*8}。この機 能はシステムボリューム(Cドライブ)のみに適用されますが、 近年のPCのドライブ構成はCドライブのみということも珍し くないため、この機能の影響は大きいと言えます。

機能仕様の詳細が公開されていないので、テスト結果からの推 測を含みますが、ファイルを限定する動作は完璧に制御されて いるわけではないようで、ユーザデータの一部だけがスナップ ショットに保存される場合もあります。このような不完全な ユーザデータを復元しようとした際に不足しているデータ部 分が0x00に置き換わっている可能性があります。なお、ファイ ルがレジデント^{*9}であればユーザデータであっても、スナップ ショットに保存されていました。

			_				
Stirling - iir_vol27_EN.pdf - 🗖 🗙							
7/4(F) 編集(E) 検索・移動(S) 設定(C) ?2/Y?(W) ヘル7(H)							
	<u> * .+ * .</u>						
iir_vol27_EN.pdf		iir_vol27_EN.pdf					
Image: Product State Image: P	O123456789.46CDEF A IBi Ap., 8) XGy. ct. Swig27. + オン科書 ・ オン科書 ・ ・ オン科書 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	C 回 这 O123456789ABCDEF ^ · 小は、 · 、 · 小は、 · 、 · 小は、 · 、 · への ·				
17*4		0x00000EDB	上書 5778421 Bytes SHIFT-IIS				

図-9 正常なデータと破損データの比較

- *6 Calling SRSetRestorePoint(https://msdn.microsoft.com/ja-jp/library/windows/desktop/aa378727(v=vs.85).aspx)。
- *7 マイクロソフトからも、この機能が原因である可能性が高い旨の回答を得ている。
- *8 このような仕様変更が行われた理由は公にはなっていないが、すべてのデータをスナップショットに保存することのパフォーマンスの問題やスナップショット用 領域の使用効率の問題、ユーザデータの肥大化、ユーザデータのバックアップに「ファイル履歴」が推奨されるようになったことなどが関係していると推測される。
 *9 NTFSはファイルデータが小さい場合、データ用に領域を確保せず、NTFSのMFTレコード内の\$DATAアトリビュートに直接保存する。この状態をレジデントと呼ぶ。



ScopeSnapshotsはレジストリの「HKLM\Software\ Microsoft\Windows NT\CurrentVersion\SystemRestore」 キーに「ScopeSnapshots」という名前でDWORD値「0」を 設定し、OSを再起動することで無効化できます(図-10)。 ScopeSnapshotsを無効化したWindows 10で、スナップ ショットからユーザデータが正常に復元できることも確認し ています^{*10}。

確認した限り、サーバ系Windowsでは、ScopeSnapshotsの 無効化なしでスナップショットからユーザデータを正常に復 元することができました。デフォルト設定のOSごとに復元したユーザデータの破損の有無を表-2にまとめました。

2.7 まとめ

VSSはWindows XPの頃から存在する機能ですが、OSのバー ジョンアップに伴って仕様が変更されていたことが今回分 かりました。このように従来から使用されていた機能でも仕 様が変更される場合があるため、OSのリリースなどに合わせ て、仕様変更の確認や使用しているツールの検証を行うこと が重要です。

Registry Editor			- 0	×
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SO	FTWARE\Microsoft\Win	dows NT\CurrentVers	ion\SystemRestore	
RemoteRegistry 🔺	Name	Туре	Data	
> Schedule	ab (Default)	REG SZ	(value not set)	
> SecEdit	10 FirstRun	REG DWORD	0x00000000 (0)	
> Sensor	2001 actindey	REG DWORD	0x00000002 (2)	
> - setup	20 LastMainenance	REG_OWORD	0x1d24066fe2f5df0 (121520520823885206)	
> SoftwareProtection	BDCossionIntenal	REG_QWORD	0.00000001 (1)	
> SPP		REG_DWORD	0x0000001(1)	
> . SRUM	and standbolle	NEO_DWOND		
> Superfetch	ScopeSnapshots	REG_DWORD	0x00000000 (0)	
> SvcHost				
> SystemRestore				
Sure Terminal Server				

図-10 ScopeSnapshots無効化の設定

表-2 OS別復元したユーザデータの破損の有無

	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2012/2012 R2	Windows Server 2016
復元したユーザデータの破損	なし	あり	あり	なし	なし



^{執筆者:} **齋藤 衛**(さいとう まもる)

IIJ セキュリティ本部 本部長、セキュリティ情報統括室 室長兼務。法人向けセキュリティサービス開発などに従事の後、2001年よりIIJグループの緊 急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。ICT-ISAC Japan、日本セキュリティオペレーション事業者協議 会など、複数の団体の運営委員を務める。

小林 稔(VSSはユーザデータを守らない) IIJ セキュリティ本部 セキュリティ情報統括室