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。

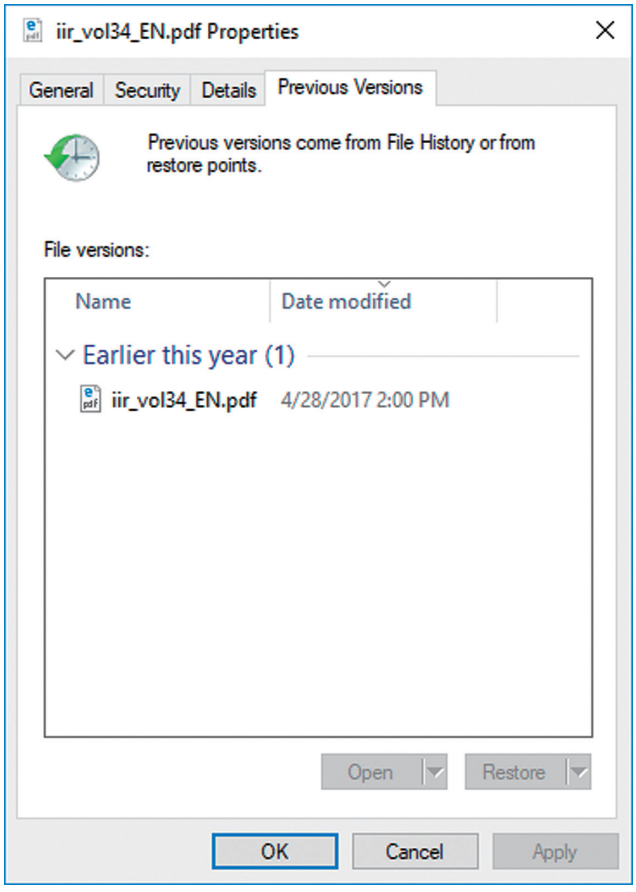

図-1「以前のバージョン」タブ

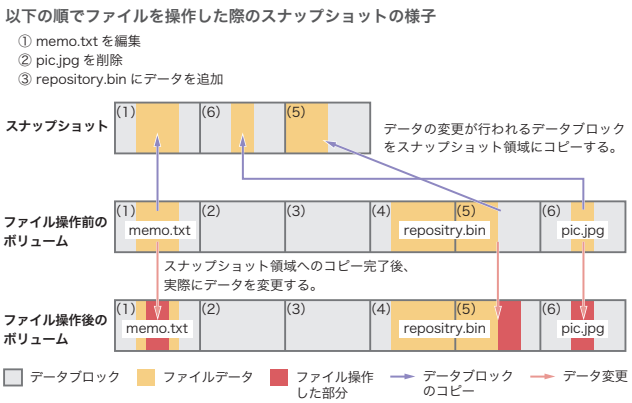

図-2 差分データ保存の仕組み

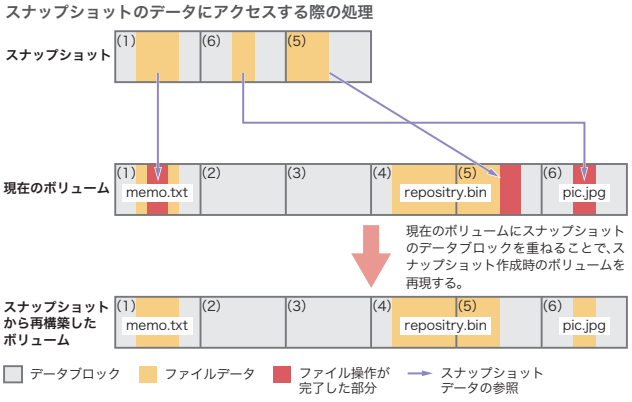

図-3 スナップショットアクセスの仕組み

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。

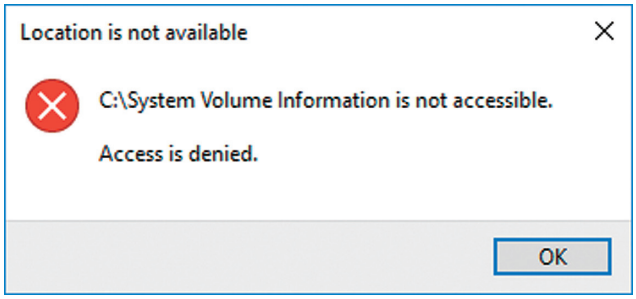

図-4 スナップショットはユーザアクセスから保護されている

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。

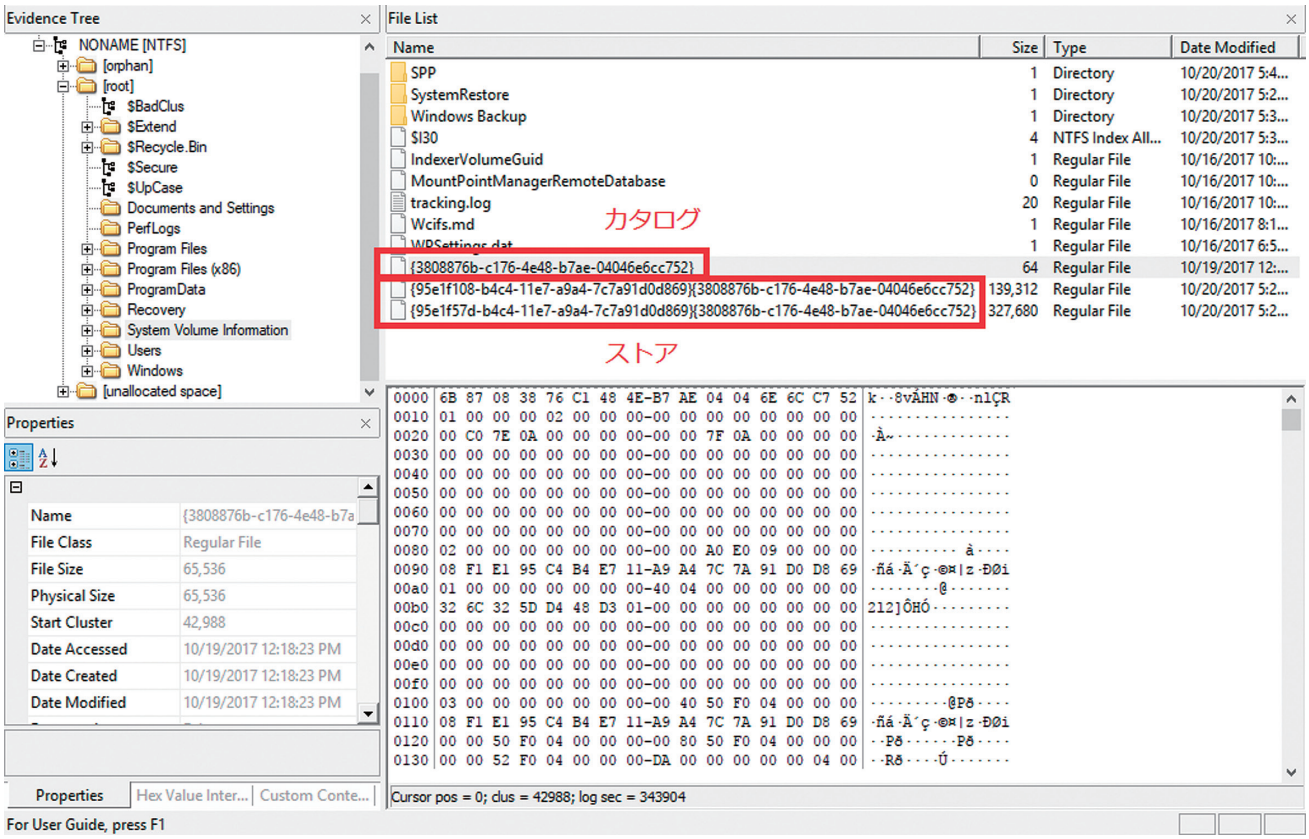

図-5「System Volume Information」フォルダ内のファイル構成

*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

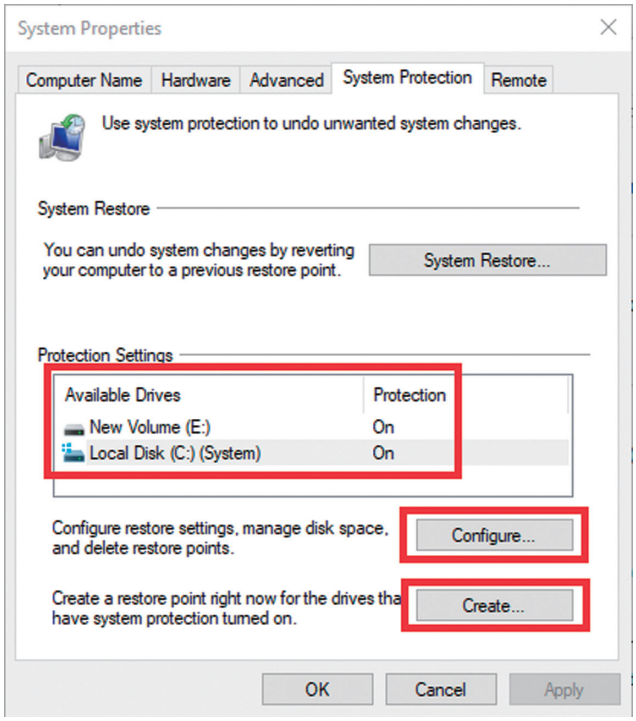

図-6「システムのプロパティ」ダイアログ

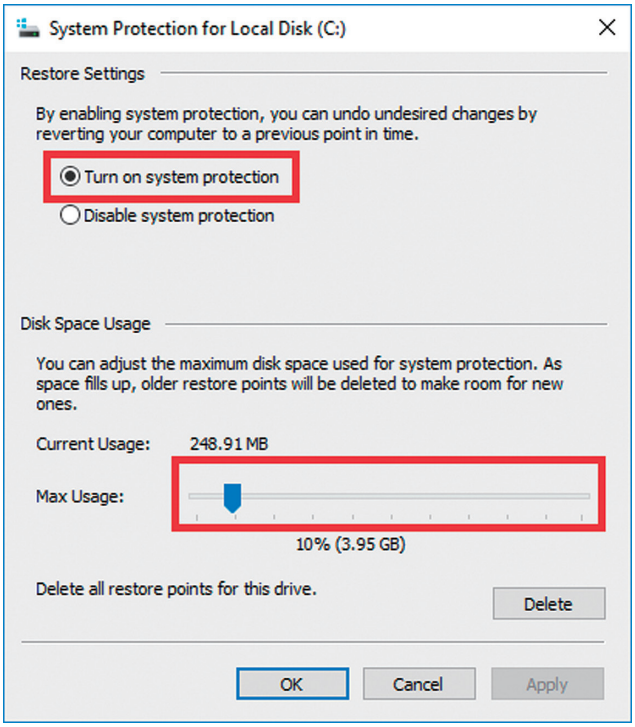

図-7「システム保護対象」ダイアログ

*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。

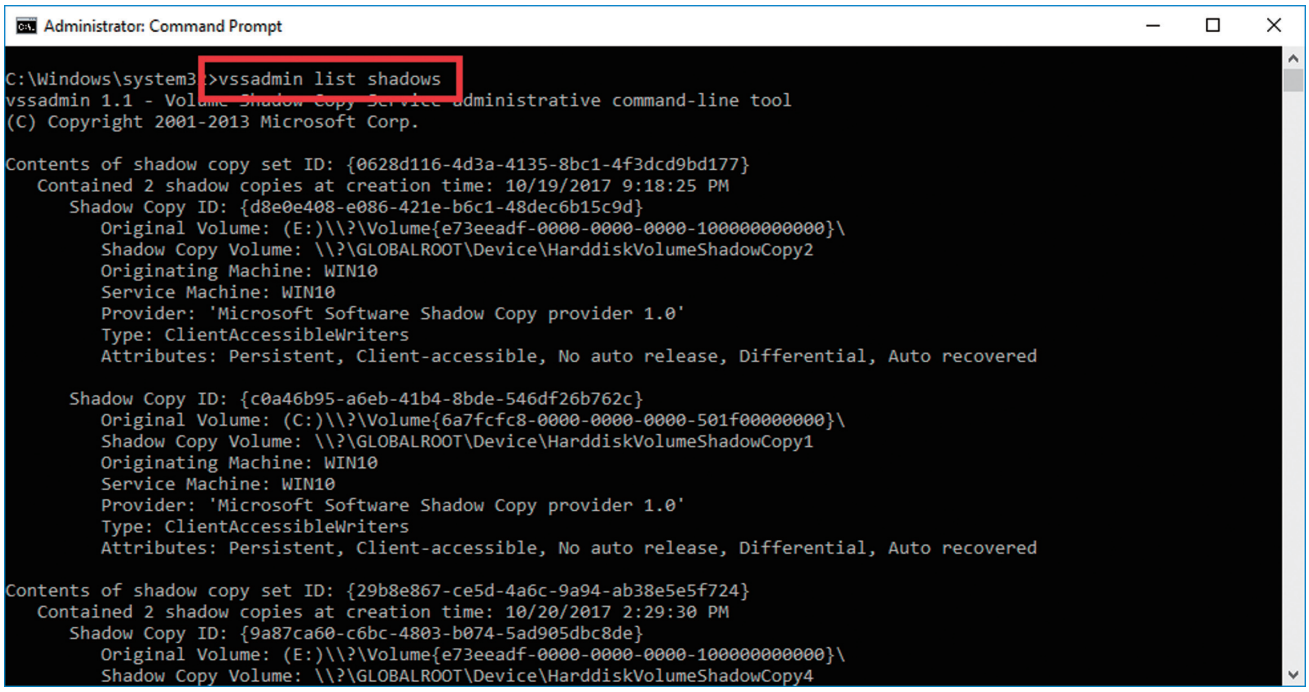

図-8 スナップショット一覧

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

表-1 復元ファイルの比較

*3 SDelete(https://technet.microsoft.com/ja-jp/sysinternals/sdelete.aspx)。
*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。

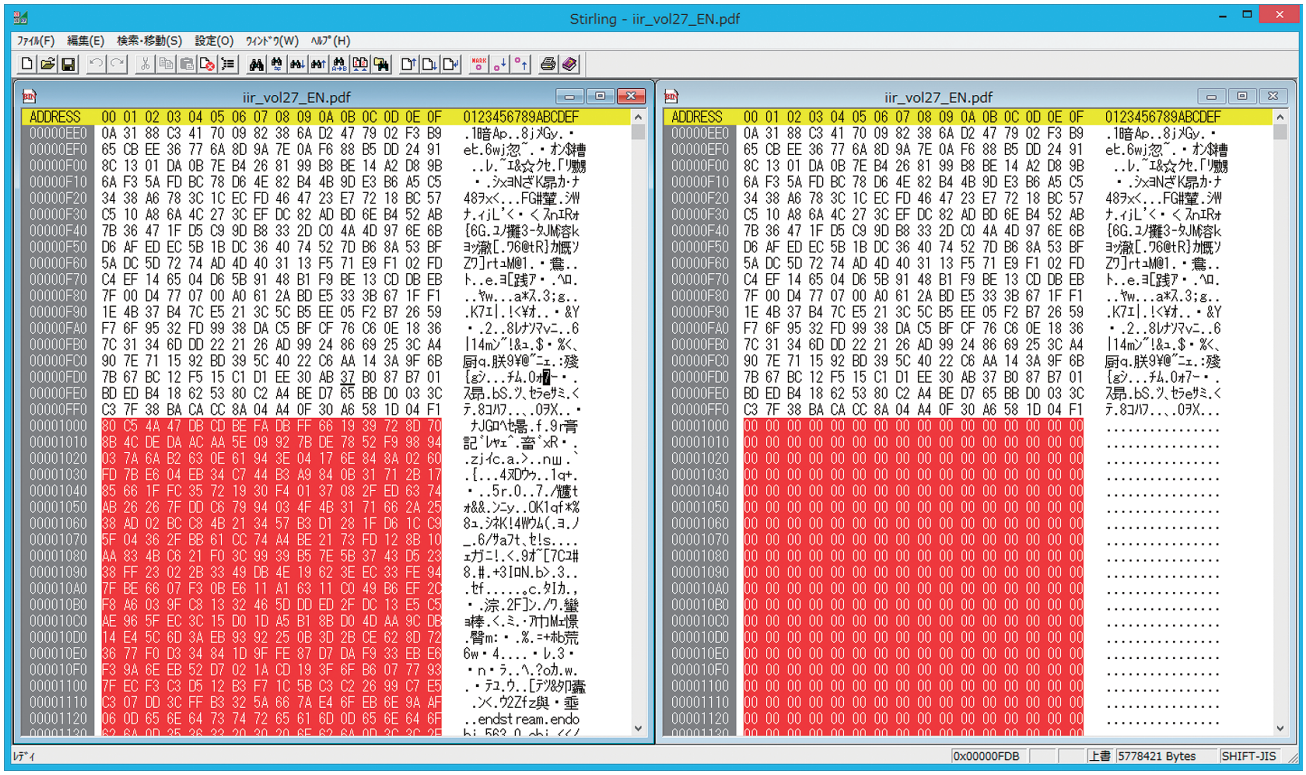

図-9 正常なデータと破損データの比較

*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。

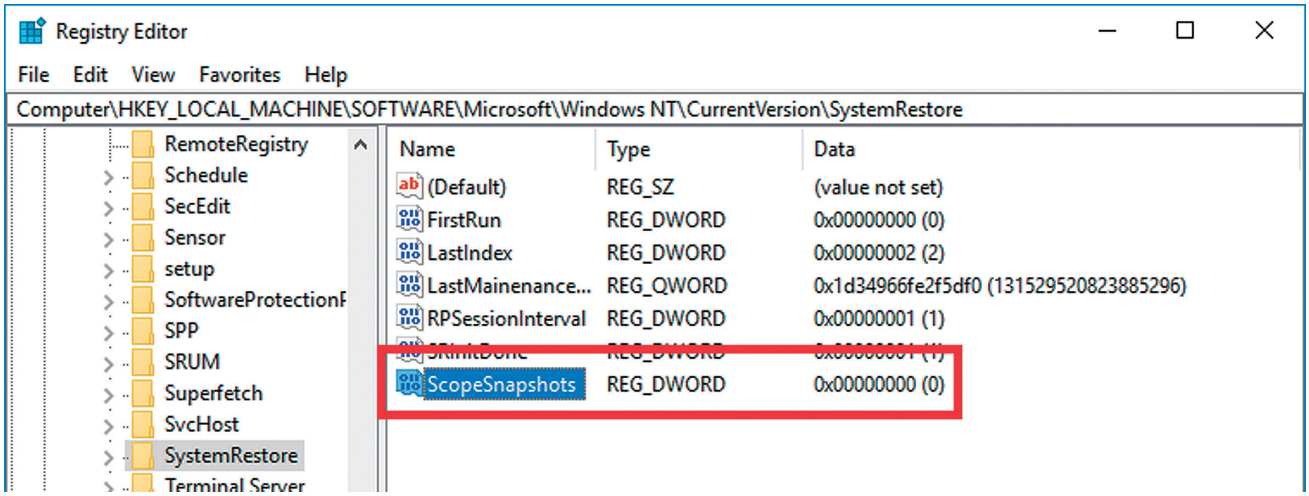

図-10 ScopeSnapshots無効化の設定

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

*10 Windows 8.1でも一連の検証を行ったが、Windows 10と同様の結果になった。