シャドウコピーを利用したデータ管理・復元ツールの提案と評価

松高直輝[1] 江口雅人[1] 岡崎拓哉[1]
松本 隆[1] 上原 哲太郎[2] 佐々木良一[1]

概要： 近年，HDD に代わり半導体を用いた記憶装置である SSD(Solid State Drive)の普及が進んでいる．SSD は Trim 機能により削除されたファイルを完全消去することでデータ処理の高速化を実現している．その反面，一度ファイルを削除してしまうと復元できないという問題を抱えている．そのため，定期的にデータのバックアップを取っておくことが求められる．本稿では，ボリュームシャドウコピーサービスを利用したバックアップを推奨している．シャドウコピーの作成やファイルの復元をおこなうツールはすでに存在するが，操作方法が複雑であり，実装している機能も不十分である．本稿は，一般ユーザが使用することを想定とした，シャドウコピー管理ツールの提案とそのツールの評価をおこなう．併せて，内部の人間による証拠隠滅の対策や，ランサムウェアを用いたシャドウコピーへの攻撃対策についても言及する．

Proposal of data management and recovery tools with ShadowCopy

NAOKI MATSUTAKA[1] MASATO EGUCHI[1] TAKUYA OKAZAKI[1]
TAKASHI MATSUMOTO[1] TETSUTAROU UEHARA[2] RYOICHI SASAKI[1]

1. はじめに

近年，HDD に代わる記憶装置として Solid State Drive（以後，SSD）の普及が進んでいる，SSD は半導体を用いた記憶装置であり，HDD のようにディスク上でヘッドを移動させる時間が必要ないため，データを高速に読み込むことができる．データ容量の増加や性能の向上が進み，SSD の普及率は今後も高まると思われる．その一方，デジタルフォレンジックやファイルの誤削除に対しての課題がある．

SSD には Trim 機能とよばれる，不要になったデータが書き込まれているセクタを検知して，空きブロックを自動的に作成する機能が備わっている．これにより SSD は，半導体の欠点である書き込み速度の低下を抑えることができる．しかし，その反面，削除したファイルを復元することができなくなるという課題を抱えている．HDD や USB メモリなど，Trim 機能が存在しない従来の環境であれば，ファイルを削除しても，その時点では実データは消去されない．しかし，Trim 機能が有効になっている場合，ファイルが削除されると，それを不要なデータと認識して，そのファイルの実データまでも完全消去してしまう．これが SSD におけるデジタルフォレンジックを困難にしている理由である．また，同様の理由で，ユーザの操作ミスによるファイルの削除についても復元することができない．

山前らは SSD における消去ファイルの復元の可能性について実験をしている [1]．その結論として，Trim 有効時では削除直後でも一切復元はできず，また，Trim 無効時であってもデータの多くは一日しか残らないという結果を示している．

ファイルの復元が不可能である以上，事前にファイルのバックアップをとっておくことが求められる．本研究では，バックアップをおこなう方法としてボリュームシャドウコピーサービスの利用を推奨する．シャドウコピーの概要とそれを利用する利点については 2 章で説明する．

シャドウコピーの作成やファイルの復元をおこなうツールはすでに存在する．しかし，これらのツールは操作方法が複雑であり，また，実装している機能も不十分である．そのため，一般ユーザにあまり使用されていない節がある．既存のツールについては 3 章でその概要を述べる．

そこで本稿は，一般ユーザが使用することを想定とした，シャドウコピーによるデータ管理・復元ツールの提案をする．また，実装した機能の使いやすさについて，テストユーザに使用してもらい評価を行った．

本研究では提案するバックアップツールのほか，内部の人間やランサムウェアによる意図的なシャドウコピーの削除を防ぎ，記録するツールの開発を視野にいれている．これらのツールを統合することで，悪意ある攻撃からシャドウコピーを安全に守り，データの復元を可能にする．統合するツールの構成については 4 章にて説明する．

2. シャドウコピーを利用したバックアップ

2.1 ボリュームシャドウコピーサービス(VSS)

ボリュームシャドウコピーサービス（以後，VSS）は，WindowsOS の機能であり，シャドウコピーとよばれるスナップショットを作成することができる．シャドウコピー（以後，SC）とは，ストレージに保存されているファイルを複

1 東京電機大学
2 立命館大学

製して，専用の領域（以後，保管領域）に保管する機能のことである．誤ってファイルを削除・上書きした場合であっても，SC を利用することで，保管されているファイルに戻すことができる．

2.2 SC の優位性

SC の作成には，ストレージの状態を記録するスナップショットが必要である．スナップショット後，ファイルが削除・変更される度にバックグラウンドで変更前のファイルを複製する．実質上，バックアップにかかる時間は，スナップショットを取るわずかな時間であるといえる．また，変更された部分のみを保存するため，バックアップに要するデータ容量を抑えることができる．例として，表 2 に 100GB のファイルでの通常コピーと SC でバックアップをおこなった際に要する時間とデータ容量を示す．

さらに，従来のバックアップでは実行中やロックされているファイルをバックアップできなかったが，SC では作成時点での状態でバックアップ処理をおこなうことができる．

表 2　100GB ファイルのバックアップ(HDD)

比較内容	通常のコピー	**SC**
バックアップ時間	777.4秒	**3.7秒**
必要なデータ容量	100GB	**55.5MB**

3. 既存のツール

3.1 SC を利用したバックアップツール

SC を利用してバックアップをおこなうツールは，複数存在する．ここでは，「復元ポイント」，「ShadowExplorer」の概要をそれぞれ 3.1.1 項，3.1.2 項で述べる．

3.1.1 復元ポイント(Windows)

Windows OS(Vista,7,10)には復元ポイントと呼ばれる機能が備わっている．復元ポイントでは，SC の作成，保管領域の設定，ファイルの復元をおこなうことができる[2]．以下，図 1 に復元ポイントを扱う 2 つの画面を示す．

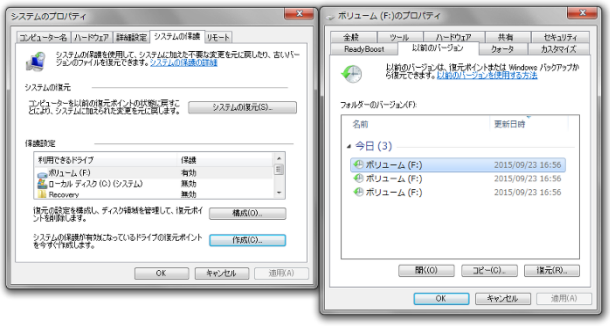

図 1　復元ポイントの画面
システムのプロパティ(左)とボリュームのプロパティ(右)

3.1.2 ShadowExplorer

ShadowExplorer とは，SC からバックアップファイルを一覧で表示し，その中から任意のファイルを復元することができるツールである[3]．以下，図 2 に ShadowExplorer の画面を示す．

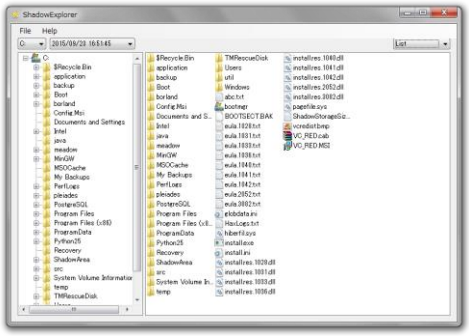

図 2　ShadowExplorer の画面

3.2 既存ツールの課題点

3.1.1 項で述べたように，復元ポイントでは SC の作成や保管領域の設定，ファイルの復元（以後，「SC 作成」，「保存設定」，「復元」）をおこなうことができるが，すべての機能を使用するためには複数の画面をひらく必要がある．具体的に述べると，SC 作成と保存設定をおこなうには「システムのプロパティ」，復元をおこなうには「ボリュームのプロパティ」からおこなう．つまり，SC に関連する機能が一元化されていないといえる．ファイルのバックアップとその復元をおこなう機能が別離していると，ユーザはこれらの操作をおこなうことが面倒になり，定期的にバックアップをせず，結果的にインシデントの対策を行わなくなると考えられる．また，復元ポイントの操作についてアンケートを行ったところ，「機能を使用するまでに時間がかかる」「操作方法がわかりづらい」という意見があり，操作面に対しても課題があると考えられる．

3.1.2 項で述べた ShadowExplorer は，ファイルの復元を目的としたツールであるため，SC 作成や保存設定をおこなうことができない．また，操作面に関しても使いづらい点がある．フォルダ遷移をする際に上の階層戻れない，ファイルが表示される一覧にファイル情報が欠如しているという欠点を持っている．これら操作面の課題が，目的のファイルを探すことを困難にしていると考えられる．

以下，表 3 に既存ツールが実装している機能を示す．丸で示されているところが実装されている機能である．

表 3　既存ツールの機能

機能	復元ポイント		Shadow Explorer
	システム	ボリューム	
SC作成	○	-	-
SC削除	○	-	-
保存設定	○	-	-
SCの一覧	-	-	○
ファイル復元	-	○	○
ファイル検索	-	○	-

表 3 から，既存ツールは各々使用できる機能が分散しており，機能を一元的に扱えないため非効率な印象を受ける．また，SC を定期的に作成する機能やファイルを検索する機能が不十分であるなど，既存ツールはバックアップをおこなうために必要な機能が欠如していると考えた．

4.　SC を安全に管理するツール「ShadowBox」の提案

4.1　提案するツールの概要

本稿が提案するツール（以後，ShadowBox）は，ユーザが SC によるバックアップ機能を容易に扱えること，SC の削除する不正なコマンドからの防御とその記録をおこなうことを目的とする．これにより，組織の内部での意図的なデータ消去，また，ランサムウェアによる SC の削除を防止することができると考えた．以下，実装する主な機能を示す．

①　SC の作成とファイルの復元をおこなう機能
②　不正な削除コマンドから SC を防御する機能
③　データ管理者に向けての情報提供

①は従来のバックアップツール同様，実装されている基本的な機能である．ShadowBox では，これらの基本機能を効率よく，容易に使用できるように，既存ツールの課題点を解消する．加えて，②，③の機能を実装することで，不正な SC 削除を防止し，安全にデータの管理をすることができる．これらの機能を一元化することで，ユーザの PC データを安全に保護することが本ツールの目的である．

4.2　提案手法

ShadowBox は，「VSSManager」，「VSSaver」，「VSSLogger」の 3 つのアプリケーションから構成される．VSSManger は，一般ユーザが容易に SC の作成やファイルの復元を行えることを目的としたツールである．VSSaver と VSSLogger は密に連携しており， SC の保管領域の防御と記録をおこなう．

ShadowBox は常駐アプリケーションとして VSSaver を起動し，SC 削除コマンドの発生を監視する．監視中に SC 削除を行おうとしたプロセスを検知した場合，それを遮断させる．またこのとき，VSSLogger を起動させ，SC が削除されようとした旨や，コマンドを起動させた実体 PE ファイルについて，管理者やフォレンジック技術者に向けて情報提供をおこなう．もし，ランサムウェアによって PC 上のファイルが暗号されている場合は，VSSManager を起動して，SC からファイルの復元をおこなう．以下，システム全体の説明として図 3 に示す．

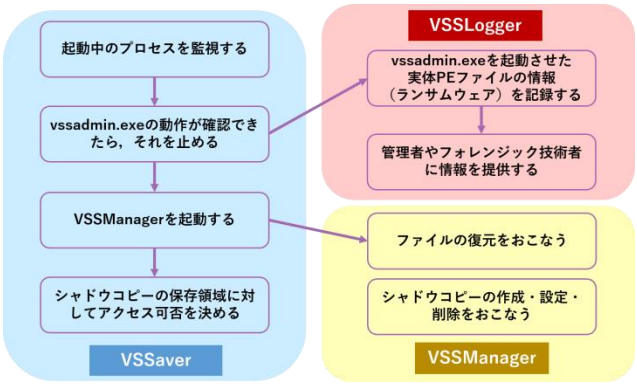

図 3　ShadowBox の全体図

この 3 つのアプリケーションは統合することでより安全にデータの管理をすることができるが，単一のアプリケーションとしても使用することができる．まず，ユーザが容易にバックアップを行えることを目的としたバックアップツール「VSSManager」の開発から説明する．

5.　一般ユーザ向けバックアップツール「VSSManager」の開発

5.1　VSSManager の概要

VSSManager は，3.2 項で述べた既存ツールの課題点を解消し，加えて，ユーザがバックアップや復元をおこなう際に求める機能を実装する．また，一般ユーザが操作することを想定した GUI を意識して開発を行った．

基本機能としては，「SC の作成」，「SC の管理」，「ファイルの復元」である．「SC の管理」は，保管領域の拡大・縮小や保管されている SC の削除をおこなうことを目的とする．基本機能を一元化することで，効率的にバックアップやファイルの復元をおこなうことができる．

5.2　課題点の解消

以下，表 4 に既存ツールの課題点と，それに対する改善方法を示す．

表 4　既存ツールの課題と改善方法

既存ツールの課題点	改善方法
SC作成やファイル復元等を一括して使用できない	5.1項で述べた基本機能を実装することで機能の一元化を図る
ボリューム単位でSC作成ができない	SCを作成する対象のボリュームを選択可能にする
単一のSCだけを対象にした検索機能	複数のSCを対象にした検索を可能にする
保存設定の操作が分かりづらいこと	直感的に操作ができるUIにする
表示されるファイル情報が充分でない	各ファイルの表示に，そのファイルであることを特定できるアイコンやサムネイルを使用する
フォルダ間の移動が面倒であること	現在のフォルダ階層の表示や「戻る」,「進む」ボタンの実装により階層の移動を簡易におこなう

表 4 に示した課題点の解消に加え，基本機能に関しても，一般ユーザが簡単にバックアップとファイル復元を行えるようなインターフェースを心掛けて開発を行った．

既存ツール「復元ポイント」の SC 作成では，自動的に作成する機能がある．しかし，自動的に作成されるタイミングについては複雑な条件があり，ユーザの意図しないタイミングで作成されてしまう可能である．そのため，VSSManager では，ユーザが自由にスケジュールの設定を行える機能を実装する．

5.3 開発環境

VSSManager は動作環境として，現時点では Windows7 のみを想定している．以下，表 5 に開発環境を示す．なお，SC 作成や SC からバックアップファイルを一覧表示する際に AlphaVSS ライブラリを使用した．[4]

表 5　開発環境

OS	Windows 7
開発言語	C#
ライブラリ	.NET Framework4.0 AlphaVSS.1.2.4000.3
ステップ数	4617

6. 製作物

VSSManager は「SC の作成」「保管設定」「ファイルの復元」「ファイルの検索」の画面から構成される．以下，図 4 ～図 7 に VSSManager の各画面を示す．

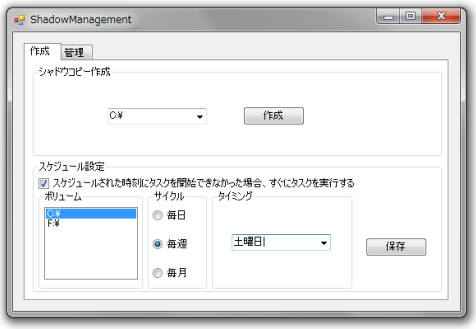

図 4　SC の作成画面

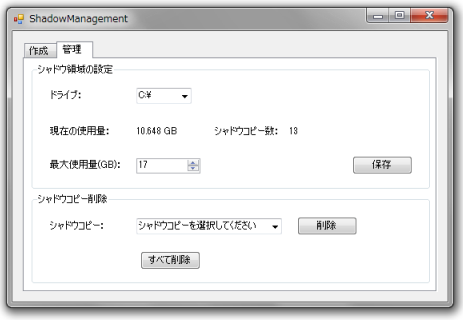

図 5　保管設定画面

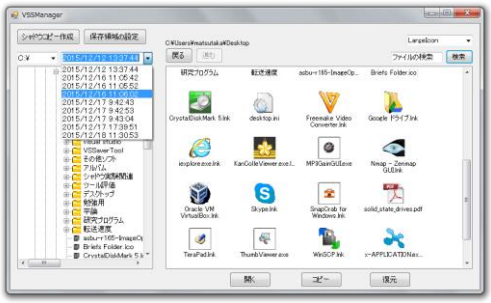

図 6　ファイルの復元画面

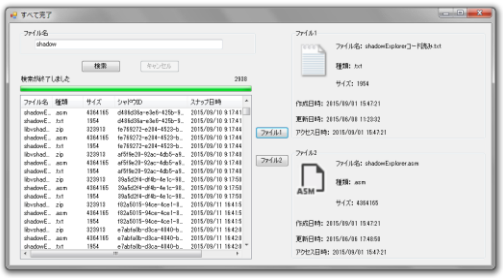

図 7　ファイルの検索画面

7. 評価

7.1 評価方法

制作したツールが一般ユーザにとって使いやすいツールであるかを確認するために評価を行った．評価の方法とし

て，テストユーザにツールを使用してもらい使いやすさの評価を取ることにする．テストユーザに既存ツールである「復元ポイント」と「ShadowExplorer」，開発した「VSSManager」を比較しながら，「SC の作成」，「保管領域の設定」，「ファイルの検索」をおこなってもらい，それぞれの操作方法に関して使いやすさを 5 段階の点数で付けてもらう．また，使用して感じたことを意見してもらう．なお，ShadowExplorer には SC 作成と保存設定を行う機能が実装されていないため，評価対象は「ファイルの検索」のみとする．また，ユーザは各ツールの操作方法を知っていることを条件にしたため，操作手順を教えながら使用してもらった．

7.2 評価結果

評価にあたり，テストユーザとして学生 10 人に協力を仰いだ．表 6 に評価結果を示す．なお，「非常に使いづらい」を「1」，「非常に使いやすい」を「5」として，その 5 段階評価の平均値を載せている．

表 6　テストユーザによる評価(5 段階平均)

機能	復元ポイント	Shadow Explorer	VSS Manager
SC作成	2.6	×	**4.7**
保存設定	1.5	×	**4.9**
ファイル検索	3.4	3.0	**3.6**

7.3 考察

表 6 より，「シャドウコピーの作成」と「保管領域の設定」に関して，既存ツールよりも「VSSManager」は高い評価を得られたことがわかる．これは操作を簡略化してユーザが直感的に操作できる GUI を実現したためだと考える．ユーザからの意見でも，「SC 作成にかかるステップ数が少ない」，「既存ツールに比べて操作方法が分かりやすい」という好評価を得られた．よって以上の 2 点に関しては，研究の目的を達成できたといえる．一方，「ファイルの検索」に関しては，ほぼポイントが変化しなかったことがわかる．その理由として，ユーザは普段 WindowsOS を使用しており，ファイル操作をエクスプローラの画面で行っているため「復元ポイント」の方が比較的容易に扱えたということである．そのため，VSSManager を初めて使うユーザには，ファイルを探す際にボタンの配置やファイルの表示の仕方に違和感を覚えたのではないかと考えた．

7.4 課題点

5.3 項より，画面レイアウトを Windows エクスプローラに近づけることが求められる，また，「ファイルの検索」についてユーザから「ファイルが探しづらい」，加えて，評価の取り方として「ファイル名を覚えていることを前提とした検索では無意味である」という意見があった．従来からの課題点が解消されなかった理由として，根本的にファイルの検索機能が使いづらいということが挙げられる．通常の検索機能は，ファイル名を入力し，それと適合するファイルを SC 全体から探し出す必要がある．それが結果的に，膨大なファイルから適合するものを探すまでに時間がかかり，使いやすさの改善には至らなかった．また，ユーザがファイル名を覚えていること前提としたため，実際のインシデントを考えたうえで，検索機能の詳細を考える必要がある．

7.5 「ファイル検索」機能の改善案

7.4 項で挙げた課題点を解消するため，ファイル検索機能を改良する．従来のファイル検索に加えて，目的のファイルが容易に見つかるように「削除されたファイル」と「更新されたファイル」というリストに絞る機能を考えている．現在，考案する 2 つの実装方法を 7.5.1 項，7.5.2 項で説明する．

7.5.1 現在のボリュームと SC を比較する手法

この手法は，現時点でボリューム内に存在するファイルと SC 内のファイルを比較して，SC 側にのみ存在するファイルを「削除されたファイル」，SC と現在のボリュームの両方で存在し，かつ，タイムスタンプが更新されているファイルを「更新されたファイル」とする．これよって，探索対象であるファイルを大幅に絞ることができるため，ユーザがファイルを探す手間も減らすことができると考える．以下，ボリュームと SC を比較する手法について説明した図 8 を示す．

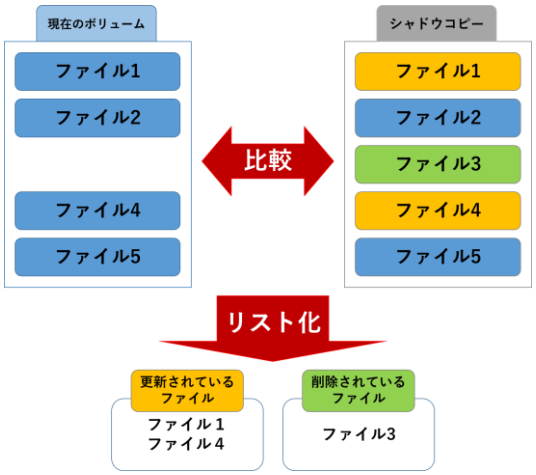

図 8　ボリュームと SC を比較する手法

7.5.2 ファイルの削除を事前に検知する手法

この手法は，ボリューム上のファイルを監視して，削除がおこなわれたときに，そのファイルのパスを取得するというものである．その後，SC からファイルを探す際にその

ファイルパスを参考にすることで，削除ファイルを探索するというものである．これにより，ユーザが目的のファイルを探す時間を短縮できると考えた．以下，削除ファイルを検知する手法について説明した図 9 を示す．

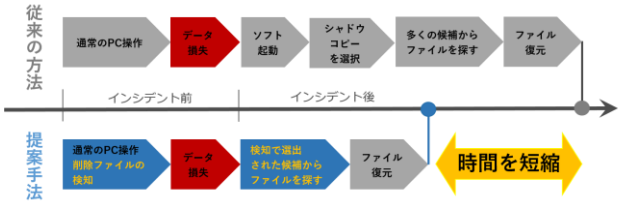

図 9　削除ファイルを検知する手法

8.　今後の展望

8.1　VSSManager の機能の改善

今後は 7.5 項で述べたように，VSSManager の改良をおこなっていく．ファイル検索機能の改善案として「ボリュームと SC を比較する手法」と「削除ファイルを検知する手法」を提案とした．これについては両手法を実装した後，ユーザに使用してもらい，より使いやすかったものを機能として採用したい．

8.2　SC 総合管理ツール「ShadowBox」の開発

本研究の目標は，SC を安全に管理するツール「ShadowBox」の開発である．本稿では，「VSSManager」の概要を主に述べた．今後は「VSSaver」，「VSSLogger」の開発を進めたい．それぞれのツールの開発手法を 8.2.1，8.2.2 項で説明する．

8.2.1 VSSaver の概要

ボリュームシャドウコピーサービスは保存領域にアクセスして SC の削除をおこなう際，Windows のユーティリティである vssadmin.exe を利用する必要がある．VSSaver は vssadmin.exe の起動を監視して，起動が検知された場合は，その起動を強制終了させる．その後，vssadmin.exe の起動があったことをユーザに知らせ，ランサムウェアによる攻撃の可能性があることを説明したアラートを出す．このとき，ランサムウェアによってファイルの暗号化がおこなわれた場合は，VSSManager を起動して SC によるファイルの復元を選択することができる．[5]

8.2.2 VSSLogger の概要

VSSLogger は「System Volume Information」フォルダ（SC が保存されているフォルダ）について監視をおこない，フォルダ内のファイルについて変更や削除がおこなわれた際に，その処理をおこなったプロセスの情報を記録し，内部不正やランサムウェアの挙動解析のために情報提供をおこなう．現時点では，管理者やフォレンジック技術者へメールによってログファイルの提供をおこなうことを考えている．[6]

9.　おわりに

SSD のデータ削除の対策として，SC を用いたバックアップを提案した．SC は従来のバックアップよりも処理時間を短縮し，容量を抑えられるというメリットがある．

既存ツールにおいて使いづらい部分を改善し，SC 作成スケジューリングの設定などの機能の追加をおこなった．その結果，SC の作成や設定の機能において，ユーザに高い評価を得ることができた．しかし，いまだにファイルを探し出す機能に課題が残っている．今回は新たなファイル検索方法について，その手法を説明するまでに留まったが，今後は実装した機能をユーザに実際に使用してもらい，より使いやすいツールになるよう改良を加えていく．

SC はユーザにあまり認知されていないという現状があるが，今後多くのユーザが，本稿が提案する「VSSManager」を利用することで，手軽に SC によるバックアップをおこなえる環境になればと思う．また引き続き，SC 総合管理ツール「ShadowBox」の開発をおこなう．このツールにより，ユーザの PC 内のデータを SC で安全に管理し，かつ悪意ある処理を記録することで，組織内部犯行の抑止やランサムウェアの解析を手助けできると考える．

参考文献

[1]　山前碧，佐々木良一：“廃棄のためのSSDデータの復元可能性の実検と評価”，卒業研究論文梗概集(2015)

[2]　Microsoft：以前のバージョンのファイル よく寄せられる質問，入手先 <http://windows.microsoft.com/ja-jp/windows/previous-versions-files-faq#1TC=windows-7>(参照2015-12-11)

[3]　ShadowExplorer.com：http://www.shadowexplorer.com/(参照2015-12-11)

[4] AlphaVSS,http://alphavss.codeplex.com/(参照2015-12-11)

[5]　岡崎拓哉，佐々木良一：“シャドウ領域における不正アクセス検知ツールの開発”東京電機大学卒業研究論文梗概集(2016)

[6]　江口雅人，佐々木良一：“シャドウコピー総合管理ツール「ShadowBox」の提案と評価”，東京電機大学修士課程学位論文・研究成果報告書予稿集(2016)