2022 年度 秋学期

卒　業　論　文

暗号化消去ツールの実装

指導教員:　上原　哲太郎

立命館大学 情報理工学部

卒業研究 3 (BA)

コース:　セキュリティネットワーク

学生証番号:　2600180210-0

氏名:　長野　和真

概要

500 字くらい

第 1 章

はじめに

近年，ハードディスクドライブ (HDD) などの記憶媒体の大容量化が進んでいる。これから，さらに記憶媒体の大容量化が進んでいくことが予想される。記憶媒体の大容量化に伴い，保存できるデータの量が増えるのは自明である。保存できるデータが増えたことにより，廃棄処理をした記憶媒体から情報流出する事故が起きた場合，1 つの記憶媒体から流出するデータの量は多くなる。そのため，廃棄した記憶媒体から情報流出が起きないために，適切な廃棄処理をすることが必要である。現在の一般的な廃棄処理としては，特定のデータパターンで上書きする廃棄処理や記憶媒体の物理的破壊による廃棄処理が行われている。しかし，記憶媒体の大容量化が進んだことにより，上書きによる消去にはさらに時間がかかるようになった。また，物理的破壊による消去を素人が行うには手間がかかる上，業者に物理的破壊を頼むと，業者が記憶媒体を盗む可能性が出てくるため，信頼できる業者でないと安全な廃棄処理とは言えない。さらに，物理的破壊による消去を行うと，記憶媒体を再利用することはできないため，コストや環境のことを考えると，とても良い消去方法とは言えない。

そこで，別の消去方法として暗号化消去というものがある。暗号化消去とは，データが記憶媒体に書き込まれる際に，データが暗号化された状態で保存されている場合に実行できる消去方法であり，データを暗号化する際に使用した暗号化キーを消去することによってデータの消去を行う。そのため，暗号化消去はデータに特定のデータパターンを上書きして消去する方法に比べて高速に消去することができる。また，部分的な領域を暗号化した暗号化キーを消去することにより，部分的な抹消，選択的な抹消を行うことができる。しかし，暗号化消去には，暗号化消去を行うためには消去するデータを暗号化しておく必要があることや，暗号化キーが格納されている場所を把握している必要があることや，暗号化消去を行うためのコマンドを使用することが難しいといった問題点がある。消去するデータを暗号化しておく必要があるという問題点の解決策として，自己暗号化ドライブ（Self Encrypting Drive）と呼ばれる，データを常に暗号化した状態で記憶する記憶媒体が存在している。暗号化キーが格納されている場所を把握している必要があるという問題点に対しては，自己暗号化ドライブの規格として，代表的なものに TCG（Trusted Computing Group）が策定している OPAL と呼ばれる規格があり，OPAL に準する自己暗号化ドライブである限り，暗号化キーは隠されている。暗号化消去を行うためのコマンドを使用することが難しいとい問題点に対しては，OPAL 規格に対応したドライブに対して，自己暗号化ドライブ特有の命令を与えることができるオープンソースである SEDutil というツールがある。しかし，SEDutil を使うためには複雑な設定が必要であり，そのうえコマンドラインによる操作で暗号化消去を行う必要があるため，誰もが簡単に行えるツールだとは言えない。

そこで本論文では，OPAL 規格で暗号化キーの管理についてどのように決められているのかを説明し，SEDutil の機能を使うことにより，自己暗号化ドライブに対して暗号化消去を簡単に実行することができるツールの実装に関し

て説明し，作成したツールを使って暗号化消去できたか検証し，その検証から得られた問題点や，これからの課題について説明する論文である。

本論文の構成は，第 2 章では研究背景について説明する。第 3 章では暗号化消去ツールを実装するまでの調査について説明する。第 4 章では暗号化消去ツールを実装する手法について説明する。第 5 章では実装したツールを使うことで暗号化消去を実行できたかの検証について説明する。第 6 章では全体を通してのまとめ，これからの課題について説明する。

第 2 章

研究背景

2.1　研究の動機

2019 年，インターネットオークションで落札されたハードディスクドライブ（HDD）から神奈川県庁の機密データが流出した事件 [1] が起こった。事件の概要を説明する。神奈川県は富士通リースとのリース契約満了に伴い，行政文書を保存していた HDD が内蔵されたサーバーを初期化したうえで返却した。富士通リースは，データ消去作業をブロードリンクに委託していた。作業を実施するブロードリンクの社員の一人が，データ消去する前の HDD を盗み，インターネットオークションで売買した。その HDD を購入したうちの一人（以下「A 氏」と表記）がデータ復元ソフトウェアを使用したところ，一部のデータが復元できた。その後，A 氏によって復元されたデータの確認をしたところ，機密データが含まれていることが判明した。また，A 氏が購入した HDD のシリアルナンバーが神奈川県が返却した HDD のシリアルナンバーと一致したことから，機密データが流出していることが発覚した。この事件に代表されるように，廃棄した HDD から情報が流出してしまうことがある。この問題を解決するには，常に HDD 内のデータを暗号化して保存しておくこと，記憶媒体を消去する際には，その記憶媒体に適した消去方法を実行することが重要である。

2.2　データ抹消ランク

データ消去技術ガイドブック [2] によると，HDD のデータ抹消ランクは Clear，Purge，Destroy の 3 段階存在する。Clear は，一般的に入手できるツールを利用した攻撃に対して耐えられるレベルの消去と定義されている。Purge は，ATA コマンドの Enhanced SECURITY ERASE UNIT を使用することや，Cryptographic Erase（暗号化消去）を行うことや，外部磁界等による消磁を行うことにより，研究所レベルの攻撃に対して耐えられる消去と定義されている。Destroy は，消磁設備や物理的破壊装置により，再使用不可能になるように破壊することで，再組立てに耐えられる消去と定義されている。

2.3　Clear レベルの消去

Clear レベルを満たす消去の方法としては，ソフトウェア製品またはハードウェア製品を使用することによって，デバイスの標準的な読み書きコマンドを使用して，ユーザがアクセス可能な領域を特定のデータパターンで上書きすることである。デバイスによって書き換えがサポートされていない場合，メーカーによる工場出荷状態に戻す機能や，

書き換えを含まない手順で消去を行う必要があるが，消去したデータの復元を容易にしない限り，Clear レベルの消去となる。

2.4 SECURITY ERASE UNIT コマンド

Purge レベルの消去方法である Enahanced SECURITY ERASE とは，Enhanced Erase モードを指定した SECURITY ERASE UNIT コマンドのことである。SECURITY ERASE UNIT コマンドには Normal Erase モードと Enhanced Erase モードがあり，Normal Erase モードを指定した場合，すべてのユーザ・データ領域に対してバイナリ・ゼロを書き込む。ここで，ユーザ・データ領域とは HPA（Host Protected Area），DCO（Device Command Overlay）を含む論理ブロックアドレスが与えられた全ての領域のことを指す。HPA とは初期状態に復帰させるリカバリ機能のための情報が記録された領域のことである。また，DCO とは容量の大きな記憶媒体を，容量の小さな PC のパーツとして使用するための意図的な容量削減を目的とした領域のことである。Enhanced Erase モードを指定した場合，すべてのユーザ・データ領域に加え，再割り当て済セクタと呼ばれる領域も設定されたデータパターンを書き込む。再割り当て済みセクタとは，工場出荷後に記憶媒体の自己判定によって不良セクタと判定され，データを他の論理ブロックアドレスに転写されたセクタのような OS が認識できない領域のことを指す。このような上書きによる消去を行う場合，上書きを何回行うことで十分な消去と言えるのかという疑問が出てくる。米国国立標準技術研究所（NIST）が発表した SP800-88 では，上書きされた部分から前に書き込まれたデータがはみ出す幅が，現在の技術では読みだし不可能なほど小さいため，「2001 年以降に生産された 15GB 以上の HDD では上書き回数は 1 回で十分である。」と記載されている。

2.5 外部磁界等による消去

HDD はヘッドと呼ばれる部品と磁性体が塗られたプラッタ（記録円盤）によって，読み書きが行われている。そのため，外部磁界等による消去では，記憶媒体を装置の磁気回路の内部に置き，誘起される磁界を記憶媒体に対して与える専用の消磁装置によって磁性体がもつ情報を消すことで行われる。しかし，外部磁界等による消去が終了したかどうかの判定を外観で行うことが難しいことや，プラッタの磁気を完全に消磁しない限り，データを読み出す技術が存在することは注意すべき点である。また，消磁装置を扱う作業員が介在してしまうので，盗まれる等の悪意による不正行為が行われる可能性が出てきてしまう。

2.6 物理的破壊による消去

NIST の SP800-88Rev.1[3] では物理的破壊について「分解、粉砕、溶融、焼却。これらのデータ抹消方法は、媒体を完全に破壊するように設計されています。これらは通常、これらの活動を効果的、安全、かつ安全に実行するための特定の機能を備えた外部委託の金属破壊施設または認可を受けた焼却施設で実施されます。」と記載されている。しかし，日本にはそのような施設は存在しないため，一般的な物理的破壊による消去としては，記憶媒体に穴をあける方法や，記憶媒体を細かく裁断することで物理的破壊による消去を行っている。物理的破壊による消去の注意点として，製品によっては製品の大きさより小さなプラッタを使用している場合があり，物理的破壊の方法として開ける穴の位置によってはプラッタに損傷を与えられない場合がある。また，外部磁界等による消去と同様に，人の手が介在してしまうので，悪意による不正行為が行われる可能性が出てきてしまう。

2.7　SSD におけるデータ抹消ランクと方式

SSD においてもデータ抹消ランクは Clear，Purge，Destroy の 3 段階存在する。Clear レベルの消去方法として，特定のデータパターンで上書きすることによる方法と，ATA コマンドの SECURITY ERASE UNIT コマンドを使用する方法がある。Purge レベルの消去方法として，ATA コマンドの BLOCK ERASE コマンドを使用する方法と，暗号化消去を行う方法がある。Destroy レベルの方法として，物理的破壊装置により，記憶媒体を粉砕破壊する方法がある。

第 3 章

暗号化消去

3.1　暗号化消去

第 1 章でも説明した通り，暗号化消去はデータを暗号化する際に使用した暗号化キーを消去することによってデータの消去を行う。暗号化消去は ATA Sanitize Device 機能セットコマンドの 1 つである CRYPTO SCRAMBLE EXT コマンドによる方法や TCG が策定している Opal Security Subsystem Class（SSC）の Revert コマンド，RevertSP コマンドまたは，Enterprise SSC の Erase コマンドを行うことで消去することができる。これらのコマンドによって暗号化消去が記憶媒体に正常に適用された後，上書きコマンドをサポートしている場合，0 または特定のデータパターンを 1 回書き込む。上書きコマンドをサポートしていない場合，SECURITY ERASE UNIT コマンド等を代替として使用することができる。

3.2　OPAL で定められた暗号鍵の管理と暗号化消去

TCG が策定している OPAL に関する文書は，TCG Storage Architecture Core Specification[4]，TCG Storage Security Subsystem Class: Opal[5]，TCG Storage Security Subsystem Class: Enterprise[6]，TCG Storage Opal SSC Feature Set: PSID[7] のようなものがある。

3.2.1　暗号鍵の管理

ユーザデータの暗号化には共通暗号鍵方式である Advanced Encryption Standard（AES）が使われる。TCG Storage Architecture Core Specification では，鍵の長さが異なる AES_128 と AES_256 の暗号鍵や AES のモードなどの情報を格納するためのテーブルが定義されている。テーブルでは UID，名前，一般名，暗号鍵，暗号モード，フィードバックサイズ，オプションのデータ，ハッシュの情報をもつように決められている。さらに TCG Storage Security Subsystem Class: Opal で，その 2 つのテーブルのうちの 1 つの暗号鍵は SecretProtect テーブルに設定する必要があると明記されている。保護のメカニズムについてはベンダーユニークとして決めることとなっている。また，SecretProtect テーブルは TCG Storage Architecture Core Specification で定義されている。このように 2 つの文書によって，ユーザデータの暗号鍵は保護されるようになっている。

3.2.2 OPAL の暗号化消去

TCG Storage Security Subsystem Class: Opal で定められているメゾットで Revert メゾットというものがある。Revert メゾットが呼び出されると，媒体を工場出荷状態に戻す。Revert メゾットの呼び出しが成功すると，工場出荷状態に戻す過程で暗号鍵を消去する。また，RevertSP メゾットというメゾットも定義されている。RevertSP メゾットは，媒体を工場出荷状態に戻すメゾットであり，Revert メゾットとの違いとして，指定された範囲の暗号鍵を消去することなく暗号化消去することができる。

また，TCG Storage Security Subsystem Class: Enterprise では Erase メゾットが定義されている。Erase メゾットは呼び出されたオブジェクトが管理する暗号鍵を消去し，新たな暗号鍵を生成する。消去したい範囲を管理するオブジェクトから Erase メゾットを呼び出すことで，特定のユーザデータを消去することができ，EraseMaster オブジェクトから呼び出すことによって，すべての範囲を暗号化消去することができる。

3.3 ATA コマンドによる暗号化消去

この研究では ATA コマンドについて調べるために, Information technology - ATA Command Set - 5（ACS-5）[8] を参照した。ACT-5 によると, ATA コマンドには Sanitize Device feature set と呼ばれる記憶媒体を消去するためのコマンドセットがある。Sanitize Device feature set は, SANITIZE STATUS EXT, CRYPTO SCRAMBLE EXT, BLOCK ERASE EXT，OVERWRITE EXT，SANITIZE FREEZE LOCK EXT，SANITIZE ANTIFREEZE LOCK EXT の 6 つのコマンドで成っている。暗号化消去を実行するためのコマンドは CRYPTO SCRAMBLE EXT である。CRYPTO SCRAMBLE EXT は，Sanitize Device feature set をサポートしているとき，CRYPTO SCRAMBLE EXT コマンドをサポートしているとき，LBA の 31:0 ビットが特定の値であるとき，記憶媒体の状態が Sanitize Idle state のような特定の状態であるとき，実行することができる。

3.4 Sedutil

Sedutil は Windows と Linux 環境で使用することができるオープンソースのツールであり，OPAL 準拠であるデバイスに命令を与えることができる。Sedutil を使うことでデバイスに様々な命令を与えることができる。例えば，query オプションを指定すると，指定した記憶媒体の Level 0 Discovery の情報を表示する。Sedtuil に scan オプションを指定すると，OS が認識している記憶媒体が接続されている場所，OPAL 準拠であるかどうか，記憶媒体の名前，ファームウェア番号を表示する。scan オプションの OPAL 準拠であるかどうかは，Level 0 Discovery の情報をもとに OPAL1.0 準拠，OPAL2.0 準拠，Enterprise SSC 準拠であるかを表示する。eraseLocckingRange オプションを指定すると，指定した記憶媒体の指定した Locking Range を消去することができる。eraseLockingRange は EraseMaster が Locking_GlobalRange に対して Erase メゾットを行っている。revertTper オプションを指定すると，指定した記憶媒体を工場出荷状態に戻すことができる。revertTper は AdminSP である SID が Revert メゾットを行っている。PSIDrevert オプションを指定すると，PSID を使って記憶媒体を工場出荷状態に戻すことができる。

第 4 章

実装

4.1　開発環境

VirtualBox-6.1.30 を使用することにより，ubuntu-20.04.3 を OS として利用し開発を行った。暗号化消去ツールの開発言語として python3.8 を利用した。python3.8 で使用したモジュールとして os，re，tkinter を使用した。

4.2　Sedutil の実行準備

Sedutil のプログラムは GitHub からダウンロードすることができる。そこで，始めに ubuntu 上で Sedutil のプログラムをダウンロードする。Sedutil のプログラムには BUILDING ファイルが含まれている。BUILDING ファイルに書かれている通りにコンパイルするために，特権モードで make，g++，autoconf automake libtool をインストールする。インストール後，BUILDING ファイル通りにコマンドを実行することで，Sedutil のプログラムがコンパイルされ，Sedutil の実行ファイルが作成される。また，Sedutil を使用するためには/sys/module/libata/parameters/allow_tpm の値を 1 にする必要がある。そこで，/etc/default/grub ファイルを書き換え，特権モードで update-grub コマンドを実行し，リブートすることで allow_tpm の値を変更する。

4.3　プログラムの自動起動

暗号化消去ツールを ubuntu でログイン後に自動起動するように設定する。bash ファイルを「自動起動するアプリケーションの設定」に登録することで自動起動を行っている。作成した bash ファイルの中身はユーザー変更後にディスプレイの制御ができるようにするコマンドと暗号化消去ツールを起動するコマンドになっている。また，Sedutil の実行には特権モードで行う必要がある。そこで doas コマンドを使用することにより，特権モードで暗号化消去ツールを起動するプログラムとなっている。

4.4　実装内容

暗号化消去ツールとして作成したファイルは複数の bash ファイルと python ファイルである。各 bash ファイルは始めに bash ファイルの引数が適当な数であるかを調べる。ここでいう適当な数とは，Sedutil にオプションを指定した際に必要な引数の数に 1 を足した数である。bash ファイルの引数が適当な数であれば，第一引数で指定された値に

カレントディレクトリを移動させる。その後，bash ファイルの名前に応じた Sedutil のオプションを指定して，bash ファイルの残りの引数を使い，Sedutil を実行するプログラムとなっている。

python ファイルは，GUI を表示し，消去する記憶媒体に応じて暗号化消去するための bash ファイルを実行するプログラムとなっている。GUI を表示させるために tkinter モジュールを使用した。記憶媒体に応じて暗号化消去するプログラムを説明する。プログラムでは始めに Sedutil の scan オプションを指定して実行している。scan オプションで得られた結果を，re モジュールの正規表現を使用することで，OS が認識している記憶媒体の情報だけを表示させている。その後，tkinter の Radiobutton を使い，ユーザーに消去したい記憶媒体を選択させる。プログラムは選択された記憶媒体が OPAL1.0 対応か OPAL2.0 対応か Enterprise SSC 対応か OPAL 準拠でないかによって暗号化消去の方法を変えている。選択された記憶媒体が OPAL1.0 対応であった場合，initialSetup オプションを指定した Sedutil を実行した後, revertTper オプションを指定した Sedutil を実行することによって, 暗号化消去を行っている。この時 initialSetup オプションを実行するためには，パスワードの入力が必要となる。ユーザーの入力が必要となるときは，実行前にユーザーにパスワードを入力してもらうように実装されている。選択された記憶媒体が OPAL2.0 対応であった場合，yesIreallywanttoERASEALLmydatausingthePSID オプションを指定した Sedutil を実行した後，initialSetup オプションを指定した Sedutil を実行し，revertTper オプションを指定した Sedutil を実行することによって，暗号化消去を行っている。yesIreallywanttoERASEALLmydatausingthePSID オプションを実行するためには，PSID の入力が必要となる。PSID は 32 桁の英数字であるため，ユーザーが 32 桁入力したときのみ暗号化消去できるように実装されている。選択された記憶媒体が Enterprise SSC 対応であった場合，eraseLockingRange オプションを指定した Sedutil を実行することによって，暗号化消去を行っている。eraseLockingRange オプションを実行するためにも，パスワードの入力が必要となる。選択された記憶媒体が OPAL 準拠でなかった場合，選択された記憶媒体はこのツールによって暗号化消去することができないことを表示させる。その後，暗号化消去を行う各 Sedutil のコマンドについて実行結果を表示し，エラー結果が返った場合，暗号化消去に失敗したことを表示させる。全てのコマンドが正常に終了した場合，暗号化消去に成功したことを表示させる。

第 5 章

検証・考察

5.1　検証方法

始めに Windows10 Home 環境で記憶媒体に対してフォーマットをする。フォーマット後，エクスプローラーを使い，容量が約 10GB のディスクイメージファイルを記憶媒体に書き込む。ディスクイメージファイルの書き込み後，開発した暗号化消去ツールを用いて記憶媒体を暗号化消去する。その後，フォレンジックツールである autopsy4.19.3 を利用することで暗号化消去できているか検証する。autopsy を使って，書き込まれたディスクイメージファイルが読み取れなかった場合，暗号化消去できたと判断する。

5.2　検証に用いた記憶媒体

検証に用いた記憶媒体を表 5.1 に示す。

5.3　検証結果

autopsy を使ってファイルを読み取った結果，検証に用いた記憶媒体の全てにおいて書き込まれたディスクイメージファイルを読み取ることはできなかった。

5.4　考察

考察

表 5.1　検証に用いた記憶媒体

デバイス名	記憶容量
KINGSTON SKC600256G	256GB
SAMSUNG SSD 870 EVO	1000GB
SAMSUNG SSD 970 EVO Plus	1000GB

第 6 章

まとめ

まとめ

謝辞

謝辞

参考文献

[1] IPA セキュリティセンター：企業の CISO 等やセキュリティ対策推進に関する実態調査-調査報告書-，独立行政法人情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000081199.pdf⟩（参照 2021-01-19）.

[1]