(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-155159
(P2006-155159A)
(43)公開日　平成18年6月15日(2006.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/06	(2006.01)	G06F	12/14	560E	5B017
H04L 9/10	(2006.01)	H04L	9/00	621A	5J104

審査請求 未請求　請求項の数 2　OL　（全 8 頁）

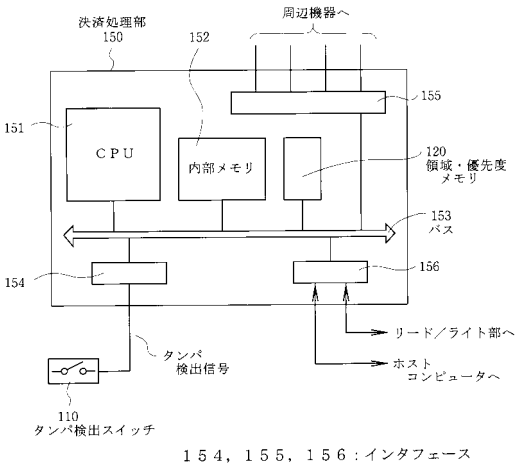
(21)出願番号　特願2004-343863 (P2004-343863)
(22)出願日　平成16年11月29日 (2004.11.29)

(71)出願人　000005234
富士電機ホールディングス株式会社
神奈川県川崎市川崎区田辺新田１番１号
(74)代理人　100091281
弁理士　森田　雄一
(72)発明者　澤田　孝雄
神奈川県横須賀市長坂二丁目２番１号　富士電機アドバンストテクノロジー株式会社内

Fターム(参考)　5B017 AA03　BA08　BB02　BB04　CA14
CA16
5J104 AA44　AA47　NA42　PA07　PA14

(54)【発明の名称】耐タンパ装置

(57)【要約】
【課題】機密情報の重要度に応じてメモリ領域に優先度を設け、タンパ検出時に、ソフトウェアにて優先度順にメモリ領域内のデータを消去することにより、低コストでセキュリティ性能を向上させた耐タンパ装置を提供する。
【解決手段】機密情報としてのデータに対する不正アクセスを検出するタンパ検出スイッチ１１０と、内部メモリ１５２におけるデータの記憶領域を、データの機密性、重要性に応じた消去優先度と共に定義し記憶した領域・優先度メモリ１２０と、不正アクセス検出時に、前記消去優先度に従って内部メモリ１５２のデータを消去するＣＰＵ１５１とを備える。内部メモリ１５２は、暗号キーの記憶領域と、この暗号キーを用いて暗号化されたデータの記憶領域とを有し、領域・優先度メモリ１２０は、内部メモリ１５２内の暗号キーの記憶領域を消去優先度が最も高い記憶領域として記憶する。
【選択図】図３



１５４，１５５，１５６：インタフェース

【特許請求の範囲】
【請求項１】
機密情報としてのデータが機密情報記憶手段に格納された電子機器において、
前記データに対する不正アクセスを検出するタンパ検出手段と、
前記機密情報記憶手段におけるデータの記憶領域を、データの機密性、重要性に応じた消去優先度と共に定義し記憶してなる領域・優先度定義記憶手段と、
前記タンパ検出手段による不正アクセス検出時に、前記消去優先度に従って前記記憶領域のデータを消去する消去手段と、
を備えたことを特徴とする耐タンパ装置。
【請求項２】
請求項１に記載した耐タンパ装置において、
前記機密情報記憶手段は暗号キーの記憶領域を有し、かつ、この暗号キーを用いて暗号化されたデータの記憶領域を有すると共に、
前記領域・優先度定義記憶手段は、前記暗号キーの記憶領域を、消去優先度が最も高い記憶領域として記憶してなることを特徴とする耐タンパ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部からの不正アクセスを防止してメモリ内の機密情報を保護するために各種電子機器に適用される耐タンパ装置に関するものである。
【背景技術】
【０００２】
近年、ＩＣカード型電子マネーやネットワーク型電子マネーを利用した電子決済システムが徐々に普及してきている。
これらの電子決済システムでは、電子マネー機能を有するＩＣカードや、携帯電話、ＰＤＡ（Personal Digital Assistants）、決済端末、チャージ端末等の各種端末機器に、データの暗号化／復号化に使用する暗号キー情報、ＩＤ、パスワード等の認証情報、氏名、電話番号等の個人情報、電子マネーの金額等の電子価値情報といった各種の機密情報が格納されている。このため、第三者による不正アクセスによってこれらの機密情報の読み出し、解析、改ざん等を防ぐための機能、いわゆる耐タンパ機能が必要不可欠である。
【０００３】
この耐タンパ機能を実現する従来技術としては、下記の特許文献１に記載されたものが知られている。
特許文献１に記載された耐タンパ装置及び方法は、端末機器等の筐体の開放により不正行為を検出する耐タンパスイッチ等の不正行為認識手段と、不正行為を認識した際にＲＡＭ等の記憶手段への電源供給を遮断して記憶内容を破壊する電源制御手段とを備えている。また、回路電源のオフ時に不正行為認識手段が動作すると記憶手段への電源供給を遮断し、回路電源のオン時に不正行為認識手段が動作すると、ＣＰＵに割り込みをかけてプログラムにより記憶内容を消去する手段を備えている。
この従来技術は、回路電源の有無に関係なく機密情報が不正にアクセスされるのを防ぐ方式であり、不正アクセス検出時に記憶手段への電源供給を遮断してデータを破壊したり、あるいは、割り込み処理によってデータを消去することにより、機密情報の保護を行っている。
【０００４】
【特許文献１】特開２００３－３３７７５３号公報（請求項１，２，５，６、段落［００２６］～［００３３］，［００５８］～［００７５］、図１，図２，図９～図１２等）
【発明の開示】
【発明が解決しようとする課題】
【０００５】
上記の従来技術には以下のような問題があった。

まず、不正アクセス時に記憶手段への電源供給を遮断する回路が必要であり、この回路は半導体スイッチ素子を用いた電子スイッチ等により構成されているため、製造コストが高くなる。

また、近年では、電子機器のメモリ容量の増加に伴って機密情報のデータ量も増加の一途を辿っている。言い換えれば、不正アクセス時にソフトウェアによってこれらのデータを消去する場合には、その消去動作に長時間を要することになり、その間に未消去のデータが読み出されて解析されるおそれがある。

従って、従来では、耐タンパ装置やこれを内蔵した電子機器の製造コストが高くなったり、セキュリティが万全ではない等の問題を有していた。

【０００６】

そこで本発明の解決課題は、機密情報の重要度に応じてメモリ領域に消去優先度を設け、タンパ（不正アクセス）検出時に、ソフトウェアにて消去優先度順に当該メモリ領域内のデータを消去することで、製造コストを抑えると共にセキュリティを向上させた耐タンパ装置を提供することにある。

【課題を解決するための手段】

【０００７】

上記課題を解決するため、請求項１に記載した発明は、機密情報としてのデータが機密情報記憶手段に格納された電子機器において、

前記データに対する不正アクセスを検出するタンパ検出手段と、

前記機密情報記憶手段におけるデータの記憶領域を、データの機密性、重要性に応じた消去優先度と共に定義し記憶してなる領域・優先度定義記憶手段と、

前記タンパ検出手段による不正アクセス検出時に、前記消去優先度に従って前記記憶領域のデータを消去する消去手段と、を備えたものである。

【０００８】

請求項２に記載した発明は、請求項１に記載した耐タンパ装置において、

前記機密情報記憶手段は暗号キーの記憶領域を有し、かつ、この暗号キーを用いて暗号化されたデータの記憶領域を有すると共に、

前記領域・優先度定義記憶手段は、前記暗号キーの記憶領域を、消去優先度が最も高い記憶領域として記憶してなるものである。

【発明の効果】

【０００９】

本発明においては、機密情報の機密性や重要性に応じてメモリ領域の消去優先度を予め定義しておき、不正アクセスの検出時には、ソフトウェアにより前記消去優先度に従って順に機密情報を消去していく。これにより、機密性、重要性の高いデータを優先的に保護することができ、また、暗号キーを組み合わせることで、データの解析、改ざんが困難なセキュリティシステムを構築することができる。

更に、タンパ検出時に電源供給を遮断する従来技術に比べてハードウェアの追加も少なくて済み、低コスト化を図れるという利点がある。

加えて、暗号キーの記憶領域を最優先に消去することで実質的に他のデータの解析等が困難または不可能になるので、最短の場合には暗号キーの記憶領域を消去する時間だけあれば機密情報の保護が一応可能であり、消去時間の長期化を回避することができる。

【発明を実施するための最良の形態】

【００１０】

以下、図に沿って本発明の実施形態を説明する。

まず、図１は本実施形態にかかる耐タンパ装置の機能ブロック図である。なお、この実施形態の耐タンパ装置は、決済端末、チャージ端末、携帯電話、ＰＤＡ等の各種端末機器や、ＩＣカードに内蔵されるものであり、以下では、これらの各種端末機器やＩＣカードを便宜的に電子機器と総称する。

【００１１】

図１において、１１は、電子機器内の内部メモリ（主メモリ）に格納されたデータ（機

密情報）に対する不正アクセスを検出するためのタンパ検出手段、１２は、前記データの機密性、重要性に応じて、データを消去するべきメモリ領域を優先度（消去優先度）順に定義して記憶した消去メモリ領域・優先度定義記憶手段、１３は、タンパ検出手段１１によるタンパ検出信号をトリガとして、内部メモリのデータ消去を実行するメモリ領域消去手段である。

ここで、不正アクセスとは、電子機器の筐体の破壊、正規の手順以外の手順による分解、あるいは、データが格納された内部メモリの取り外し、外部からのスキミング等による機密情報への各種アクセスを意味し、前記タンパ検出手段１１は、これらの不正アクセス行為を物理的、電気的な手段によって検出可能となっている。

【００１２】

次に、図２及び図３は、本実施形態の耐タンパ装置を含む電子機器のハードウェア構成を示す図であり、例えば電子マネー用の決済端末に耐タンパ装置を内蔵した場合のものである。

図２において、１１０は図１におけるタンパ検出手段１１としてのタンパ検出スイッチ、１５０はＣＰＵを備えた決済処理部、２１０はキーボード、２２０はディスプレイ、２３０はプリンタ、２４０はハードディスク等の補助記憶装置、２５０はリード／ライト（読み出し／書き込み）部である。

【００１３】

決済処理部１５０は、通信回線を介してホストコンピュータ（図示せず）に接続されている。また、リード／ライト部２５０は、例えば電子マネー機能を有するＩＣカードとの間で情報を送受信可能なカードリーダ／ライタや、非接触の無線通信により情報を送受信する送受信部等を含む。

なお、図２におけるタンパ検出スイッチ１１０以外の構成は、従来の決済端末が有するハードウェアであり、キーボード２１０、ディスプレイ２２０等の周辺機器は、端末の機能、性質（決済端末、チャージ端末等）に応じて適宜、選択的に接続される。

【００１４】

図３は、図２における決済処理部１５０の構成図である。

この決済処理部１５０は、通常のコンピュータシステムと同様に、ＣＰＵ１５１、内部メモリ１５２、バス１５３を備え、また、図２に示したキーボード２１０、ディスプレイ２２０等の周辺機器が接続されるインタフェース１５５と、リード／ライト部２５０やホストコンピュータが接続されるインタフェース１５６とを備えている。

【００１５】

決済処理部１５０による決済処理は、周知のように、内部メモリ１５２に格納されたプログラム及びデータを用い、更には、必要に応じて図２の補助記憶装置２４０内のデータを用いて、ＣＰＵ１５１が暗号キー情報や認証情報、個人情報の照合、認証を行い、また、電子価値情報の更新（利用者の有する電子マネーの減額及び売上げの計上）を行うと共に、これらの処理結果や前記各種情報をホストコンピュータとの間で送受信して実行されるものである。

【００１６】

上記内部メモリ１５２は、いわゆる主メモリやキャッシュメモリを纏めて表したものであり、フラッシュＲＯＭ（フラッシュメモリ）、ＥＥＰＲＯＭ（電気的に消去可能なプログラマブルＲＯＭ）等のＲＯＭ、ＳＲＡＭ（スタティックＲＡＭ）、ＤＲＡＭ（ダイナミックＲＡＭ）等のＲＡＭによって構成されている。

不正アクセスから保護するべきデータは、主として上記内部メモリ１５２に格納されているが、補助記憶装置２４０に記憶されていても良い。

【００１７】

また、図３において、１２０は図１の消去メモリ領域・優先度定義記憶手段１２としての領域・優先度メモリであり、このメモリ１２０には、不正アクセスから保護するべきデータの機密性、重要性に応じて、これらのデータが格納された内部メモリ１５２（または補助記憶装置２４０）内のメモリ領域が優先度順に定義して記憶されている。

更に、タンパ検出スイッチ１１０は、インタフェース１５４を介してバス１５３に接続されている。

なお、以下において、機密情報であるデータは内部メモリ１５２に記憶されており、領域・優先度メモリ１２０には、内部メモリ１５２のメモリ領域が消去優先度順に記憶されているものとして説明する。

【００１８】

図３のＣＰＵ１５１は、図１におけるメモリ領域消去手段１３に相当しており、タンパ検出スイッチ１１０からタンパ検出信号が入力されると、これをトリガとして、消去プログラムを実行し、前記領域・優先度メモリ１２０から読み出したメモリ領域及びその優先度に従って内部メモリ１５２内のメモリ領域を順番に選択してそのデータを消去するものである。

ここで、前記消去プログラムは、内部メモリ１５２以外のメモリや領域・優先度メモリ１２０に常駐させておけばよい。

【００１９】

図４は、図３における領域・優先度メモリ１２０に予め記憶された情報、すなわち、内部メモリ１５２内の、データを消去するべきメモリ領域を優先度と共に定義した情報を示している。

この情報は、消去メモリ領域定義数１２１（その定義数をＮとする）と、Ｎ個分の消去メモリ領域定義情報１２２とから構成されており、消去メモリ領域定義情報１２２には、内部メモリ１５２内のデータの機密性、重要性に応じて、各データが格納されているＮ個のメモリ領域に関する情報が優先度と共に定義されている。図示例では、消去メモリ領域定義情報１に格納されているデータが最高の優先度を持ち、消去メモリ領域定義情報Ｎに格納されているデータが最低の優先度を持っている。

【００２０】

各々の消去メモリ領域定義情報１２２は、内部メモリ１５２のメモリ領域のアドレス１２２ａ、サイズ１２２ｂ、メモリ種別１２２ｃ、及びクリアデータ１２２ｄからなっている。ここで、アドレス１２２ｂは消去するメモリ領域の先頭アドレスであり、サイズ１２２ｂは当該領域に格納されたデータのサイズである。メモリ種別１２２ｃは、例えばＳＲＡＭ、フラッシュＲＯＭ、ＥＥＰＲＯＭ等の種別であり、クリアデータ１２２ｄは消去する際にメモリ領域に書き込むデータである。

ＣＰＵ１５１は、上記の定義情報に基づいてタンパ検出時のデータ消去処理を行う。

【００２１】

図５は、上述した消去メモリ領域の定義例である。

この例では、消去メモリ領域の定義数が５であり、優先度が最高（優先度１）のデータを暗号キーとしてそのメモリ領域を定義情報１とし、以下、優先度に応じて、電子価値情報のメモリ領域を定義情報２、認証情報のメモリ領域を定義情報３、個人情報のメモリ領域を定義情報４、決済処理に必要なプログラムのメモリ領域を定義情報５に設定している。

ＣＰＵ１５１は、消去プログラムにより、上記優先度順に各メモリ領域のデータを消去するように動作する。

【００２２】

また、内部メモリ１５２においては、上記定義情報１のメモリ領域内の暗号キーを用いて、定義情報２～５の各メモリ領域のデータが暗号化されたうえ記憶されている。

なお、各定義情報１～５によって定義されるメモリ領域のアドレスは必ずしも連続している必要はなく、ランダムであっても良い。これにより、複数種類の機密情報をそれぞれの優先度にかかわらず分散させてメモリ領域に格納することも可能である。

【００２３】

次いで、図６はタンパ検出時のメモリ領域の消去処理を示すフローチャートである。

外部からの不正アクセスが発生し、タンパ検出スイッチ１１０からタンパ検出信号が出力されると、ＣＰＵ１５１により消去プログラムが呼び出され、以下に述べるデータ消去

処理が開始される。

【００２４】

まず、領域・優先度メモリ１２０から図４の消去メモリ領域定義数１２１を読み込む（ステップＳ１）。次に、消去メモリ領域定義情報１２２を読み込み（Ｓ２）、消去するべきメモリ領域の開始アドレス及びサイズをセットする（Ｓ３）。

そして、このメモリ領域のメモリ種別を判定し（Ｓ４）、当該メモリ領域が揮発性メモリ（例えばＳＲＡＭ）領域であれば、予め指定されたクリアデータによりメモリ領域をクリア、すなわちデータを消去する（Ｓ５）。また、当該メモリ領域が不揮発性メモリ（例えばフラッシュＲＯＭ、ＥＥＰＲＯＭ）であれば、各メモリ種別毎に指定されているクリアシーケンスに従って、当該メモリ領域のデータを消去する（Ｓ６）。

その後、消去メモリ領域定義数分だけ消去したか否かを判定し（Ｓ７）、定義数に達するまでステップＳ２～Ｓ７の処理を繰り返し実行する。

【００２５】

以上の処理を行うことにより、例えば、図５に例示したごとく暗号キーのメモリ領域を定義情報１（優先度１）に割り付けてその他のメモリ領域を定義情報２～５に順次割り付けると共に、上記暗号キーを用いて定義情報２～５の各メモリ領域のデータを暗号化しておけば、タンパ検出時に一番優先度の高いメモリ領域の暗号キーが最初に消去されるため、その後、仮に優先度２以下の領域でデータを不正に読み出されたとしても、暗号キーは不明であるからこれらのデータの解析や改ざんが困難になり、データを保護することができる。

このため、定義情報２以下のメモリ領域を消去するために長時間を要する場合であっても、少なくとも定義情報１の暗号キーを最優先で消去することにより、必要最低限のセキュリティ性能を確保することが可能である。

【図面の簡単な説明】

【００２６】

【図１】本発明の実施形態を示す機能ブロック図である。

【図２】図１に示した機能ブロックを含む決済端末のハードウェアの構成例である。

【図３】図２における決済処理部の構成図である。

【図４】図３における領域・優先度メモリの記憶情報の説明図である。

【図５】図４に対応する消去メモリ領域の定義例を示す図である。

【図６】本発明の実施形態におけるメモリ領域の消去処理を示すフローチャートである。

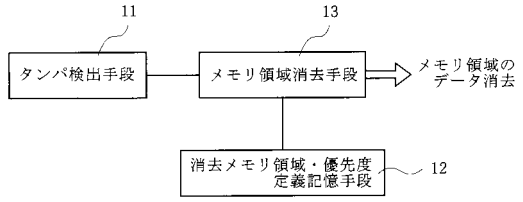
【符号の説明】

【００２７】

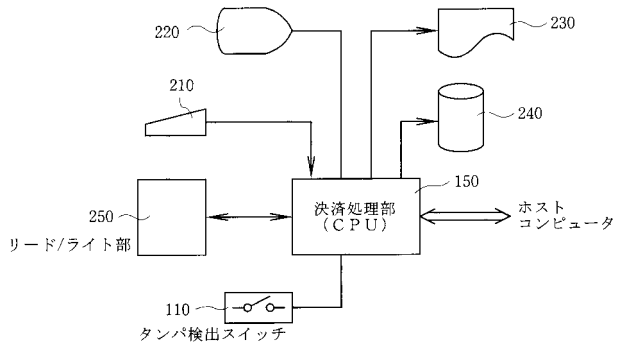
１１：タンパ検出手段
１２：消去メモリ領域・優先度定義記憶手段
１３：メモリ領域消去手段
１１０：タンパ検出スイッチ
１２０：領域・優先度メモリ
１２１：消去メモリ領域定義数
１２２：消去メモリ領域定義情報
１２２ａ：アドレス
１２２ｂ：サイズ
１２２ｃ：メモリ種別
１２２ｄ：クリアデータ
１５０：決済処理部
１５１：ＣＰＵ
１５２：内部メモリ
１５３：バス
１５４，１５５，１５６：インタフェース
２１０：キーボード

２２０：ディスプレイ
２３０：プリンタ
２４０：補助記憶装置
２５０：リード／ライト部

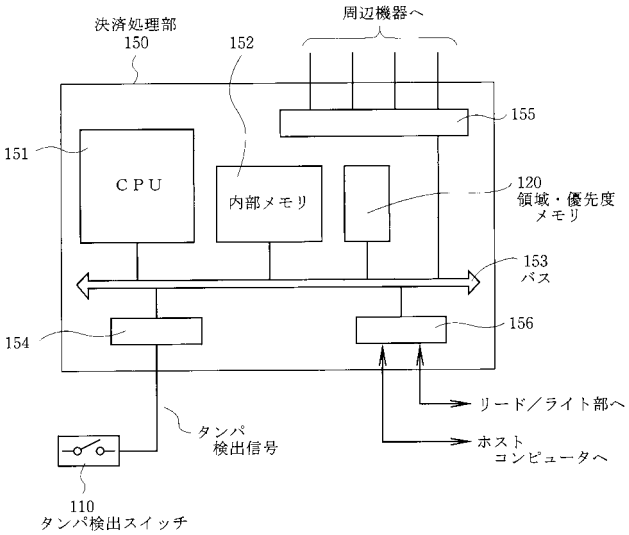
【図１】



【図２】

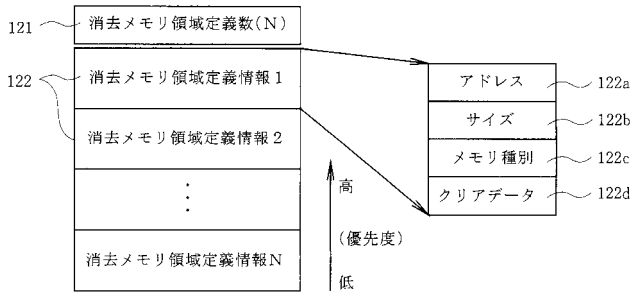


【図３】

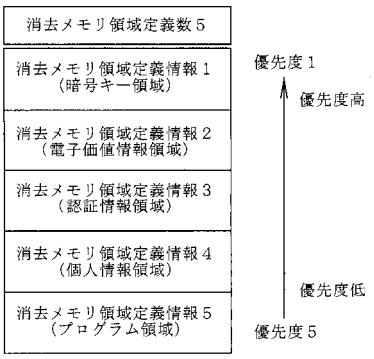


１５４，１５５，１５６：インタフェース

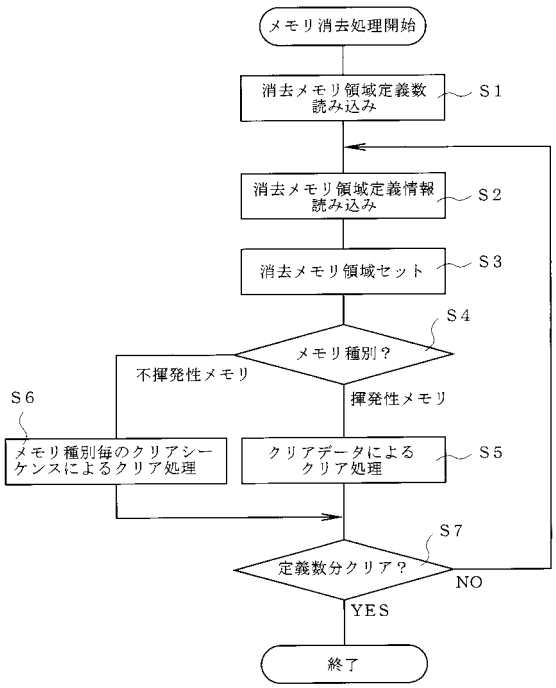
【図４】


121
消去メモリ領域定義数(N)
122
消去メモリ領域定義情報１
消去メモリ領域定義情報２
消去メモリ領域定義情報N
アドレス
122a
サイズ
122b
メモリ種別
122c
クリアデータ
122d
高
(優先度)
低

【図５】


消去メモリ領域定義数５
消去メモリ領域定義情報１
(暗号キー領域)
消去メモリ領域定義情報２
(電子価値情報領域)
消去メモリ領域定義情報３
(認証情報領域)
消去メモリ領域定義情報４
(個人情報領域)
消去メモリ領域定義情報５
(プログラム領域)
優先度１
優先度高
優先度低
優先度５

【図６】


メモリ消去処理開始
消去メモリ領域定義数
読み込み
S１
消去メモリ領域定義情報
読み込み
S２
消去メモリ領域セット
S３
S４
メモリ種別？
不揮発性メモリ
揮発性メモリ
S６
メモリ種別毎のクリアシーケンスによるクリア処理
クリアデータによるクリア処理
S５
S７
定義数分クリア？
NO
YES
終了