(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4462849号
(P4462849)

(45)発行日　平成22年5月12日(2010.5.12)　(24)登録日　平成22年2月26日(2010.2.26)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560A
G06F 3/06	(2006.01)	G06F	3/06	304K
G06F 12/00	(2006.01)	G06F	12/00	537Z

請求項の数 5　(全 17 頁)

(21)出願番号　特願2003-154870 (P2003-154870)
(22)出願日　平成15年5月30日 (2003.5.30)
(65)公開番号　特開2004-355498 (P2004-355498A)
(43)公開日　平成16年12月16日 (2004.12.16)
審査請求日　平成18年1月17日 (2006.1.17)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(74)代理人　100084032
弁理士　三品　岩男
(72)発明者　下岡　健一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　淺野　正靖
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】データの保護装置、方法およびプログラム

(57)【特許請求の範囲】

【請求項１】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に記憶されているデータの複製を記憶する、複数の複製記憶領域と、前記記憶領域に対してデータの読込みまたは書込みを行う計算機と、を有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

前記記憶領域と前記計算機とは、前記記憶領域と前記計算機との通信を制御するインタフェース部を介して接続されており、

前記データ保護装置は、前記記憶領域と、複数の前記複製記憶領域と、前記インタフェース部と、に接続され、

前記データ保護装置が、

前記計算機システムへの不正アクセス及び前記計算機システムのコンピュータウイルスを検出するイベント検出部と、

前記イベント検出部が不正アクセス及びコンピュータウイルスのうち少なくとも一方を検出すると、前記計算機と前記記憶領域との通信の停止を前記インタフェース部に指示し、さらに、前記複数の複製記憶領域の全てに対するデータ複製の中断を、前記記憶領域又は前記複数の複製記憶領域に指示するパス切断部とを有すること

を特徴とするデータ保護装置。

【請求項２】

請求項１記載のデータ保護装置であって、

前記複製記憶領域の各々は、ある前記複製記憶領域が、前記記憶領域に記憶されたデータを自身に複製し、他の前記複製記憶領域は、当該複製処理から所定時間経過後に、前記記憶領域に記憶されたデータを自身に複製すること
を特徴とするデータ保護装置。
【請求項３】
請求項２記載のデータ保護装置であって、
前記計算機システムは、前記複製記憶領域毎に、当該複製記憶領域に記憶されているデータの複製を記憶する複数のサブ複製記憶領域をさらに有し、
前記複数のサブ複製記憶領域の各々は、ある前記サブ複製記憶領域が、データ複製の対象とする前記複製記憶領域（以下、対象複製記憶領域）に記憶されたデータを自身に複製し、前記対象複製記憶領域をデータ複製の対象とする他の前記サブ複製記憶領域は、当該複製処理から所定時間経過後に、前記対象複製記憶領域に記憶されたデータを自身に複製すること
を特徴とするデータ保護装置。
【請求項４】
データを記憶するために割り当てられる記憶領域と、前記記憶領域に記憶されているデータの複製を記憶する、複数の複製記憶領域と、前記記憶領域に対してデータの読込みまたは書込みを行う計算機と、を有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置によるデータ保護方法であって、
前記記憶領域と前記計算機とは、前記記憶領域と前記計算機との通信を制御するインタフェース部を介して接続されており、
前記データ保護装置は、前記記憶領域と、複数の前記複製記憶領域と、前記インタフェース部と、に接続され、
演算装置と、記憶装置と、入出力装置と、を有する前記データ保護装置が、
前記計算機システムへの不正アクセス及び前記計算機システムのコンピュータウイルスを検出するステップと、
不正アクセス及びコンピュータウイルスのうち少なくとも一方を検出すると、前記計算機と前記記憶領域との通信の停止を前記インタフェース部に指示し、さらに、前記複数の複製記憶領域の全てに対するデータ複製の中断を、前記記憶領域又は前記複数の複製記憶領域に指示するステップと、を実行すること
を特徴とするデータ保護方法。
【請求項５】
データを記憶するために割り当てられる記憶領域と、前記記憶領域に記憶されているデータの複製を記憶する、複数の複製記憶領域と、前記記憶領域に対してデータの読込みまたは書込みを行う計算機と、を有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置によるデータ保護プログラムであって、
前記記憶領域と前記計算機とは、前記記憶領域と前記計算機との通信を制御するインタフェース部を介して接続されており、
前記データ保護装置は、前記記憶領域と、複数の前記複製記憶領域と、前記インタフェース部と、に接続され、
演算装置と、記憶装置と、入出力装置と、を有する前記データ保護装置に、
前記計算機システムへの不正アクセス及び前記計算機システムのコンピュータウイルスを検出するステップと、
不正アクセス及びコンピュータウイルスのうち少なくとも一方を検出すると、前記計算機と前記記憶領域との通信の停止を前記インタフェース部に指示し、さらに、前記複数の複製記憶領域の全てに対するデータ複製の中断を、前記記憶領域又は前記複数の複製記憶領域に指示するステップと、を実行させること
を特徴とするデータ保護プログラム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
本発明は、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護する技術に関する。
【０００２】
【従来の技術】
近年、コンピュータネットワークの普及に伴い、計算機システムを利用した電子商取引などのサービス事業が活発に行なわれるようになっている。一方で、計算機システムに対する不正侵入、コンピュータウィルス等（以下、これらを総称して「不正行為」とする）によるデータ破壊、データ漏洩、データ改竄などの被害が深刻な問題となっている。これらの不正行為によるデータ破壊等は、計算機システムが保持する取引情報などを失わせ、莫大な損失を発生させるおそれがある。これにより、当該計算機システムの運営企業に対する信頼も失墜させかねない。また、破壊等されたデータを復旧するためには、一般に、相当の費用と時間とが必要となる。このため、計算機システムにおいて、不正行為からデータを保護することは、極めて重要である。
【０００３】
不正行為への対策としては、まず第１に防止が挙げられる。従来から、計算機システムと外部ネットワークとの間におけるファイアウォールの構築、ワンタイムパスワードなどによるユーザ認証、ユーザ毎にアクセス可能なファイル・プログラムを定義するＡＣＬ（Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｌｉｓｔ）の設定等により、計算機システムへの不正行為を阻止することが行なわれてきた。しかし、不正行為の手法は日々進化、多様化しており、完全に防止することは事実上不可能に近い。
【０００４】
そこで、防止できずに侵入された場合に備えて、監視および事後対応が重要となる。従来から知られている代表的な監視手段としては、不正侵入に対する侵入検知システム（ＩＤＳ：Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）、コンピュータウィルスに対するウィルス検知ソフトウェアが挙げられる。
【０００５】
侵入検知システムは、例えば、ログファイルのモニタやポートスキャンの解析を行なって不正侵入等を監視する。そして、不正侵入等を検知した場合には、侵入者とのセッションを切断したり、侵入された計算機システムと外部ネットワークとの間にあるフロントエンドのスイッチを操作して侵入元とのパスを切断したりする。また、ウィルス検知ソフトウェアは、例えば、ファイルの内容とコンピュータウィルスのコードパターンとのマッチングを行なうことによりコンピュータウィルスの検査を行なう。そして、コンピュータウィルスを検知した場合には、感染したファイルを削除したり、ウィルスパターンを消去したりする。これらの技術の詳細については、例えば、非特許文献１に記載されている。
【０００６】
【非特許文献１】
財団法人マルチメディア振興センターネットワーク管理部会、“初心者でも分かるネットワーク管理入門”、６．３．３．侵入検知システム、[online]、平成１４年５月１５日、［平成１４年１２月１９日検索］、インターネット＜ＵＲＬ：http://www.fmmc.or.jp/~fm/nwmg/manage/main.html＞
【０００７】
【発明が解決しようとする課題】
一般に、侵入検知システムは、不正侵入が行なわれてから不正侵入を検出するまでに、ある程度の時間を必要とする。侵入者はこの時間を利用し、侵入先の計算機システムにトロイの木馬を仕掛けたり、再侵入のためのバックドア（裏口）を設けたりすることがある。ここでトロイの木馬とは、無害だと思って実行すると破壊活動を起こしたり、コンピュータウィルスを感染させたりする偽装したプログラムである。
【０００８】
この場合、上述のセッションの切断あるいはフロントエンドのパス切断では、計算機シス

テム内のデータを十分には保護できない。なぜなら、正規ユーザがトロイの木馬をそれと知らず起動してしまったり、侵入者がバックドアから侵入検知システムをすり抜け、再侵入できてしまう可能性があるからである。

【０００９】

また、他のファイルやプログラムに次々と感染していく自己増殖型のコンピュータウィルスに感染した場合には、ウィルス検知ソフトウェアがコンピュータウィルスを検出し削除したとしても、他のファイル等を検査するまでに感染が広がってしまう可能性がある。

【００１０】

そこで、本発明は、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護することを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成するため、データを記憶するために割り当てられる記憶領域と、前記記憶領域に記憶されているデータの複製を記憶する、複数の複製記憶領域と、前記記憶領域に対してデータの読込みまたは書込みを行う計算機と、を有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、前記記憶領域が、前記複数の複製記憶領域の各々と接続されており、前記記憶領域と前記計算機とは、前記記憶領域と前記計算機との通信を制御するインタフェース部を介して接続されており、前記データ保護装置は、前記記憶領域と、複数の前記複製記憶領域と、前記インタフェース部と、に接続され、前記データ保護装置が、前記計算機システムへの不正アクセス及び前記計算機システムのコンピュータウイルスを検出するイベント検出部と、前記イベント検出部が不正アクセス及びコンピュータウイルスのうち少なくとも一方を検出すると、前記計算機と前記記憶領域との通信の停止を前記インタフェース部に指示し、さらに、前記複数の複製記憶領域の全てに対するデータ複製の中断を、前記記憶領域又は前記複数の複製記憶領域に指示するパス切断部とを有することを特徴とする。

【００１３】

本態様によれば、不正行為を検出した際、不正行為を受けた計算機とその記憶領域の間のバックエンドのパスを切断することにより、データを保護することができる。

【００１５】

記憶制御装置は、前記記憶領域への書込みデータを、一定時間遅らせて、前記複製領域へ転送したり、複製領域を複数設けて、記憶領域への書込みデータを転送する対象を、一定時間毎に、前記複数の複製領域間で切り替えることができる。

【００１６】

本態様によれば、さらに、不正行為が行なわれる前のデータの複製を確保することができる。

【００１７】

【発明の実施の形態】

＜第１の実施形態＞

図１は第１の実施形態のシステム構成を示したブロック図である。

【００１８】

第１の実施形態のシステムは、フロントエンドのスイッチ３０と、ホスト４０と、バックエンドのスイッチ５０と、記憶装置６０と、データ保護装置７０とを有し、ネットワーク２０に接続している。

【００１９】

尚、データ保護装置７０は、本実施形態並びに他の実施形態においても１個の独立した装置として記載しているが、ホスト４０内部に設けてもよいし、スイッチ３０内部に組み込んでもよい。また、スイッチ５０も、本実施形態並びに他の実施形態においても１個の独立した装置として記載しているが、ホスト４０内部に設けてもよいし、記憶装置６０内部に設けてもよい。また、記憶装置６０も、本実施形態並びに他の実施形態においても１個の独立した装置として記載しているが、ホスト４０内部に設けてもよい。更に、ホスト４

０とデータ保護装置７０との関係は、図１並びに他の図においても１対１の関係で記載しているが、多対１であってもよい。また、ホスト４０と記憶装置６０との関係も、図１において１対１で記載しているが、１対多、多対１、あるいは、多対多であってもよい。

【００２０】

ネットワーク２０に接続した計算機１０は、ホスト４０が提供するサービスを利用するための端末として用いられる。しかし、クラッカーが計算機１０を用いてホスト４０に対する不正行為を行うこともあり得る。計算機１０としては、例えばＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）や携帯情報端末などがある。尚、計算機１０は、図１並びに他の図においても１台しか記載していないが、複数台存在していてもよい。

【００２１】

ネットワーク２０は、例えば、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）を用いたＩｎｔｅｒｎｅｔ、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、あるいは、ＦＣ（Ｆｉｂｒｅ Ｃｈａｎｎｅｌ）を用いたＳＡＮ（Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）等で構成することができる。

【００２２】

フロントエンドのスイッチ３０は、ネットワーク２０とホスト４０との接続を制御する。尚、本実施形態並びに他の実施形態においても、スイッチ３０が存在せず、ネットワーク２０とホスト４０とが直結していてもよい。

【００２３】

ホスト４０は、スイッチ３０、ネットワーク２０を介して計算機１０に電子商取引や動画像ストリーミングなどのサービスを提供する。ただし、ホスト４０は、サービス提供用ホストには限られず、例えば、外部にサービスを行なわない内部データ管理用ホストであってもよい。ホスト４０は、フロントエンドのスイッチ３０とのインタフェースであるポート４１と、不正アクセスを検出するための侵入検知プログラム４３およびコンピュータウィルスを検出するためのウィルス検知ソフトウェア４４を格納した記憶領域４２と、メモリ４５と、プロセッサ４６と、バックエンドのスイッチ５０とのインタフェースであるポート４７と、データ保護装置７０とのインタフェースであるポート４８とを備えて構成される。

【００２４】

なお、侵入検知プログラム４３、ウィルス検知ソフトウェア４４等は、本実施形態並びに他の実施形態においてもホスト４０が備える記憶領域４２に格納されているよう記載しているが、記憶装置６０、データ保護装置７０、他の計算機内の記憶領域、あるいは記憶媒体に格納されていてもよい。これらの場合、ホスト４０は記憶領域４２を省いて構成してもよい。また、侵入検知プログラム４３およびウィルス検知ソフトウェア４４は双方存在することが好ましいが、いずれか一方のみであってもよい。また、ポート４１、４７は、図１並びに他の図においてもそれぞれ１個ずつ記載しているが、それぞれ複数存在していてもよい。

【００２５】

記憶装置６０は、保護すべきデータを格納する記憶領域６４を備えた記憶装置である。記憶領域６４には、例えば、計算機１０に提供するサービスを実行するためのプログラム、その他のデータを格納する。また、記憶装置６０は、データをやり取りするスイッチ５０とのインタフェースであるポート６１と、構成情報の取得や設定を行うインタフェースであるＳＶＰ（Ｓｅｒｖｉｃｅ Ｐｒｏｃｅｓｓｏｒ）６２と、ＳＶＰ６２で設定された構成情報に基づいてポート６１と記憶領域６４との接続を制御するコントローラ６３とを備えている。尚、ポート６１および記憶領域６４は、図１では１個ずつ記載しているが、それぞれ複数個存在してもよい。

【００２６】

データ保護装置７０は、本発明の特徴的な装置であり、ホスト４０とのインタフェースであるポート７１と、記憶領域７２と、メモリ７５と、プロセッサ７６とを備えている。記憶領域７２は、後述する侵入検知部４３ｘおよびウィルス検知部４４ｘの不正行為検出結

果を受信するための不正行為受信プログラム７３とホスト４０とホスト４０が利用している記憶領域６４とのパスを切断する処理を行なうためのデータ保護プログラム７４とを格納している。なお、不正行為受信プログラム７３およびデータ保護プログラム７４は、他の計算機や記憶装置あるいは記憶媒体に格納されていてもよい。この場合、記憶領域７２は省くことができる。なお、データ保護装置７０は、専用装置として構成するほか、ＰＣ等の一般的な情報処理装置等で構成することができる。

【００２７】

次に、本実施形態のシステムにおける動作を説明する。

【００２８】

ホスト４０は、提供するサービスのプログラムをメモリ４５にロードし、プロセッサ４６により実行する。前記プログラムは、計算機１０からの要求によって、または定期的に、または、あるイベントの発生を契機として、ポート４７、バックエンドのスイッチ５０、記憶装置６０のポート６１、コントローラ６３を介し、記憶領域６４のデータを読み書きし、ポート４１、フロントエンドのスイッチ３０、ネットワーク２０を介し、計算機１０にサービスを提供する。

【００２９】

同時に、侵入検知プログラム４３、ウィルス検知ソフトウェア４４も、メモリ４５にロードされ、プロセッサ４６により実行される。これにより、ホスト４０に侵入検知部４３ｘ、ウィルス検知部４４ｘ（いずれも図示せず）が仮想的に構成され、これらが不正行為等がホスト４０に対して行われていないかを監視する。尚、侵入検知プログラム４３、ウィルス検知ソフトウェア４４は、データ保護装置７０あるいはその他の計算機内のメモリにロードされ、ネットワーク経由でホスト４０を監視するようにしてもよい。

【００３０】

また、データ保護装置７０における不正行為受信プログラム７３も、メモリ７５にロードされ、プロセッサ７６により実行される。これにより、データ保護装置７０に不正行為受信部７３ｘ（図示せず）が仮想的に構成され、不正行為検出の通知を待ち受ける。なお、不正行為受信部７３ｘは、侵入検知部４３ｘあるいはウィルス検知部４４ｘが不正行為を検出したかどうかを能動的に監視するようにしてもよい。この場合、データ保護装置７０自身のセキュリティのため、データ保護装置７０から他装置へのアクセスは許可するが、ホスト４０などの他装置からデータ保護装置７０へのアクセスは許可しないよう設定することが好ましい。

【００３１】

図２は、本実施形態のシステムにおいてホスト４０が不正行為を受けてから記憶領域６４のデータを保護するまでの流れを示すシーケンス図である。

【００３２】

クラッカー（侵入者）が計算機１０を用いてホスト４０に不正侵入したり、コンピュータウィルスを送り込んだとする（Ｓ１０１）。

【００３３】

侵入検知部４３ｘがホスト４０に対する不正侵入を検出する（Ｓ１０３）と、不正行為受信部７３ｘにポート４８、７１を介して通知する（Ｓ１０４）。また同様に、ウィルス検知部４４ｘがコンピュータウィルスを検出すると、ポート４８、７１を介して不正行為受信部７３ｘに通知する。

【００３４】

不正行為受信部７３ｘは、ホスト４０に対する不正行為の検出を受信すると、データ保護プログラム７４をメモリ７５にロードし、プロセッサ７６に実行させる（Ｓ１０５）。これにより、データ保護装置７０に、データ保護部７４ｘ（図示せず）が仮想的に構成される。尚、データ保護プログラム７４は、あらかじめメモリ７５にロードしておいてもよい。

【００３５】

データ保護部７４ｘは、ホスト４０と記憶領域６４との間のバックエンドのパスを切断す

るような構成変更を、ポート７１を介して、スイッチ５０あるいはＳＶＰ６２に対して命令する（Ｓ１０６）。

【００３６】

これにより、侵入検知部４３ｘが不正侵入を検出する前に、トロイの木馬が記憶領域６４等に仕込まれた場合であっても、ホスト４０と記憶領域６４との間のバックエンドのパスが切断されるため、トロイの木馬が記憶領域６４のデータ改竄を試みても（Ｓ１０７）、ホスト４０から記憶領域６４へアクセスすることができず失敗する（Ｓ１０８）。

【００３７】

このように本実施形態によれば、不正侵入の事後的に引き起こされる可能性があるデータ破壊等を防止することができる。

【００３８】

また、侵入検知部４３ｘが不正侵入を検出する前に、侵入者が再侵入のためのバックドアを仕掛けたとしても、再侵入の際には、ホスト４０と記憶領域６４との間のバックエンドのパスが切断されているため、やはり記憶領域６４のデータにアクセスすることはできない。

【００３９】

記憶領域６４に自己増殖型コンピュータウィルスが仕掛けられた場合には、ウィルス検知部４４ｘがコンピュータウィルスを検出した時点には、別ファイルに感染している可能性がある。しかし、データ保護プログラム７４がホスト４０と記憶領域６４との間のパスを切断するため、前記感染ファイルがメモリ４５にロードされ実行される（発病する）ことがない。すなわち、更なる感染（破壊）から記憶領域６４のデータを保護することができる。

【００４０】

次に、Ｓ１０６におけるバックエンドのパスを切断する方法について説明する。本発明はバックエンドのパスを切断する方法については限定しないが、例えば、スイッチ５０のゾーニングを利用する方法、記憶装置６０のパス構成管理を利用する方法、記憶装置６０のＡＣＬを利用する方法がある。データ保護部７４ｘはこれらのいずれか１つを実行してもよいし、複数を組み合わせて実行してもよい。

【００４１】

まず、スイッチ５０のゾーニングを利用する方法を説明する。ゾーニングとは、スイッチにおいて特定のポート間でのみ通信を許す機能である。例えば、ゾーンをポートａ、ｂ、ｃで構成すると、スイッチは、ポートｂがポートａ、ｃとは通信できるが、ポートｄとは通信できないように制御する。

【００４２】

図３は、本実施形態におけるスイッチ５０が保持するゾーニングテーブル１００の一例を示す図である。

【００４３】

ゾーンＩＤ１０１は、スイッチ５０内でゾーンを一意に識別する値である。尚、図３ではゾーンＩＤ１０１を数字で記載しているが、文字列であってもよい。

【００４４】

ポートＩＤリスト１０２は、ゾーンを構成する各ポートのポートＩＤのリストである。前記ポートＩＤはポートを一意に識別するための値である。ポートＩＤとしては、例えばポート名称やWWN（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）などがある。

【００４５】

データ保護部７４ｘは、ポート７１を介し、スイッチ５０に対してゾーニングテーブル１００の全ポートＩＤリスト１０２からポート４７を削除するよう命令する。ここでポートＩＤリスト１０２の構成ポートが１個になった場合は、当該ゾーン全体を削除してもよい。

【００４６】

例えばポート４７をポートａとすると、図３の例では、データ保護部７４ｘにより、ゾー

ンＩＤ１がポートｂ、ｃでのみ構成されるようになる。
【００４７】
この結果ポート４７はどの記憶装置６０にもアクセスできなくなり、ゆえに記憶領域６４内のデータを保護できる。
【００４８】
つぎに、バックエンドのパスを切断する方法として、記憶装置６０のパス構成管理を利用する方法を説明する。
【００４９】
パス構成管理とは、ホスト側から見た記憶領域のＩＤと記憶装置内部での記憶領域のＩＤの対応付けを管理する機能である。前記対応付けがなされていない記憶領域へはホストからアクセスできない。
【００５０】
図４は、本実施形態におけるコントローラ６３が保持するパス構成テーブル１１０の一例を示す図である。
【００５１】
内部ポートＩＤ１１１は記憶装置６０内のポート６１を一意に識別するためのＩＤである。ホストＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）１１２は、ホスト４０側から見た記憶領域６４のＩＤである。内部ＬＵＮ１１３は、記憶装置６０内において記憶領域６４を一意に識別するＩＤである。
【００５２】
図４の例では、ホスト４０がポートＡを介して１番の記憶領域にアクセスを試みると、内部ＬＵＮが１５６である記憶領域６４にアクセスすることになる。
【００５３】
尚、ホストＬＵＮ１１２、内部ＬＵＮ１１３は、図４ではそれぞれ数字で記載しているが、文字列であってもよい。
【００５４】
データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、パス構成テーブル１１０からホスト４０が利用する記憶領域６４に該当する項目を削除するよう命令する。ここで、該当する項目を判別するために、侵入検知部４３ｘまたはウィルス検知部４４ｘは不正行為の検出を不正行為受信部７３ｘに通知する際に、ホスト４０が利用しているポート６１の内部ポートＩＤ１１１と記憶領域６４のホストＬＵＮ１１２の情報を同時に送信する。データ保護部７４ｘは不正行為受信部７３ｘから前記情報を受け取り、パス構成テーブル１１０から前記情報に該当する項目を削除するようコントローラ６３に要求する。尚、ホスト４０が利用する記憶領域６４が運用時に不変であるならば、本実施形態におけるシステムの管理者が予めデータ保護部７４ｘに対してホスト４０と記憶領域６４の内部ＬＵＮ１１３の情報を与えておいてもよい。前記情報の設定は、データ保護装置７０が有するキーボードやマウスなどの入力装置を用い、データ保護部７４ｘが提供するＵＩ（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）を通じて実行する。この場合、不正行為受信部７３ｘがホスト４０に対する不正行為検出を受信すると、データ保護部７４ｘは前記情報を用い、パス構成テーブル１１０から前記記憶領域６４の内部ＬＵＮ１１３に該当する項目をすべて削除するようコントローラ６３に要求する。
【００５５】
例えばホスト４０が利用する記憶領域６４の内部ＬＵＮ１１３を１５６とすると、図４の例では、データ保護部７４ｘにより第１行と第４行の項目が削除される。
【００５６】
この結果、記憶領域６４はどのホスト４０からもアクセスされなくなる。これにより、記憶領域６４内のデータは保護される。
【００５７】
つぎに、バックエンドのパスを切断する方法として、記憶装置６０のＡＣＬを利用する方法を説明する。

【００５８】
記憶装置のＡＣＬとは、各記憶領域に対して特定のホスト側のポートからしかアクセスを受け付けない機能である。
【００５９】
図５は、本実施形態におけるコントローラ６３が保持するＡＣＬテーブル１２０の一例を示す図である。
【００６０】
内部ポートＩＤ１２１は記憶装置６０内のポート６１を一意に識別するためのＩＤである。ホストＬＵＮ１２２は、ホスト４０側から見た記憶領域６４のＩＤである。尚、ホストＬＵＮの代わりに、記憶装置６０内において記憶領域６４を一意に識別するＩＤである内部ＬＵＮを用いてもよい。ホストポートＩＤリスト１２３は、内部ポートＩＤ１２１とホストＬＵＮ１２２で表されるパスを利用できるポート４７のポートＩＤのリストである。即ち、図４、５の例の場合、ホスト側のポートａ、ｂ、ｃは記憶装置側のポートＡを介して内部ＬＵＮが１５６である記憶領域６４にアクセスできるが、ポートｄ、ｅはアクセスできない。
【００６１】
データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対してＡＣＬテーブル１２０内のすべてのホストポートＩＤリスト１２３からポート４７を削除するよう命令する。ここでホストポートＩＤリスト１２３の構成ポートがなくなった場合、その項目自身を削除してもよい。
【００６２】
例えば、ポート４７をポートａとすると、図５の例では、データ保護部７４ｘにより第１行と第２行とからポートａが削除される。
【００６３】
この結果ポート４７はどの記憶領域６４にもアクセスできなくなる。これにより記憶領域６４内のデータを保護できる。
【００６４】
「スイッチ５０のゾーニングを利用する方法」と「記憶装置６０のＡＣＬを利用する方法」とは同等の効果があるが、「記憶装置６０のパス構成管理を利用する方法」は少し効果が異なる。前者の２方法は不正行為を受けたホスト４０からのみ記憶領域６４へアクセスできなくなるのに対し、後者の方法はすべてのホストから記憶領域６４へアクセスできなくなる。すなわち、前者の方法を用いると、不正行為を受けていないホストは継続して記憶領域６４へアクセスでき、サービスを提供し続けられる。よって、データ保護部７４ｘは、記憶領域６４を複数のホストで共有している場合であって、記憶領域６４のデータを改竄されていたりコンピュータウィルスが侵入していないことが明らかな場合には前者の方法を採用し、そうでない場合は後者の方法を採用することが好ましい。
【００６５】
以上のように、本実施形態では侵入検知部４３ｘまたはウィルス検知部４４ｘが不正行為を検出すると、データ保護部７４ｘがホスト４０と記憶領域６４との間のバックエンドのパスを切断する。これにより、侵入検知部４３ｘあるいはウィルス検知部４４ｘが不正行為を検出する前に、トロイの木馬あるいはバックドアを仕掛けられたり、コンピュータウィルスに感染したとしても、記憶領域６４のデータを保護できる。ホスト４０からデータを取得しようとしても記憶領域６４へアクセスできないし、逆に記憶領域６４に存在するコンピュータウィルスが、メモリ４５にロードされプロセッサ４６により実行されることがないためである。
＜第２の実施形態＞
図６は、第２の実施形態のシステム構成を示したブロック図である。
【００６６】
第２の実施形態のシステムは、フロントエンドのスイッチ３０と、ホスト４０と、バックエンドのスイッチ５０と、記憶装置６０ａ、６０ｂと、データ保護装置７０とを有し、ネ

ットワーク２０に接続している。また、ネットワークには計算機１０が接続している。
【００６７】
計算機１０と、ネットワーク２０と、フロントエンドのスイッチ３０と、ホスト４０と、バックエンドのスイッチ５０とは、第１の実施形態と構成、機能とも同様とすることができる。
【００６８】
記憶装置６０ａは、第１の実施形態の記憶装置６０に加え、記憶装置６０ｂとのインタフェースであるポート６５ａと、記憶領域６４から複製領域６７へのデータ反映を一定時間遅らせる転送遅延部６６とを更に有する。
【００６９】
記憶装置６０ｂは、第１の実施形態の記憶装置６０に加え、記憶装置６０ａとのインタフェースであるポート６５ｂと、記憶領域６４の複製データを保持する記憶領域である複製領域６７とを更に有する。
【００７０】
尚、転送遅延部６６は、本実施形態ではコントローラ６３ａ内に実現されているよう記載しているが、コントローラ６３ｂ内に設けてもよいし、ポート６５ａと６５ｂとの間に独立した装置として設けてもよい。また、本実施形態では記憶装置６０ａ、６０ｂはそれぞれ独立した装置として記載しているが、単一の記憶装置であってもよい。即ち、記憶領域６４と複製領域６７が同一記憶装置内に存在してもよい。更に、本実施形態では複製領域６７は１個しか記載していないが、複数個存在してもよい。また、ポート６５ａ、６５ｂも、本実施形態では１個ずつしか記載していないが、それぞれ複数存在してもよい。
【００７１】
データ保護装置７０の構成は、第１の実施形態と同様である。しかし、プロセッサ７６がデータ保護プログラム７４を実行することにより仮想的に構成されるデータ保護部７４ｘは、第１の実施形態における機能に加え、記憶領域６４から複製領域６７へのデータ反映を停止させる機能を更に保持する。
【００７２】
本実施形態のシステムにおける動作は、基本的には第１の実施形態と同様である。しかし、記憶領域６４の複製データを保持する複製領域６７を予め設定し、更に転送遅延部６６に記憶領域６４から複製領域６７へのデータ反映をΔＴ時間だけ遅らせるよう設定しておく点が、第１の実施形態とは異なる。これにより、通常運用時において複製領域６７は常に記憶領域６４のΔＴ時間前のデータを保持する。
【００７３】
次に、本実施形態のシステムにおいてホスト４０が不正行為を受けてから記憶領域６４のデータを保護するまでの流れを説明する。データ保護部７４ｘがホスト４０と記憶領域６４との間のバックエンドのパスを切断するような構成変更をスイッチ５０あるいはＳＶＰ６２ａに対して命令するまでは、第１の実施形態と同様である。本実施形態ではこれに加え更に、データ保護部７４ｘは、ポート７１を介し、さらに、ＳＶＰ６２ａまたはＳＶＰ６２ｂを介し、コントローラ６３ａまたはコントローラ６３ｂに対し、記憶領域６４と複製領域６７との間の複製関係（データ反映）を解消あるいは一時停止するよう命令する。
【００７４】
これにより、本実施形態では、第１の実施形態に加え更に、ホスト４０に対する不正行為を検出した時刻よりΔＴ時間前に記憶領域６４が保持していたデータを複製領域６７に確保できる。
【００７５】
なお、ホスト４０に対する不正行為を検出した時刻よりΔＴ時間前に記憶領域６４が保持していたデータを確保するという目的においては、記憶領域６４と複製領域６７との間の複製関係（データ反映）を解消あるいは一時停止すれば足り、ホスト４０と記憶領域６４との間のバックエンドのパスは、必ずしも切断しなくてもよい。
【００７６】

ここで、侵入検知部４３ｘおよびウィルス検知部４４ｘが、不正行為がなされてから、最悪でもＴ１時間未満には不正行為を検出可能であるとすると、ΔＴ≧Ｔ１を満たすようにΔＴを設定することにより、複製領域６７に不正行為がなされる前のデータが格納されていることが保証される。このため、仮に記憶領域６４のデータが被害を受けたとしても、複製領域６７に格納したデータを用いることで、システムの早期復旧を図ることができる。

＜第３の実施形態＞

図７は、第３の実施形態のシステム構成を示したブロック図である。

【００７７】

第３の実施形態のシステムは、フロントエンドのスイッチ３０と、ホスト４０と、バックエンドのスイッチ５０と、記憶装置６０と、データ保護装置７０とを有し、ネットワーク２０に接続している。また、ネットワークには計算機１０が接続している。

【００７８】

計算機１０と、ネットワーク２０と、フロントエンドのスイッチ３０と、ホスト４０と、バックエンドのスイッチ５０とは、第２の実施形態と構成、機能とも同様とすることができる。

【００７９】

記憶装置６０は、第１の実施形態に加え、記憶領域６４の複製データを保持する記憶領域である複製領域６７ａ～６７ｃを更に有する。尚、本実施形態では複製領域６７ａ～６７ｃを記憶領域６４と同一の記憶装置６０内部に設けるよう記載しているが、第２の実施形態と同様に異なる記憶装置に設けてもよい。また、複製領域は、本実施形態では３個記載しているが、複数であればいくつ存在してもよい。

【００８０】

データ保護装置７０の構成は、第２の実施形態と同様である。しかし、プロセッサ７６がデータ保護プログラム７４を実行することにより仮想的に構成されるデータ保護部７４ｘは、第２の実施形態における機能に加え、記憶領域６４のデータを反映させる複製領域６７ａ～６７ｃをΔＴ’時間毎に順次切り替える機能を保持する。

【００８１】

本実施形態のシステムにおける動作は、基本的には第１の実施形態と同様である。しかし、記憶領域６４の複製データを保持する複製領域６７ａ～６７ｃを予め設定しておく点が第１の実施形態とは異なる。また、データ保護部７４ｘが、ΔＴ’時間毎にポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４のデータを反映させる複製領域を切り替えるよう命令する点も異なる。

【００８２】

図８は、本実施形態において記憶領域６４のデータを反映させる複製領域６７ａ～６７ｃを切り替える流れを示したシーケンス図である。

【００８３】

データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４のデータを複製領域６７ａに反映させるように命令する（Ｓ２０１）。次に、ΔＴ’時間経過後（Ｓ２０２）、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４と複製領域６７ａとの間の複製関係を一時停止させ、記憶領域６４のデータを複製領域６７ｂに反映させるように命令する（Ｓ２０３）。更に、ΔＴ’時間経過後（Ｓ２０４）、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４と複製領域６７ｂとの間の複製関係を一時停止させ、記憶領域６４のデータを複製領域６７ｃに反映させるように命令する（Ｓ２０５）。

【００８４】

そして、更に、ΔＴ’時間経過後（Ｓ２０６）、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４と複製領域６７ｃとの間の複製関係を一時停止させ（Ｓ２０７）、記憶領域６４のデータを複製領域６７ａに反映させ

るように命令する（Ｓ２０１）。これらの処理を繰り返すことにより、データ保護部７４ｘは、記憶領域６４のデータを反映させる複製領域６７ａ～６７ｃを、ΔＴ’時間毎に切り替える。なお、ΔＴ’時間毎に記憶領域６４のデータを反映させる複製領域を切り替える処理は、コントローラ６３が行なうようにしてもよい。

【００８５】

以上により、通常運用時において複製領域６７ａ～６７ｃは、それぞれΔＴ’時間ずつずれた記憶領域６４のスナップショットを保持する。

【００８６】

なお、記憶装置の中には、記憶領域６４のデータを直接反映できる複製領域の数を制限し、前記各複製領域のデータを更に別の複数の複製領域に反映（多段接続）することにより、記憶領域６４の複製を数多く保持できるものがある。

【００８７】

図９は、多段接続した場合の記憶領域と複製領域との関係の一例を示した図である。

【００８８】

複製領域６７Ａは記憶領域６４の複製先であるとともに、複製領域６７Ａａ、６７Ａｂの複製元である。同様に、複製領域６７Ｂは記憶領域６４の複製先であるとともに、複製領域６７Ｂａ、６７Ｂｂの複製元である。

【００８９】

このような記憶装置に対しては、データ保護部７４ｘは、例えば、まず、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、記憶領域６４のデータを複製領域６７Ａに反映させ、複製領域６７Ａのデータを複製領域６７Ａａに反映させるよう命令する。次に、ΔＴ’時間経過後、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、複製領域６７Ａと複製領域６７Ａａとの間の複製関係を一時停止させ、複製領域６７Ａのデータを複製領域６７Ａｂに反映させるよう命令する。更に、ΔＴ’時間経過後、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、複製領域６７Ａと複製領域６７Ａｂ、及び記憶領域６４と複製領域６７Ａとの間の複製関係を一時停止させ、記憶領域６４のデータを複製領域６７Ｂに反映させ、複製領域６７Ｂのデータを複製領域６７Ｂｂに反映させるよう命令する。更に、ΔＴ’時間経過後、データ保護部７４ｘは、ポート７１、ＳＶＰ６２を介し、コントローラ６３に対して、複製領域６７Ｂと複製領域６７Ｂａとの間の複製関係を一時停止させ、複製領域６７Ｂのデータを複製領域６７Ｂｂに反映させるよう命令する。これを繰り返すことにより、データ保護部７４ｘは、別の複製領域に対する複製元でない末端の複製領域６７Ａａ、６７Ａｂ、６７Ｂａ、６７Ｂｂに対し、記憶領域６４のΔＴ’時間毎のスナップショットを保持させることができる。

【００９０】

本実施形態のシステムにおいてホスト４０が不正行為を受けてから記憶領域６４のデータを保護するまでの流れは第２の実施形態と同様である。ただし、すべての複製領域６７との間の複製関係を停止させる。

【００９１】

以上より、本実施形態には第１の実施形態に加え更に、Ｎ個の複製領域に記憶領域６４のΔＴ’時間毎のスナップショットを保持する効果がある。図７の例ではＮは３としている。

【００９２】

なお、ホスト４０に対する不正行為がなされる前のデータを確保するという目的においては、記憶領域６４とすべての複製領域６７との間の複製関係（データ反映）を解消あるいは一時停止すれば足り、ホスト４０と記憶領域６４との間のバックエンドのパスは、必ずしも切断しなくてもよい。

【００９３】

ここで、侵入検知部４３ｘおよびウィルス検知部４４ｘが、不正行為がなされてから、最悪でもＴ１時間未満には不正行為を検出可能であるとすると、ΔＴ’≧Ｔ１／（Ｎ－２）

を満たすようにΔＴ’を設定することにより、少なくとも１個の複製領域６７には不正行為がなされる前のデータが格納されていることが保証される。なぜなら、記憶領域６４のデータを反映させる複製領域を切り替えた直後に不正行為が検出されるという最悪のケースであっても、Ｎ個の複製領域６７のそれぞれには、記憶領域６４の０時間前（現在の複製対象）、０時間前（直前の複製対象）、ΔＴ’時間前、…、（Ｎ－２）ΔＴ’時間前のデータが保持されているからである。すなわち、ΔＴ’≧Ｔ１／（Ｎ－２）であれば、（Ｎ－２）ΔＴ’時間前のデータは、Ｔ１時間前のデータより以前のものであり、不正行為が行われたのはＴ１時間前より以降である。このため、Ｎ個の複製領域６７のうち１個は記憶領域６４の（Ｎ－２）ΔＴ’時間前の、不正行為が行われる以前のデータを保持していることになる。これにより、仮に記憶領域６４のデータが被害を受けたとしても、いずれかの複製領域６７に格納したデータを用いることで、システムの早期復旧を図ることができる。

【００９４】

また、不正行為検出後にログファイルの解析などを行うことによって、記憶領域６４のデータが破壊され始めた時刻、あるいは不正行為が開始された時刻が具体的に判明することがある。本実施形態では、前記時刻より以前のうちの最新であるＴ１／（Ｎ－２）時間前のデータを確保可能である。この点において、少なくともＴ１時間分のデータロスが発生する第２の実施形態に比して有利である。

【００９５】

さらに、本実施形態においてログデータを記憶領域６４に格納するようにすると、不正行為の検出にも役立つ。クラッカー（侵入者）は不正アクセスの痕跡を消すためにログを改竄することがある。本実施形態ではログデータのΔＴ’時間毎のスナップショットを複製領域６７に保持できる。例えば、ログ改竄検出プログラムをデータ保護装置７０、ホスト４０、他の計算機、またはコントローラ６３等に格納し、このプログラムを実行することにより各複製領域に格納されたログデータを比較することによりログの改竄を検出するログ改竄検出部を仮想的に構成することで、ホスト４０に対する不正行為の監視を行なうことができる。すなわち、ログ改竄検出部がログの改竄を検出すると、不正行為受信プログラム７３に通知するようにすれば、ホスト４０が使用する記憶領域のデータを保護できる。また、複製領域に格納されたログデータのスナップショットを解析することで、再侵入を企てようとするクラッカーを特定したり、待ち受け等の対策を行なうことが可能となる。

【００９６】

【発明の効果】

上述のように、本発明によれば、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護することができる。

【図面の簡単な説明】

【図１】第１の実施形態のシステム構成を示すブロック図である。

【図２】第１の実施形態における、不正行為がホスト４０になされてから記憶領域６４のデータを保護するまでの処理の流れを表すシーケンス図である。

【図３】第１の実施形態におけるスイッチ５０が保持するゾーニングテーブル１００の一例を表す図である。

【図４】第１の実施形態におけるコントローラ６３が保持するパス構成テーブル１１０の一例を表す図である。

【図５】第１の実施形態におけるコントローラ６３が保持するＡＣＬテーブル１２０の一例を表す図である。

【図６】第２の実施形態におけるシステム構成を示すブロック図である。

【図７】第３の実施形態におけるシステム構成を示すブロック図である。

【図８】第３の実施形態における、記憶領域６４の複製対象となる複製領域６７ａ～６７ｃを切り替える処理の流れを表すシーケンス図である。

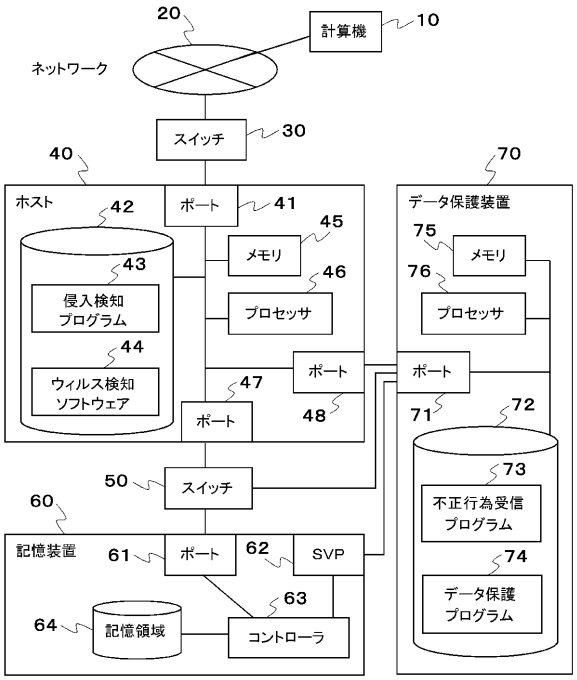
【図９】第３の実施形態における複製領域の多段接続の一例を表す図である。

【符号の説明】

１０…計算機、２０…ネットワーク、３０…（フロントエンド）スイッチ、４０…ホスト、４３…侵入検知プログラム、４４…ウィルス検知ソフトウェア、５０…（バックエンド）スイッチ、６０…記憶装置、６２…ＳＶＰ、６３…コントローラ、６４…記憶領域、６６…転送遅延部、６７…複製領域、７０…データ保護装置、７３…不正行為受信プログラム、７４…データ保護プログラム、１００…ゾーニングテーブル、１１０…パス構成テーブル、１２０…ＡＣＬテーブル

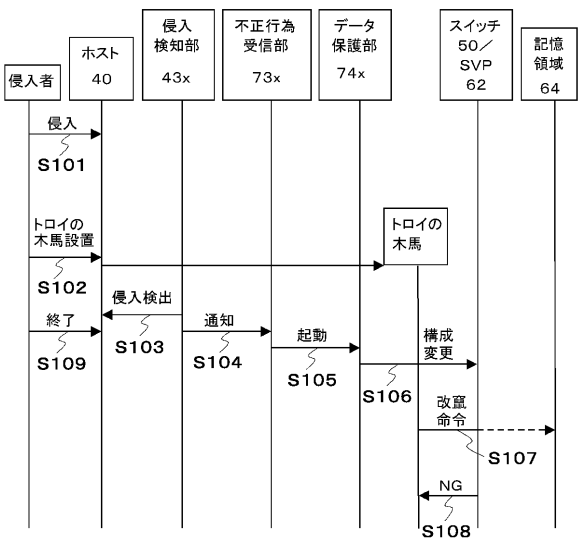
【図１】

図1



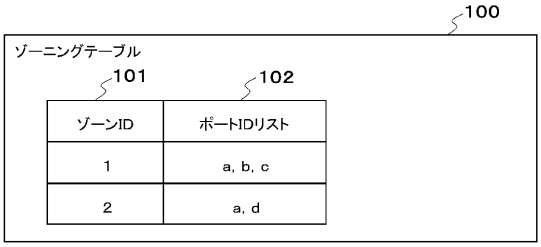
【図２】

図2



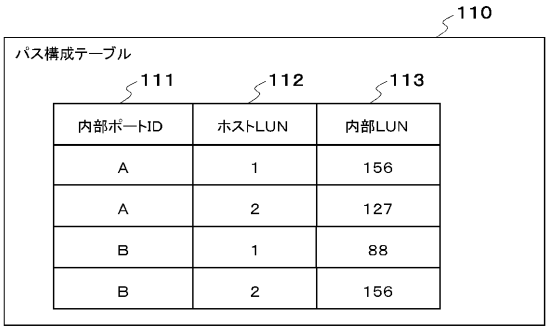
【図３】

図3



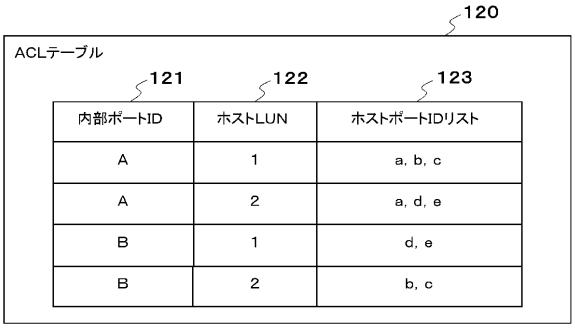
【図４】

図4



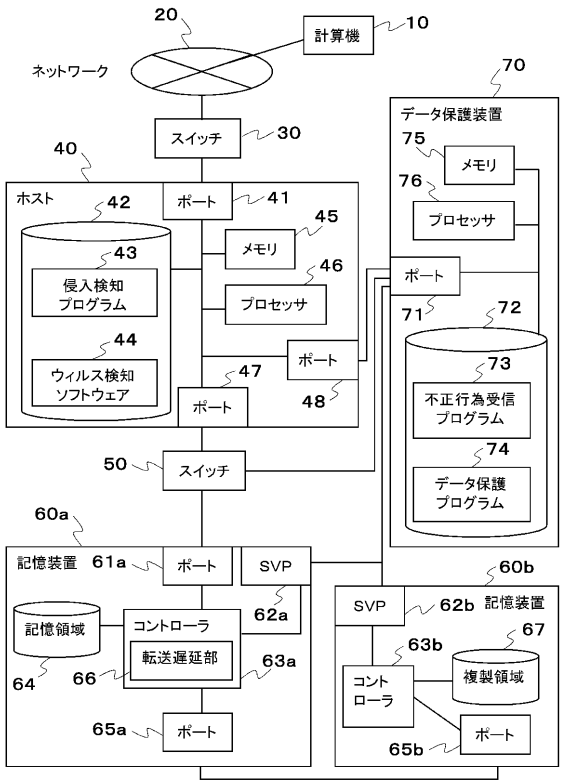
【図５】

図5



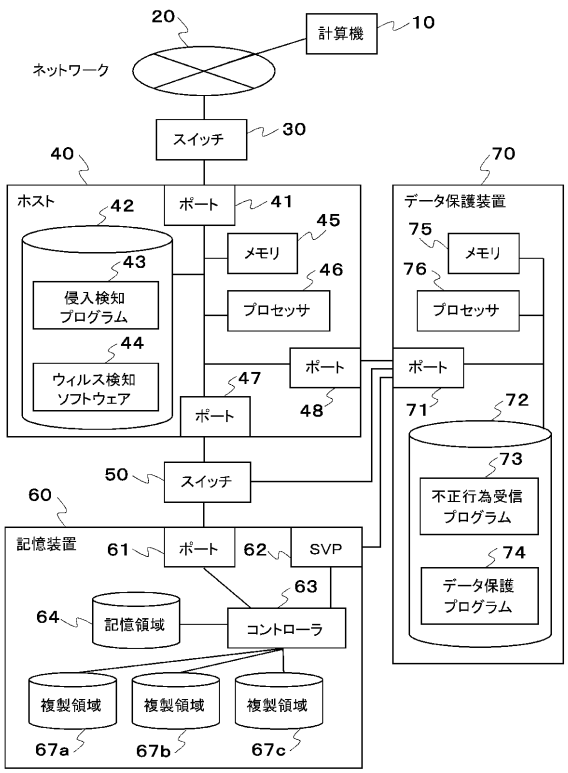
【図６】

図6



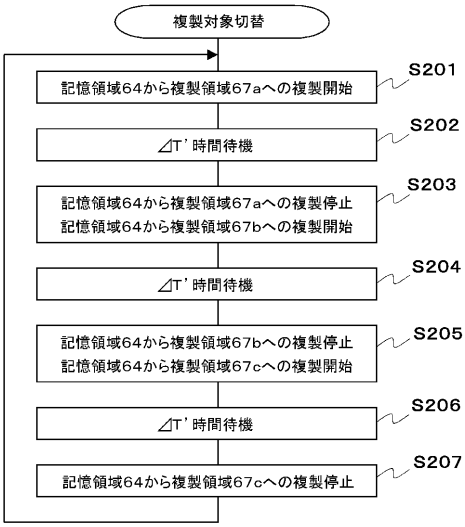
【図７】

図7



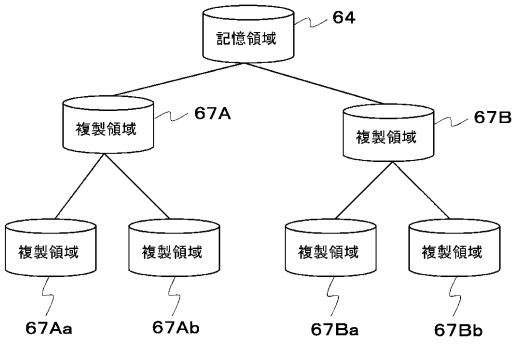
【図８】

図8


複製対象切替
記憶領域64から複製領域67aへの複製開始
S201
⊿T'時間待機
S202
記憶領域64から複製領域67aへの複製停止
記憶領域64から複製領域67bへの複製開始
S203
⊿T'時間待機
S204
記憶領域64から複製領域67bへの複製停止
記憶領域64から複製領域67cへの複製開始
S205
⊿T'時間待機
S206
記憶領域64から複製領域67cへの複製停止
S207

【図９】

図9


記憶領域
64
複製領域
67A
複製領域
67B
複製領域
複製領域
複製領域
複製領域
67Aa
67Ab
67Ba
67Bb

フロントページの続き

審査官　高橋　克

(56)参考文献　特開平１０－２５４７８４（ＪＰ，Ａ）
特開２０００－２１６８３０（ＪＰ，Ａ）
米国特許出願公開第２００２／０１４７９１５（ＵＳ，Ａ１）
特開２００２－１３２５８８（ＪＰ，Ａ）
特開２００３－３０３１１８（ＪＰ，Ａ）
特開２００２－１７５２２４（ＪＰ，Ａ）
特開平０１－２２００４８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 3/06
G06F 12/00