(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5204211号
(P5204211)
(45)発行日　平成25年6月5日(2013.6.5)　(24)登録日　平成25年2月22日(2013.2.22)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00　351Z
G06F 15/00 (2006.01)　　G06F 15/00

請求項の数 8　(全 7 頁)

(21)出願番号　特願2010-502634 (P2010-502634)
(86)(22)出願日　平成20年4月6日 (2008.4.6)
(65)公表番号　特表2010-524114 (P2010-524114A)
(43)公表日　平成22年7月15日 (2010.7.15)
(86)国際出願番号　PCT/IL2008/000473
(87)国際公開番号　WO2008/122976
(87)国際公開日　平成20年10月16日 (2008.10.16)
審査請求日　平成23年3月18日 (2011.3.18)
(31)優先権主張番号　60/910,708
(32)優先日　平成19年4月9日 (2007.4.9)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/769,760
(32)優先日　平成19年6月28日 (2007.6.28)
(33)優先権主張国　米国 (US)

(73)特許権者　508159260
サンディスク　アイエル　リミテッド
イスラエル国、４４４２５、クファー　サバ、アティール　イエダ　ストリート　７
(74)代理人　100075144
弁理士　井ノ口　壽
(72)発明者　ゴルデ，イッタイ
イスラエル国、７５３２１、リション　レツィオン、ビール　ストリート　６２Ａ
(72)発明者　ペイリー，アレクサンダー
イスラエル国、クファーサバ、ハカルメル　ストリート　８３、アパートメント　＃１６

最終頁に続く

(54)【発明の名称】ＵＳＢ記憶装置にファイアウォール保護を使用するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
ＵＳＢ取り外し可能なドライブ（ＵＲＤ）であって、
不揮発性記憶メモリと、
前記不揮発性記憶メモリと通信するコントローラであって、
前記不揮発性記憶メモリ上で実行される操作を制御し、
ネットワークプロトコルにより、ホストに常駐するファイアウォールを通じてホストと通信することによって、ホストに対してＵＲＤをローカルな大容量記憶装置としてよりもネットワークドライブとして提示し、かつ
ネットワークプロトコルを用いてホストからのデータの復号化を行い、かつ
データをＵＲＤの不揮発性記憶メモリに書き込むように構成されたコントローラと、
を備えるＵＲＤ。
【請求項２】
請求項１記載のＵＲＤにおいて、
前記不揮発性記憶メモリは、フラッシュメモリを含むＵＲＤ。
【請求項３】
請求項１記載のＵＲＤにおいて、
前記コントローラは、ホストに対してＵＲＤをネットワークドライブとして提示するのを実行可能なファームウェアを備えるＵＲＤ。
【請求項４】

ＵＳＢ取り外し可能なドライブ（ＵＲＤ）に起因する情報セキュリティリスクからホストシステムを保護する方法であって、
コントローラと通信する不揮発性記憶メモリを有するＵＲＤのコントローラにおいて、
ＵＲＤのホストシステムとの接続を検出するステップと、
ホストシステムに対してＵＲＤをローカルな大容量記憶装置としてよりもネットワークドライブとして提示するステップと、
ネットワークプロトコルにより、ホストシステムに常駐するファイアウォールを通じて、ホストシステムと通信するステップと、
ネットワークプロトコルを用いてホストシステムからのデータの復号化を行い、かつデータをＵＲＤの不揮発性記憶メモリに書き込むステップと、
を含む方法。
【請求項５】
請求項４記載の方法において、
前記ファイアウォールは、ソフトウェアファイアウォールである方法。
【請求項６】
請求項４記載の方法において、
前記ファイアウォールは、ハードウェアファイアウォールである方法。
【請求項７】
請求項４記載の方法において、
前記通信するステップは、前記ファイアウォールのセキュリティ措置に応じて通信することを含む方法。
【請求項８】
請求項７記載の方法において、
前記通信するステップは、ホストシステム上の少なくとも１つのアプリケーションへの規制されたアクセスを受信することをさらに含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークプロトコルにより通信経路を定めることによって、そしてファイアウォールを適用することによって、大容量記憶装置に起因する情報セキュリティリスクからホストシステムを保護するシステムに関する。
【背景技術】
【０００２】
ＵＳＢフラッシュドライブ（ＵＦＤ）は、ポータブルなデータ記憶装置を提供する周知のデバイスである。ＵＦＤは通常、多数のコンピュータへ互換的に接続できるように構成されている。こうした特徴のために、ＵＦＤは特有の情報セキュリティリスクをホストコンピュータに投げかける。そのようなリスクのためのセキュリティ措置の実施が必要となる。
【０００３】
先行技術では、ポータブルなデータ記憶装置に関わるリスクからホストコンピュータを保護する様々なセキュリティ措置を提供している。ウイルス対策プログラムやｍＴｒｕｓｔタイプの解決策（イスラエル国クファーサバのサンディスク　アイエル　リミテッドより入手可能）がそのようなセキュリティ措置の一例である。
先行技術の解決策には、その有用性を損なう特有の限界がある。先行技術は通常、１種類のセキュリティリスクにのみ対処するように構成される。ウイルス対策ツールは通常ならばウイルスのみの対処に限られ、ｍＴｒｕｓｔタイプの解決策は主に、アクセス規制に関わるリスクへの対処に限られている。
【０００４】
ホストシステムユーザの情報セキュリティ方針に適合しつつ、ＵＦＤセキュリティに起因する幅広い情報セキュリティリスクからホストシステムを保護する情報セキュリティシ

ステムが望まれている。
【発明の概要】
【０００５】
本発明の目的は、ネットワークプロトコルにより通信経路を定めることによって、そしてファイアウォールを適用することによって、大容量記憶装置に起因する情報セキュリティリスクからホストシステムを保護するシステムを提供することにある。
【０００６】
明確にするため、この後に記すいくつかの用語をここで具体的に定義する。ここで使用する用語「ネットワークプロトコル」は、ＯＳＩ（オープンシステムインターコネクション）ネットワークアーキテクチャにおけるネットワーク層の通信プロトコルを指し、ここではより具体的にインターネットプロトコル（ＩＰ）を指す。ここで使用する用語「ＵＳＢ取り外し可能なドライブ」および「ＵＲＤ」は、不揮発性記憶メモリとコントローラとを有する取り外し可能なドライブを指す。ＵＦＤは、フラッシュメモリを利用する特殊なＵＲＤである。
ここで使用する用語「トラフィック」は、通信システムにおける一定期間中の活動を指す。ここで使用する用語「非武装地帯」および「ＤＭＺ」は、内部ネットワークの一部でもなく、インターネットの端的な一部でもない、ネットワーク部分を指す。ここで使用する用語「ファイアウォール」は、ローカルアクセスセキュリティ方針に従いネットワーク間アクセスを制限するゲートウェイを指す。
【０００７】
本発明では、ＵＲＤに常駐し、ホストシステムに対してネットワークドライブをエミュレートするシステムと、そのようなシステムを実装する方法とを教示する。このネットワークドライブエミュレーションを実行するには、ＵＲＤコントローラに常駐するファームウェアを変更し、Ｍｉｃｒｏｓｏｆｔ（登録商標）Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステム（ＯＳ）上のネットワークデバイスとしてＵＲＤを有効にする。このＵＲＤはネットワークデバイスとして識別され、様々なファイルアクセスプロトコル（例えば、ＨＴＴＰ、ＦＴＰ、ＳＭＢ）によりアクセスできる。（コンピュータ工学の技術分野では周知であり、Ｗｉｎｄｏｗｓ　ＯＳに採用されているように、）ネットワークデバイスはドライブ名によって指定されるか、ファイルサーバとして指定される。
【０００８】
ネットワークドライブは、通常のファイアウォールシステム（カリフォルニア州サニーベールのマカフィー　コーポレイションより入手可能なＭｃＡｆｅｅ　Ｐｅｒｓｏｎａｌ　Ｆｉｒｅｗａｌｌ等）を使って保護されるべき共通のデバイスである。ファイアウォールを装備するホストシステムは、ネットワーク記憶装置として記憶装置を検出し、ファイアウォールの該当する全てのルールを適用することによって不正アクセス等の攻撃からホストシステムを保護する。
【０００９】
本発明によると、（ａ）ホストシステムとの通信のためのネットワークプロトコルを有効にするように構成されたプログラムコードを有する不揮発性記憶メモリと、（ｂ）不揮発性記憶メモリ上で実行される操作を制御するコントローラと、を備えるＵＲＤが初めて提供される。
好ましくは、不揮発性記憶メモリは、フラッシュメモリを含む。
【００１０】
本発明によると、（ａ）ファイアウォールを有するホストシステムと、（ｂ）ネットワークプロトコルを有効にするように構成されたプログラムコードを含む不揮発性記憶メモリを有するＵＲＤとを備え、ホストシステムへ実動的に接続されるＵＲＤとが初めて提供され、ファイアウォールがＵＲＤに関係するセキュリティ措置を提供するように構成される。
好ましくは、ファイアウォールは、ソフトウェアファイアウォールかハードウェアファイアウォールである。

【００１１】
これらの実施形態とさらなる実施形態は、この後に続く詳細な説明と実施例から明らかとなる。
ここでは専ら例示を目的とし、添付の図面を参照しながら本発明を説明する。
【図面の簡単な説明】
【００１２】
【図１】本発明の好適な実施形態による、ファイアウォールによって大容量記憶装置から保護されるホストシステムの簡略化されたブロック図である。
【図２Ａ】先行技術によるＵＲＤの簡略化されたブロック図である。
【図２Ｂ】本発明の好適な実施形態によるＵＲＤの簡略化されたブロック図である。
【図３】本発明の好適な実施形態による、ファイアウォールによって大容量記憶装置から保護されるホストシステム動作の簡略化されたフローチャートである。
【発明を実施するための形態】
【００１３】
本発明は、ネットワークプロトコルにより通信経路を定めることによって、そしてファイアウォールを適用することによって、大容量記憶装置に起因する情報セキュリティリスクからホストシステムを保護するシステムに関する。本発明による、大容量記憶装置に起因する情報セキュリティリスクからホストシステムを保護する原理と動作は、添付の説明と図面を参照することにより、より良く理解できる。
【００１４】
ここで図面を参照すると、図１は、本発明の好適な実施形態による、ファイアウォールによって大容量記憶装置から保護されるホストシステムの簡略化されたブロック図である。図１には３つのＵＳＢコネクタ２２を有するホストシステム２０が示されている。ＵＳＢマウス２４と、ＵＳＢキーボード２６と、ＵＲＤ２８は、それぞれ１つのコネクタ２２へ実動的に接続された状態で図に示されている。ネットワーク３２（ローカルエリアネットワーク、インターネット等）にはネットワーク接続３４を介してアクセスできる。
【００１５】
ホストシステム２０はファイアウォール３６を装備する。ファイアウォール３６はソフトウェアファイアウォール（ＭａｃＡｆｅｅ　Ｐｅｒｓｏｎａｌ　Ｆｉｒｅｗａｌｌ等）かハードウェアファイアウォール（カリフォルニア州サンノゼのシスコシステムズより入手可能なＣｉｓｃｏ　ＰＩＸ　Ｆｉｒｅｗａｌｌ　５１５Ｅ等）であってもよい。通常ＤＭＺ３８と呼ばれるファイアウォール３６の向こう側は、ホストシステム２０を外部に接続する働きをする。周辺デバイス（すなわち、ＵＳＢマウス２４、ＵＳＢキーボード２６、ＵＲＤ　２８）からのトラフィックはＣＰＵ４０へ流れ込む。ホストシステム２０と外部との接続は通常、ネットワーク接続３４へ実動的に接続されて最終的にはネットワーク３２に至るネットワークカード４２によって遂行される。不正アクセスからホストシステム２０を保護するファイアウォール３６の働きは当技術分野において周知であり、ここでは説明しない。
【００１６】
本発明の本質的な特徴は、ホストシステム２０のＤＭＺ３８に対するローカル周辺デバイス３０、典型的にはＵＲＤ等の大容量記憶装置の接続である。そのような構成において、ホストシステム２０によって周辺デバイス３０が大容量記憶装置（ＵＲＤ２８等）ではなくネットワークデバイスとして認識されなければならない。そのような構成において、ファイアウォール３６の堅牢で管理のいきとどいたセキュリティ機能の所要条件に適合することが本発明のシステムによりＵＲＤ３０に義務付けられる。
【００１７】
要約すると、ホストシステム２０へ直接接続されるＵＲＤ（例えば、ＵＲＤ２８）とＤＭＺ３８へ接続されるＵＲＤ（例えば、３０）には２つの違いがある。
（１）通信プロトコル－ＵＲＤ２８が大容量記憶クラスのデバイスであるのに対して、周辺デバイス３０は模擬ネットワークデバイスである。

（２）デバイス関連リスクに対するホストシステム２０のセキュリティ水準－ホストシステム２０にはＵＲＤ２８に対するセキュリティ措置がないが、周辺デバイス３０に対しては十分なファイアウォール保護がある。

【００１８】

図２Ａは、先行技術によるＵＲＤの簡略化されたブロック図である。図２Ａに示されるＵＲＤ５０は、不揮発性記憶メモリ５２と、フラッシュコントローラ５４と、大容量記憶クラスのプロトコル５６と、ＵＳＢコネクタ５８とを有する。データはＵＳＢコネクタ５８を通じて読み書きされ、大容量記憶クラスのプロトコル５６により符号化される。フラッシュコントローラ５４は、大容量記憶クラスのプロトコル５６から提供されるデータの符号化と復号化を行い、データを記憶メモリ５２に書き込む。

【００１９】

図２Ｂは、本発明の好適な実施形態によるＵＲＤの簡略化されたブロック図である。図２Ｂに示されるＵＲＤ６０は、不揮発性記憶メモリ６２と、フラッシュコントローラ６４と、ネットワークプロトコル６６と、ＵＳＢコネクタ６８とを有する。データはＵＳＢコネクタ６８を通じて読み書きされ、ネットワークプロトコル６６により符号化される。フラッシュコントローラ６４は、ネットワークプロトコル６６から提供されるデータの符号化と復号化を行い、データを記憶メモリ６２に書き込む。本発明によるシステムによりファイアウォールセキュリティ措置が有効となり、ＵＲＤ６０に適用されることが分かる。

【００２０】

図３は、本発明の好適な実施形態による、ファイアウォールによって大容量記憶装置から保護されるホストシステム動作の簡略化されたフローチャートである。ＵＲＤはホストシステムへ実動的に接続される（ステップ７０）。ＵＲＤのネットワークプロトコルは、ＵＲＤをホストシステム上のネットワークデバイスとして指定する（ステップ７２）。ホストシステムに常駐するファイアウォールはＵＲＤネットワークデバイスを検出する（ステップ７４）。ＵＲＤとホストシステムとの通信は、ファイアウォールのセキュリティ措置によって仲介される（ステップ７６）。なお、特定のアプリケーションによるＵＲＤアクセスを規制する形にファイアウォールを構成することもできる。

【００２１】

これまで限られた数の実施形態との関係で本発明を説明してきたが、本発明の変更、修正、応用が数多く可能であることが理解されるべきである。

【図１】

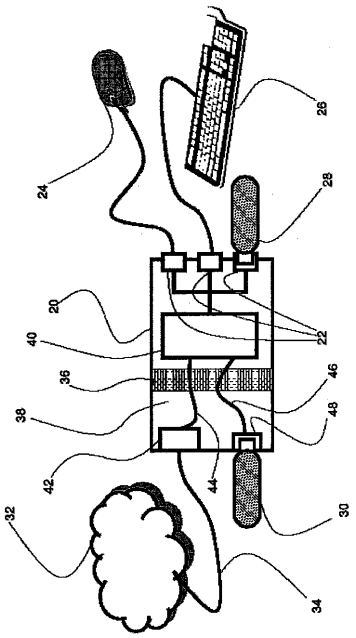

Figure 1

【図２Ａ】

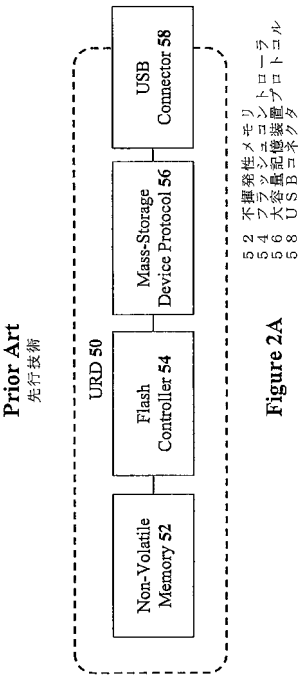

Figure 2A

【図２Ｂ】

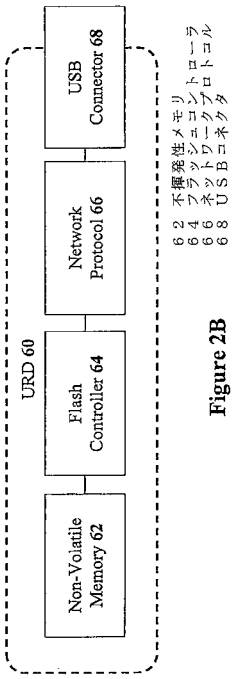

Figure 2B

【図３】

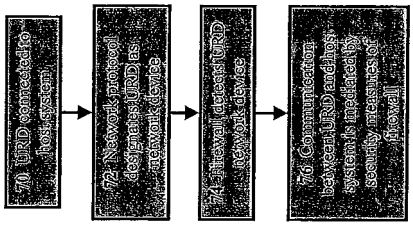

Figure 3

フロントページの続き

(31)優先権主張番号　11/769,757
(32)優先日　平成19年6月28日(2007.6.28)
(33)優先権主張国　米国(US)

(72)発明者　シュムレビッチ，レオニード
イスラエル国、７６５６９、レホボット、ドーリンスキー　ストリート　９

審査官　木村　雅也

(56)参考文献　特開２００６－１１４０４８（ＪＰ，Ａ）
国際公開第２００６／０９０３９３（WO，Ａ１）
国際公開第２００５／０５０３８４（WO，Ａ１）
国際公開第２００４／０５４１８５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　１５／００