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

特許第4256107号
(P4256107)

(45)発行日　平成21年4月22日(2009.4.22)　(24)登録日　平成21年2月6日(2009.2.6)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
G06F 11/34 (2006.01)　　G06F 11/34 B
G06F 13/00 (2006.01)　　G06F 13/00 353V

請求項の数 8　(全 21 頁)

(21)出願番号　特願2002-61800(P2002-61800)
(22)出願日　平成14年3月7日(2002.3.7)
(65)公開番号　特開2003-263413(P2003-263413A)
(43)公開日　平成15年9月19日(2003.9.19)
審査請求日　平成17年2月24日(2005.2.24)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　捧　泰士
神奈川県横浜市神奈川区新子安一丁目２番４号　株式会社富士通アドバンストソリューションズ内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】データサーバへの不正侵入対処方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
コンピュータにおいて実行される該コンピュータの不正侵入対処方法において、
前記コンピュータは、
前記コンピュータで実行されている第一のオペレーティングシステムの管理下で第二のオペレーティングシステムを実行し、該第二のオペレーティングシステムよる管理下で通信ネットワーク上でのデータの公開を行なうデータサーバを構築するアプリケーションプログラムを実行し、
前記第一のオペレーティングシステムの管理下にある比較監視部により、前記アプリケーションプログラムにより構築された前記データサーバへアクセスして該アクセスに対する該データサーバからの応答を受信し、該受信した応答が正常であるか異常であるかの判定を行ない、
前記比較監視部が前記応答を異常であると判定した場合には、前記第一のオペレーティングシステムの管理下にある復旧処理部により、前記第二のオペレーティングシステムの管理下にあるメモリに格納されているデータを取得する、
ことを特徴とするコンピュータへの不正侵入対処方法。
【請求項２】
コンピュータにおいて実行される該コンピュータの不正侵入対処方法において、
前記コンピュータは、
前記コンピュータで実行されている第一のオペレーティングシステムの管理下で第二の

オペレーティングシステムを実行し、該第二のオペレーティングシステムよる管理下で通信ネットワーク上でのデータの公開を行なうデータサーバを構築するアプリケーションプログラムを実行し、

前記第一のオペレーティングシステムの管理下にある比較監視部により、前記アプリケーションプログラムにより構築された前記データサーバへ前記通信ネットワークを介してアクセスして該アクセスに対する該データサーバからの応答を受信し、該受信した応答が正常であるか異常であるかの判定を行ない、

前記比較監視部が前記応答を異常であると判定した場合には、前記第一のオペレーティングシステムの管理下にある復旧処理部により、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる、

ことを特徴とするコンピュータへの不正侵入対処方法。

【請求項３】

コンピュータに不正侵入対処方法を実行させるためのプログラムであって、該コンピュータに、

前記コンピュータで実行されている第一のオペレーティングシステムの管理下で実行されている第二のオペレーティングシステムの管理下で実行されるアプリケーションプログラムにより構築されるデータサーバであって、通信ネットワーク上でのデータの公開を行なっている該データサーバへアクセスして該アクセスに対する該データサーバからの応答を受信し、該受信した応答が正常であるか異常であるかの判定を行なう比較監視部として動作させる処理と、

前記応答を異常であると判定した場合に、前記第二のオペレーティングシステムの管理下にあるメモリに格納されているデータを取得する復旧処理部として動作させる処理と、

を実行させることを特徴とする不正侵入対処プログラム。

【請求項４】

前記比較監視部として動作させる処理は、更に、前記比較監視部による前記データサーバへのアクセスを、前記通信ネットワークを介して行なう処理を前記コンピュータに行なわせることを特徴とする請求項３に記載の不正侵入対処プログラム。

【請求項５】

コンピュータに不正侵入対処方法を実行させるためのプログラムであって、該コンピュータに、

前記コンピュータで実行されている第一のオペレーティングシステムの管理下で実行されている第二のオペレーティングシステムの管理下で実行されるアプリケーションプログラムにより構築されるデータサーバであって、通信ネットワーク上でデータの公開を行なっている該データサーバへ該通信ネットワークを介してアクセスして該アクセスに対する該データサーバからの応答を受信し、該受信した応答が正常であるか異常であるかの判定を行なう比較監視部として動作させる処理と、

前記応答を異常であると判定した場合に、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる復旧処理部として動作させる処理と、

を実行させることを特徴とする不正侵入対処プログラム。

【請求項６】

前記復旧処理部として動作させる処理は、更に、前記応答が異常であると判定した場合に、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させた後に前記第一のオペレーティングシステムによる管理下で該第二のオペレーティングシステムを改めて実行させると共に、該第二のオペレーティングシステムによる管理下で前記アプリケーションプログラムを改めて実行させて前記データサーバを前記コンピュータで再構築させることを特徴とする請求項３又は５に記載の不正侵入対処プログラム。

【請求項７】

前記復旧処理部として動作させる処理は、更に、前記再構築されたデータサーバへのア

クセスに対する応答が異常であると前記比較監視部が判定したときには、前記第二のオペレーティングシステムの管理下にあるメモリに格納されている前記データに加えて、該データサーバの動作の履歴を取得することを特徴とする請求項６に記載の不正侵入対処プログラム。

【請求項８】

前記比較監視部として動作させる処理は、更に、前記第一のオペレーティングシステムによる管理下で実行されている前記第二のオペレーティングシステムの管理下で実行されるアプリケーションプログラムにより構築されるデータサーバであって、通信ネットワーク上でデータの公開を行なっている該データサーバへ該通信ネットワークを介してアクセスし、該アクセスに対する該データサーバからの応答を受信しなかった場合は、前記応答が異常であると判定することを特徴とする請求項３又は５に記載の不正侵入対処プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データサーバ装置で用いられる技術に関し、特に、データサーバ装置への不正侵入に対処する技術に関する。

【０００２】

【従来の技術及び発明が解決しようとする課題】

近年、ネットワークに接続されているデータサーバへの不正なアクセスが行なわれてそのシステムが乗っ取られたりそのサーバの保持しているデータの改ざんが行なわれたりする事件が多発している。

【０００３】

従来、データサーバの管理者がこのような不正侵入の事実を認識するのはそのサーバの利用者からの連絡による場合が多く、管理者がその事実を認識するまでに長い時間が経過してしまう結果、長時間に渡る不正侵入をされてしまうことが少なくなかった。

【０００４】

また、不正侵入によって乗っ取りやデータ改ざんがされてしまったデータサーバは直ちにネットワークから切り離すことが一般に要求されるが、とりわけサーバの管理者権限が乗っ取られてしまったような場合には、サーバのハードウェアとネットワークとを物理的に接続している通信ケーブル等を外すなどの作業が求められる。そのため、このような事態に常時対処するためにはそのサーバのハードウェアの傍に人が常駐することが必要となることさえあった。

【０００５】

また、このような状況に対処するために、データサーバとネットワークとを接続するルータ等の中継装置の電源を遠隔操作によって断とする手法も考えられる。しかしながら、この中継装置が他の計算機システムと共用されている場合、この手法には電源断の影響が他の計算機システムにまで及んでしまっていた。

【０００６】

また、乗っ取りやデータ改ざんがされてしまったデータサーバを復旧させる際に乗っ取りや改ざんの痕跡を示す情報をそのサーバから取得することは、同様の手口による再度の不正侵入を防止するために有益である。しかしながら、このような痕跡情報が例えば乗っ取られたサーバのメインメモリ上に残されている場合には、サーバが乗っ取られてしまっているためにメインメモリ上の痕跡情報の参照が難しく、また、サーバを再起動させて復旧させるとメインメモリ上に残されている痕跡情報が消失してしまうため、そのメインメモリ上の痕跡情報の取得は困難であった。

【０００７】

以上の問題を鑑み、データサーバへの不正侵入が発生した場合の対処を人手を介さずに行なえるようにすることが本発明が解決しようとする課題である。

【０００８】

【課題を解決するための手段】
図１は本発明の第一の原理構成を示す図である。
同図において、コンピュータ１は、制御プログラムを実行することで各構成要素を制御するＣＰＵと、ＲＯＭやＲＡＭ及び磁気記憶装置などからなり、ＣＰＵに各構成要素を制御させる制御プログラムの記憶やＣＰＵが制御プログラムを実行する際のワークエリアあるいは各種データの記憶領域として使用される記憶部と、ユーザによる操作に対応する各種のデータが取得される入力部と、ディスプレイなどに各種のデータを提示してユーザに通知する出力部と、ネットワークに接続するためのインタフェース機能を提供するＩ／Ｆ部とを備える標準的な構成を有するコンピュータである。
【０００９】
第一ＯＳ２はコンピュータ１で実行されることによってコンピュータ１の有する基本機能の管理を行なうホストオペレーティングシステムである。
第二ＯＳ３は第一のオペレーティングシステムによる管理の下でコンピュータ１で実行されるゲストオペレーティングシステムである。
【００１０】
データサーバ４は、通信ネットワーク上、例えばインターネット上でデータの公開を行なうものであり、第二ＯＳ３の管理の下でアプリケーションプログラムをコンピュータ１で実行することによってコンピュータ１で構築されるものである。
【００１１】
不正侵入対処プログラム５は本発明に係るものであり、第一ＯＳ２の管理の下でコンピュータ１で実行させることにより、アクセス処理５－１、判定処理５－２、及びデータ取得処理５－３をコンピュータ１に行なわせる。
【００１２】
アクセス処理５－１はデータサーバ４へのアクセスを行なう処理である。
判定処理５－２は、アクセス処理５－１の実行によって行なわれたアクセスに対するデータサーバ４からの応答が正常であるか異常であるかの判定を行なう処理である。
【００１３】
データ取得処理５－３は、判定処理５－２の実行によってデータサーバ４からの応答が異常であると判定されたときに、第二ＯＳ３によって管理されているメモリに格納されているデータの取得を行なう処理である。
【００１４】
上述したように、不正侵入対処プログラム５は第一ＯＳ２の管理の下でコンピュータ１で実行させる。一方、テータサーバ４を構築するアプリケーションプログラムは第一ＯＳ２の管理の下で実行されている第二ＯＳ３の管理の下で実行させている。従って、例えデータサーバ４が不正侵入されてしまったとしても、前述した痕跡情報が残されている可能性のある、第二ＯＳ３によって管理されているメモリに格納されているデータは、第一ＯＳ２の管理の下で行なわれるデータ取得処理５－３によって取得することができるのである。以上のように、図１に示した本発明の第一の構成によれば、第二ＯＳ３によって管理されているメモリ上に残されている痕跡情報の取得が可能となる。
【００１５】
なお、上述した本発明の第一の原理構成において、データサーバ４へのアクセスを前記通信ネットワークを介して行なう処理をアクセス処理５－１として実行し、アクセスに対してデータサーバ４から通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう処理を判定処理５－２として実行することができる。
【００１６】
こうすることにより、データサーバ４がデータを公開するサービスを提供している通信ネットワーク側からみたときのデータサーバ４の挙動の監視が行なわれるので、そのサービスの提供が正しく行なわれているかをより適切に監視することができる。
【００１７】
また、前述した本発明の第一の原理構成において、データサーバ４へのアクセスに対する

応答が取得されなかったときには、そのアクセスに対するデータサーバ４からの応答が異常であるとの判定を下す処理を判定処理５－２として実行することができる。

【００１８】

データサーバ４へのアクセスに対する応答が取得されなかったときは、そのアクセスがデータサーバ４で受け付けられなかったと推定され、これはすなわちデータサーバ４に対する乗っ取り等の不正侵入が発生したと考えられる。従って、こうすることにより、このような不正侵入における痕跡情報が残されている可能性のある第二ＯＳ３によって管理されているメモリに格納されているデータの取得が可能となる。

【００１９】

また、前述した本発明の第一の原理構成において、データサーバ４へのアクセスに対する応答が、予め想定されている応答と異なるものであったときにそのアクセスに対するデータサーバ４からの応答が異常であるとの判定を判定処理５－２として実行することができる。

【００２０】

データサーバ４へのアクセスに対する応答が予め想定されているものと異なるものであったときには、データサーバ４に対する改ざん等の不正侵入が発生したと考えられる。従って、こうすることにより、このような不正侵入における痕跡情報が残されている可能性のある第二ＯＳ３によって管理されているメモリに格納されているデータの取得が可能となる。

【００２１】

また、前述した本発明の第一の原理構成において、第一ＯＳ２の管理の下で不正侵入対処プログラム５を実行させることにより、判定処理５－２の実行の結果、データサーバ４へのアクセスに対する応答が異常であると判定したときに、データサーバ４をコンピュータ１で構築するアプリケーションプログラムの実行を管理している第二ＯＳ３の実行を強制終了させる処理を更にコンピュータ１に行なわせるようにすることができる。

【００２２】

データサーバ４に対する不正侵入が発生してもその影響は第二ＯＳ３までであり第一ＯＳ２には及ばないので不正侵入対処プログラム５の実行によって第二ＯＳ３の実行を強制終了させることは可能である。従って、こうすることにより、不正侵入されたデータサーバ４の動作を人手を介することなく停止させることが可能となる。

【００２３】

なお、このとき、第一ＯＳ２の管理の下で不正侵入対処プログラム５を実行させることにより、第二ＯＳ３の実行を強制終了させた後に、第一ＯＳ２による管理の下で第二ＯＳ３を改めて実行させると共に、第二ＯＳ３による管理の下で前述したアプリケーションプログラムを改めて実行させてデータサーバ４をコンピュータ１で再構築させる処理を更にコンピュータ１に行なわせるようにすることもできる。

【００２４】

こうすることにより、強制的に停止させたデータサーバ４がコンピュータ１で再構築されるので、データサーバ４への不正侵入に起因する通信ネットワークへのデータ公開のサービスの中断時間が短縮される。また、不正侵入対処プログラム５と第二ＯＳ３とはいずれもコンピュータ１で実行されている第一ＯＳ２の管理の下で実行されるので、データサーバ４の復旧は迅速である。

【００２５】

また、このとき、第一ＯＳ２の管理の下で不正侵入対処プログラム５を実行させることにより、コンピュータ１で再構築されたデータサーバ４へのアクセスに対する応答が異常であると判定したときに、第二ＯＳ３によって管理されているメモリに格納されているデータに加えて、データサーバ４の動作の履歴を取得する処理を更にコンピュータ１に行なわせるようにすることもできる。

【００２６】

こうすることにより、データサーバ４への不正侵入が繰り返されたときに、データサーバ

４の履歴を示す情報が痕跡情報の残されている可能性のある情報として取得され、犯人の特定や侵入の手口の解析などがより容易に行なえるようになる。

【００２７】

また、前述した本発明の第一の原理構成において、第一ＯＳ２の管理の下で不正侵入対処プログラム５を実行させることにより、データサーバ４へのアクセスに対する応答が異常であると判定したときに、異常の発生を示す情報を所定の連絡先に宛てて送信する処理を更にコンピュータ１に行なわせるようにすることができる。

【００２８】

こうすることにより、コンピュータ１の傍に管理者が不在であっても、データサーバ４で異常が発生した事実をその連絡先の管理者が直ちに把握することができるようになる。

【００２９】

なお、このとき、異常の発生を示す情報を送信する処理は、第二ＯＳ３によって管理されているメモリに格納されているデータの取得を行なう処理によって取得されたデータを該異常の発生を示す情報に添付して送信する処理としてコンピュータ１に行なわせるようにすることもできる。

【００３０】

こうすることにより、コンピュータ１から遠隔の地にいる管理者が痕跡情報の解析を行なうことができるようになる。

また、ここで、異常の発生を示す情報を送信する処理は、該異常の発生を示す情報を所定の連絡先に宛てて送信すると共に、該連絡先のうち予め選択されている一部の連絡先に宛てて送信する該異常の発生を示す情報には、第二ＯＳ３によって管理されているメモリに格納されているデータの取得を行なう処理によって取得されたデータを添付して送信する処理としてコンピュータ１に行なわせるようにすることもできる。

【００３１】

こうすることにより、痕跡情報の解析を行なうスキルを有する管理者にのみ上述のデータを提示することができるようになるので、セキュリティ上重要な情報である痕跡情報の漏洩のおそれが軽減される。

【００３２】

図２は本発明の第二の原理構成を示す図である。なお、同図において、図１に示したものと同一の名称が付されている構成要素には同一の符号を付している。

図２において、コンピュータ１、第一ＯＳ２、第二ＯＳ３、及びデータサーバ４は図１に示したものと同様のものであるが、コンピュータ１は通信ネットワーク６を介して行なわれるデータの授受を管理するインタフェースを複数有しており、そのうちのひとつは第一ＯＳ２によって管理されており、その他のうちのひとつは第二ＯＳ３によって管理されている。なお、通信ネットワーク６は例えばインターネットである。

【００３３】

不正侵入対処プログラム５は本発明に係るものであり、第一ＯＳ２の管理の下でコンピュータ１で実行させることにより、アクセス処理５－１、判定処理５－２、及び強制終了処理５－４をコンピュータ１に行なわせる。

【００３４】

アクセス処理５－１は、データサーバ４へのアクセスを通信ネットワーク６を介して行なう。

判定処理５－２は、アクセス処理５－１の実行によってなされたアクセスに対してデータサーバ４から通信ネットワーク６を介して送られてくる応答が正常であるか異常であるかの判定を行なう。

【００３５】

強制処理５－４は、判定処理５－２の実行によってデータサーバ４からの応答が異常であると判定されたときに、データサーバ４をコンピュータ１で構築するアプリケーションプログラムの実行を管理している第二ＯＳ３の実行を強制終了させる。

【００３６】

上述したように、不正侵入対処プログラム５は第一ＯＳ２の管理の下でコンピュータ１で実行させる。一方、テータサーバ４を構築するアプリケーションプログラムは第一ＯＳ２の管理の下で実行されている第二ＯＳ３の管理の下で実行させている。従って、例えデータサーバ４が不正侵入されてしまったとしても、その影響は第二ＯＳ３までであり第一ＯＳ２には及ばないので不正侵入対処プログラム５の実行によって第二ＯＳ３の実行を強制終了させることは可能である。従って、こうすることにより、不正侵入されたデータサーバ４の動作を人手を介することなく停止させることが可能となる。しかも、不正侵入対処プログラム５と第二ＯＳ３とはいずれもコンピュータ１で実行されている第一ＯＳ２の管理の下で実行されているので、強制終了は迅速に行なうことができる。

【００３７】

また、図１及び図２に示したコンピュータ１で上述した不正侵入対処プログラム５を実行させることによってコンピュータ１が行なう不正侵入対処方法によっても前述した課題は解決される。更に、上述した不正侵入対処プログラムを実行させた図１及び図２に示したコンピュータ１によって構成される不正侵入対処装置によっても前述した課題は解決される。

【００３８】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。なお、ここでは、ＷＷＷ（World Wide Web）システムを使用してインターネット上にＷｅｂ文書データを公開するＷｅｂサーバ装置において本発明を実施する形態について説明する。

【００３９】

図３は本発明を実施するＷｅｂサーバ装置のハードウェア構成を示している。同図に示すＷｅｂサーバ装置は、ＣＰＵ１１、ＲＡＭ１２、ＲＯＭ１３、ＨＤＤ１４、入力部１５、出力部１６、ＮＷインタフェースＡ１７、ＮＷインタフェースＢ１８がバス１９を介して相互に接続されて構成されており、ＣＰＵ１１による管理の下で相互にデータ授受を行なうことができる。

【００４０】

ＣＰＵ（Central Processing Unit ）１１はこのＷｅｂサーバ装置（以下、「本装置」という）１０全体の動作制御を司る中央処理装置である。

ＲＡＭ（Random Access Memory）１２は、各種制御プログラムをＣＰＵ１１が実行するときにワークメモリとして使用され、また各種のデータの一時的な格納領域として必要に応じて用いられるメインメモリとしても使用されるメモリである。

【００４１】

ＲＯＭ（Read Only Memory）１３は、ＣＰＵ１１によって実行される基本制御プログラムが予め格納されているメモリであり、本装置１０の起動時にＣＰＵ１１がこの基本制御プログラムを実行することによって本装置１０全体の動作の基本的な制御がＣＰＵ１１によって行なわれる。

【００４２】

ＨＤＤ（Hard Disk Drive ）１４は、本装置１０の有する基本機能の管理を行なうためのホストＯＳ（Operating System）プログラム、ホストＯＳの管理の下で実行され、ホストＯＳと同様の機能管理を行なうゲストＯＳ、ゲストＯＳの管理の下で実行されてＷｅｂサーバ機能を提供するＷｅｂサーバプログラム、ホストＯＳの管理の下で実行され、Ｗｅｂサーバプログラムによって提供されるＷｅｂサーバ機能の動作を監視して不正侵入を監視し、不正侵入が検出されたときには所定の対処措置を講じる不正侵入対処プログラム、Ｗｅｂサーバプログラムの実行によってインターネット上に公開されるＷｅｂ文書データが格納されているＷｅｂ文書データファイル、Ｗｅｂサーバプログラムの実行時に不正侵入が発見されたときにその不正侵入に関する情報を本装置１０の管理者へ送付するときの送付先を示すデータが格納されている連絡先ファイル等が記憶されているハードディスク装置である。

【００４３】

入力部１５は外部からの入力を受け取ってその入力の内容をＣＰＵ１１に渡すものであり、例えばキーボードやマウスなどといった本装置１０を操作する操作者からの指示を受け取る入力装置、あるいはＦＤ（Flexible Disk）、ＣＤ－ＲＯＭ（Compact Disc-ROM）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc-ROM）、ＭＯ（Magneto-Optics）ディスクなどといった可搬型の記録媒体の読出装置を備えて構成される。

【００４４】

出力部１６はＣＰＵ１１からの指示に応じた出力を行なうものであり、例えば各種データを表示するＣＲＴ（Cathode Ray Tube）やＬＣＤ（Liquid Crystal Display）からなるディスプレイ装置や各種データを印刷するプリンタ装置などである。

【００４５】

ＮＷ（ネットワーク）インタフェースＡ１７及びＮＷインタフェースＢ１８は本装置１０をＬＡＮ（Local Area Network）に接続して本装置１０と外部機器との間でのデータ授受を行なう際の通信管理を行なうものであり、本装置１０は２つのＮＷインタフェースを有している。

【００４６】

本装置は以上の各構成要素を備えて構成される。

なお、図３に示す本装置１０は標準的なコンピュータにＮＷインタフェースを２つ設けることでも構成することができる。

【００４７】

次に図４について説明する。同図は、本装置１０の機能構成を示している。同図において、図３に示されているものと同じ構成要素には同一の符号を付している。

【００４８】

図４に示すように、本装置１０はＮＷインタフェースＡ１７からハブ（集線装置）Ａ５０及びルータＡ７０を介してインターネット９０に接続されており、更にＮＷインタフェースＢ１８からハブＢ６０及びルータＢ８０を介してもインターネット９０に接続されている。つまり、本装置１０は異なる通信回線を経由してインターネット９０と接続されている。

【００４９】

本装置１０を起動させてＲＯＭ１３に格納されている基本制御プログラムの実行がＣＰＵ１１によって開始されると、まずホストＯＳプログラムがＣＰＵ１１によってＨＤＤ１４から読み出されてホストＯＳ２０の実行が開始される。

【００５０】

続いてＣＰＵ１１は、ゲストＯＳプログラムをＨＤＤ１４から読み出してゲストＯＳ＿Ａ３０の実行を開始する。ここで、ここで、本装置１０が有している２つのＮＷインタフェースのうち、ＮＷインタフェースＡ１７はホストＯＳ２０が管理するが、ＮＷインタフェースＢ１８はゲストＯＳ＿Ａ３０の管理下に置かれる。

【００５１】

更に、ＣＰＵ１１はＷｅｂサーバプログラム及びＷｅｂ文書データをＨＤＤ１４から読み出し、　読み出されたＷｅｂサーバプログラムをゲストＯＳ＿Ａ３０の管理下で実行することによって、読み出されたＷｅｂ文書データａ３２をインターネット９０上に公開するためのＷｅｂサーバａ３１を構築する。

【００５２】

ここで、ＣＰＵ１１は、不正侵入対処プログラム２１をＨＤＤ１４から読み出し、ホストＯＳ２０の管理下で実行を開始する。不正侵入対処プログラム２１を実行することによって、ＣＰＵ１１は比較監視部２１－１、復旧処理部２１－２、及び連絡処理部２１－３として機能する。

【００５３】

比較監視部２１－１は、Ｗｅｂサーバａ３１によってインターネット９０上に公開されているＷｅｂ文書データａ３２と、ＨＤＤ１４に記憶されているＷｅｂ文書データａ３２と同一内容であるマスタＷｅｂ文書データ２２との比較処理を行なって不正侵入の発生の有

無を監視する。
【００５４】
復旧処理部２１－２は、不正侵入によって異常な挙動をしているＷｅｂサーバａ３１から痕跡情報を収集すると共に、ホストＯＳ２０の管理下でゲストＯＳ＿Ｂ４０を実行させ、更にゲストＯＳ＿Ｂ４０の管理下でＷｅｂサーバプログラムを実行させてＷｅｂ文書データａ３２と同一であるＷｅｂ文書データｂ４２をインターネット９０上に公開するためのＷｅｂサーバｂ４１の構築の処理を行なう。
【００５５】
連絡処理部２１－３は、不正侵入の発生を示す情報、及び復旧処理部２１－２によって取得された痕跡情報を、連絡先ファイルに示されている連絡先に送付する。
【００５６】
以下、不正侵入対処プログラム２１の実行によってＣＰＵ１１によって行なわれる不正侵入対処処理の内容について説明する。図５は、この不正侵入対処処理の処理内容を示すフローチャートである。
【００５７】
図５において、Ｓ１０１からＳ１０４にかけての処理は比較監視部２１－１として行なわれるものであり、Ｓ１０５の処理は復旧処理部２１－２として、またＳ１０６の処理は連絡処理部２１－３としてそれぞれ行なわれるものである。
【００５８】
まず、Ｓ１０１では、処理の進行を所定時間だけウェイト（一時停止）させる。このウェイトの時間については、短くすると本装置１０によるＷｅｂサーバ機能の動作監視の頻度が多くなるが、それだけ本装置１０への処理負担も増加するため、両者のバランスを考慮して設定する。
【００５９】
Ｓ１０２では、ゲストＯＳ＿Ａ３０の管理下で構築されているＷｅｂサーバａ３１へのインターネット９０を介してのアクセスがＮＷインタフェースＡ１７、ハブＡ５０、及びルータＡ７０を経由して行なわれ、Ｗｅｂサーバａ３１によってハブＢ６０、ルータＢ８０を介してインターネット９０上に公開されているＷｅｂ文書データａ３２がＮＷインタフェースＡ１７より取得される。なお、このＷｅｂサーバａ３１へのアクセスは、ＩＤ（IDentification）やパスワードをインターネット９０を介してＷｅｂサーバａ３１へ送付して行なうものであってもよい。
【００６０】
Ｓ１０３では、前ステップの処理によってＷｅｂ文書データａ３２の取得が行なえたか否かが判定され、この判定結果がＹｅｓならばＳ１０４に進む。一方、Ｓ１０３の判定処理がＮｏならば、Ｗｅｂサーバａ３１に対して乗っ取り等の不正侵入が行なわれたものとみなされ、Ｓ１０５に処理が進む。
【００６１】
Ｓ１０４では、マスタＷｅｂ文書データ２２と直前に行なわれたＳ１０２の処理によってＷｅｂ文書データａ３２とのデータ内容の比較が行なわれ、この両者に相違がないかどうかが判定される。そして、この判定結果がＹｅｓ、すなわち両データのデータ内容が一致しているのであればＳ１０１へ処理が戻って本装置１０によるＷｅｂサーバ機能の監視が繰り返される。一方、このＳ１０４の判定結果がＮｏ、すなわち両データのデータ内容に異なる部分が存在するのであれば、Ｗｅｂサーバａ３１に対して改ざん等の不正侵入が行なわれたものとみなされ、Ｓ１０５に処理が進む。
【００６２】
このＳ１０４の処理を図６から図９に示されているデータ例を用いて更に説明する。
図６はＷｅｂ文書データファイルの例を示している。このＷｅｂ文書データファイルは「ｉｎｄｅｘ．ｈｔｍｌ」なる名称が付されており、このファイルにはデータサイズは「９１」バイトであり、ファイルの更新日時は「２００２．０１．２５　１１：２９：００」であることが属性として示されている。また、同図に示されているＷｅｂ文書データファ

イル「ｉｎｄｅｘ．ｈｔｍｌ」のデータ内容は図７に示されており、このデータファイルにはＨＴＭＬ（HyperText Markup Language ）で記述されたＷｅｂ文書データが格納されている。

【００６３】

この図６及び図７に示されたＷｅｂ文書データファイルの改ざん例が図８及び図９に示されている。図８に示されているＷｅｂ文書データファイルについての属性情報ではファイルの更新日時が「２００２．０２．０９　００：１１：１１」とされており図６に示されているものと異なっている。また、図９に示されている図８のＷｅｂ文書データファイル「ｉｎｄｅｘ．ｈｔｍｌ」のデータ内容は、その第４行目が「Ｇｏｏｄｂｙｅ！」となっていて図７に示されているデータ内容と異なっている。

【００６４】

Ｓ１０４の処理では、図６及び図８のようなＷｅｂ文書データファイルについての属性情報の比較を行なうと共に、図７及び図９のようなＷｅｂ文書データファイルのデータ内容の比較をも行ない、これらの全てが一致している場合にのみ両者は一致しているとの判定を下す、すなわちＳ１０４の判定結果をＮｏとするようにする。

【００６５】

図５の説明を進める。Ｓ１０５では乗っ取り改ざん対応処理が行なわれ、続くＳ１０６では乗っ取り改ざん連絡処理が行なわれる。その後はＳ１０１へ処理が戻って本装置１０によるＷｅｂサーバ機能の監視が繰り返される。乗っ取り改ざん対応処理及び乗っ取り改ざん連絡処理の詳細は次に説明する。

【００６６】

以降、Ｓ１０１からの処理が繰り返され、Ｗｅｂサーバａ３１の動作の監視がインターネット９０を介して定期的に行なわれる。

以上までの処理が不正侵入対処処理である。

【００６７】

次に、図５におけるＳ１０５の処理である乗っ取り改ざん対応処理について説明する。図１０は乗っ取り改ざん対応処理の処理内容を示すフローチャートである。

【００６８】

まず、Ｓ２０１では、Ｗｅｂサーバａ３１を機能させていたゲストＯＳ＿Ａ３０のプロセスダンプがＲＡＭ１２から取得され、更に、Ｗｅｂサーバａ３１及びゲストＯＳ＿Ａ３０の動作履歴が記録されているログデータファイル等、そのゲストＯＳ＿Ａ３０において使用していた各種データファイルのコピーが取得され、これらのデータがＨＤＤ１４に一旦記憶される。

【００６９】

ゲストＯＳ＿Ａ３０はホストＯＳ２０上で実行されているプロセスのひとつに過ぎないので、ホストＯＳ２０の管理の下で実行されている乗っ取り改ざん対応処理の実行によって、前述した痕跡情報となり得るゲストＯＳ＿Ａ３０のプロセスダンプをＲＡＭ１２から取得することができる。また、このとき併せて取得されるゲストＯＳ＿Ａ３０において使用していた各種データファイルのコピーも痕跡情報のひとつである。この他、ホストＯＳ２０より観察されるゲストＯＳ＿Ａ３０の実行環境を示す情報なども痕跡情報として取得するようにしてもよい。

【００７０】

このように、本装置１０は、Ｗｅｂサーバａ３１を提供するゲストＯＳ＿Ａ３０と不正侵入対処処理とがホストＯＳ２０上で並行して実行されているので、Ｗｅｂサーバａ３１に対する不正侵入についての痕跡情報をメインメモリであるＲＡＭ１２から容易に取得することができる。

【００７１】

Ｓ２０２では、ゲストＯＳ＿Ａ３０を強制終了させる処理が行なわれる。

Ｓ２０３では、ゲストＯＳプログラムがＨＤＤ１４から読み出されてゲストＯＳ＿Ｂ４０の実行が開始され、更にゲストＯＳ＿Ｂ４０の管理下でＷｅｂサーバプログラム及びＷｅ

ｂ文書データがＨＤＤ１４から読み出されてＷｅｂサーバプログラムが実行され、Ｗｅｂ文書データａ３２と同一であるＷｅｂ文書データｂ４２をインターネット９０上に公開するＷｅｂサーバｂ４１が構築される。ここで、Ｗｅｂサーバｂ４１及びゲストＯＳ＿Ｂ４０の動作履歴が記録されるログデータファイルへの記録の際には、Ｗｅｂサーバａ３１及びゲストＯＳ＿Ａ３０について記録された動作履歴の内容よりも更に詳細な内容を記録するように設定しておくと、再度の不正侵入がなされたときに前よりも詳細な痕跡情報が取得されるので、不正侵入の抜本的な対策を行なうときに有益である。

【００７２】

以上までの処理を終えた後には乗っ取り改ざん対応処理が終了し、処理は図５へと戻る。なお、この後に行なわれる図５のＳ１０２以降の処理では、Ｗｅｂ文書データｂ４２をインターネット９０を介して取得する処理を試みることによるＷｅｂサーバｂ４１についての動作の監視が行なわれる。また、この後に行なわれる、処理の進行を所定時間だけウェイト（一時停止）させるＳ１０１の処理において、それまでに設定されていた所定時間を短くするようにしてもよい。こうすることにより、Ｗｅｂサーバｂ４１についてなされる不正侵入の監視の間隔がＷｅｂサーバａ３１についてなされていたものよりも短くなり、再度の不正侵入の発生に対する痕跡情報の取得やＷｅｂサーバ機能の復旧がより迅速に行なえるようになり、有益である。

【００７３】

次に、図５におけるＳ１０６の処理である乗っ取り改ざん連絡処理について説明する。図１１は乗っ取り改ざん連絡処理の処理内容を示すフローチャートである。

【００７４】

まず、Ｓ３０１では、連絡先等設定ファイル２３が参照され、そこに示されている連絡先アドレスを宛先とする電子メールが作成される。この電子メールの本文には、本装置１０で提供されているＷｅｂサーバ機能に異常が発生した旨、及びその異常の具体的な内容、例えば、Ｗｅｂ文書データａ３２がインターネット９０を介して取得できなかったこと（すなわち図５のＳ１０３の判定処理の結果がＮｏであったこと）や、取得されたＷｅｂ文書データａ３２がマスタＷｅｂ文書データ２２と異なるものであったこと（すなわち図５のＳ１０４の判定結果がＹｅｓであったこと）などが記載される。

【００７５】

Ｓ３０２では、連絡先等設定ファイル２３において調査用資料送信フラグが「１」に設定されている項目が存在するか否かが判定される。そして、この判定結果がＹｅｓのときにのみＳ３０３の処理が行なわれ、この判定結果がＮｏのときはＳ３０４に処理が進む。

【００７６】

Ｓ３０３では、前述した図１０の乗っ取り改ざん対応処理におけるＳ２０１の処理によって取得された痕跡情報に対して周知のデータ可逆圧縮処理が施されて得られたデータファイルが、調査用資料送信フラグが「１」である項目に示されている連絡先アドレスを宛先に設定した電子メールに添付される。

【００７７】

連絡先等設定ファイル２３のデータ例を図１２に示す。同図に示す連絡先等設定ファイル２３では、電子メールの宛先を示す２つの連絡先アドレスの各々に調査用資料送信フラグとが対応付けられている。ここで、上の行の連絡先アドレスに対応する調査用資料送信フラグは「１」に設定されており、この連絡先アドレスを宛先とする電子メールには痕跡情報が添付される。一方、下の行の連絡先アドレスに対応する調査用資料送信フラグは「０」に設定されており、この連絡先アドレスを宛先とする電子メールには痕跡情報が添付されない。このように、本装置１０は、調査用資料送信フラグの設定により、セキュリティ上重要な情報である痕跡情報を提供する提供先を例えばその痕跡情報を解析することのできるだけのスキルを有している管理者のみ等に制限することができ、有益である。

【００７８】

Ｓ３０４では、作成された電子メールがＮＷインタフェースＡ１７からハブＡ５０及びルータＡ７０を介してインターネット９０へ送出される。

Ｓ３０５では、連絡先等設定ファイル２３に定義されている全ての連絡先アドレスについて電子メールを送信したか否かが判定され、この判定結果がＹｅｓならばこの乗っ取り改ざん連絡処理が終了し、処理は図５へと戻る。一方、この判定結果がＮｏならばＳ３０１へと処理が戻り、電子メールが未送信である連絡先アドレスを宛先とする電子メールの作成及び送信の処理が行なわれる。

【００７９】

以上までの処理が乗っ取り改ざん連絡処理である。

本装置１０のＣＰＵ１１により上述した図５、図１０、及び図１１からなる不正侵入対処処理がホストＯＳ２０の管理の下で行なわれることによって、Ｗｅｂサーバａ３１に対する乗っ取りや改ざんなどの不正侵入の監視、不正侵入によって残された痕跡情報の取得、Ｗｅｂサーバ機能の復旧といった各作業が、人手を介さずに行なわれる。

【００８０】

また、このような処理をコンピュータに行なわせる不正侵入対処プログラム２１をコンピュータで読み取り可能な記録媒体に記録させ、そのプログラムを記録媒体からコンピュータに読み出させて実行させることによって本発明をコンピュータで実施することも可能である。

【００８１】

記録させた制御プログラムをコンピュータで読み取ることの可能な記録媒体の例を図１３に示す。同図に示すように、記録媒体としては、例えば、コンピュータ１００１に内蔵若しくは外付けの付属装置として備えられるＲＡＭ若しくはＲＯＭ又はハードディスク装置などのメモリ１００２、あるいはフレキシブルディスク、ＭＯ（光磁気ディスク）、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどといった可搬型記録媒体１００３等が利用できる。また、記録媒体は通信回線１００４を介してコンピュータ１００１と接続される、プログラムサーバ１００５として機能するコンピュータが備えている記憶装置１００６であってもよい。この場合には、制御プログラムを表現するデータ信号で搬送波を変調して得られる伝送信号を、プログラムサーバ１００５から伝送媒体である通信回線１００４を通じて伝送するようにし、コンピュータ１００１では受信した伝送信号を復調して制御プログラムを再生することで当該制御プログラムを実行できるようになる。

【００８２】

その他、本発明は、上述した実施形態に限定されることなく、種々の改良・変更が可能である。

例えば、ホストＯＳ２０の管理下でゲストＯＳ＿Ａ３０及びゲストＯＳ＿Ｂ４０を動作させる代わりに、ホストＯＳ２０の管理下で本装置１０に相当するハードフェア環境を仮想的に構築するエミュレーションプログラムを動作させ、構築された仮想環境の下でゲストＯＳ及び不正侵入対処プログラムを実行させるようにすることも可能である。

【００８３】

また、ホストＯＳ２０で管理が行なえるのであれば、ホストＯＳ２０と同一のＯＳをゲストＯＳとして採用する構成とすることもできる。

また、本実施の形態では、ゲストＯＳ＿Ａ３０やゲストＯＳ＿Ｂ４０がメインメモリとして活用しているメモリは、Ｗｅｂサーバ装置１０についてのメインメモリを利用するようにしていたが、ホストＯＳ２０上で起動されるゲストＯＳ＿Ａ３０やゲストＯＳ＿Ｂ４０がＷｅｂサーバ装置１０のメインメモリ以外のメモリ（あるいはメモリ領域）を使用する構成とすることもできる。なお、この構成において図１０に示す乗っ取り改ざん対応処理を実行するときは、ホストＯＳ２０がゲストＯＳ＿Ａ３０を強制的に終了させるＳ２０２の処理の前に実行されるＳ２０１のゲスト＿ＯＳＡ３０のプロセスダンプの取得処理において、Ｗｅｂサーバ装置１０についてのメインメモリに格納されているデータを、ゲストＯＳ＿Ａ３０がメインメモリとして使用しているメモリ（あるいはメモリ領域）に格納されているデータと共に取得するようにし、これらのデータを纏めてＨＤＤ１４に記憶させるようにするとよい。

【００８４】

（付記１）　コンピュータで実行されている第一のオペレーティングシステムによる管理の下で第二のオペレーティングシステムを実行させ、
前記コンピュータで実行させることによって通信ネットワーク上でデータの公開を行なうデータサーバが該コンピュータで構築されるアプリケーションプログラムを前記第二のオペレーティングシステムによる管理の下で実行させ、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを前記第一のオペレーティングシステムによる管理の下で行ない、
前記アクセスに対する前記データサーバからの応答が正常であるか異常であるかの判定を前記第一のオペレーティングシステムによる管理の下で行ない、
前記応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータの取得を前記第一のオペレーティングシステムの管理の下で行なう、
ことを特徴とするコンピュータへの不正侵入対処方法。
（付記２）　前記データサーバへのアクセスは、前記通信ネットワークを介して行ない、
前記判定は、前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう、
ことを特徴とする付記１に記載の不正侵入対処方法。
（付記３）　コンピュータで実行されている第一のオペレーティングシステムによる管理の下で第二のオペレーティングシステムを実行させ、
前記コンピュータで実行させることによって通信ネットワーク上でデータの公開を行なうデータサーバが該コンピュータで構築されるアプリケーションプログラムを前記第二のオペレーティングシステムによる管理の下で実行させ、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを前記第一のオペレーティングシステムによる管理の下で前記通信ネットワークを介して行ない、
前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を前記第一のオペレーティングシステムによる管理の下で行ない、
前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を前記第一のオペレーティングシステムの管理の下で強制終了させる、
ことを特徴とするコンピュータへの不正侵入対処方法。
（付記４）　通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムであって、
前記第一のオペレーティングシステムによる管理の下で実行され、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを行なう処理と、
前記アクセスに対する前記データサーバからの応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータの取得を行なう処理と、
を該コンピュータに行なわせる不正侵入対処プログラム。
（付記５）　前記アクセスを行なう処理は、前記データサーバへのアクセスを前記通信ネットワークを介して行なう処理を前記コンピュータに行なわせ、
前記判定を行なう処理は、前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう処理を前記コンピュータに行なわせる、

ことを特徴とする付記４に記載の不正侵入対処プログラム。
（付記６） 前記判定を行なう処理は、前記データサーバへのアクセスに対する応答が取得されなかったときには、前記アクセスに対する該データサーバからの応答が異常であるとの判定を下す処理をコンピュータに行なわせる付記４に記載の不正侵入対処プログラム。
（付記７） 前記判定を行なう処理は、前記データサーバへのアクセスに対する応答が、予め想定されている応答と異なるものであったときに前記アクセスに対する該データサーバからの応答が異常であるとの判定を下す処理をコンピュータに行なわせることを特徴とする付記４に記載の不正侵入対処プログラム。
（付記８） 前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる処理を更に前記コンピュータに行なわせることを特徴とする付記４に記載の不正侵入対処プログラム。
（付記９） 前記第二のオペレーティングシステムの実行を強制終了させた後に、前記第一のオペレーティングシステムによる管理の下で前記第二のオペレーティングシステムを改めて実行させると共に、該第二のオペレーティングシステムによる管理の下で前記アプリケーションプログラムを改めて実行させて前記データサーバを前記コンピュータで再構築させる処理を更に該コンピュータに行なわせることを特徴とする付記８に記載の不正侵入対処プログラム。
（付記１０） 前記コンピュータで再構築されたデータサーバへのアクセスに対する応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータに加えて、該データサーバの動作の履歴を取得する処理を更に該コンピュータに行なわせることを特徴とする付記９に記載の不正侵入対処プログラム。
（付記１１） 前記応答が異常であると判定したときに、該異常の発生を示す情報を所定の連絡先に宛てて送信する処理を更に前記コンピュータに行なわせることを特徴とする付記４に記載の不正侵入対処プログラム。
（付記１２） 前記異常の発生を示す情報を送信する処理は、前記データの取得を行なう処理によって取得されたデータを該異常の発生を示す情報に添付して送信する処理を前記コンピュータに行なわせることを特徴とする付記１１に記載の不正侵入対処プログラム。
（付記１３） 前記異常の発生を示す情報を送信する処理は、前記異常の発生を示す情報を所定の連絡先に宛てて送信すると共に、前記連絡先のうち予め選択されている一部の連絡先に宛てて送信する前記異常の発生を示す情報には前記データの取得を行なう処理によって取得されたデータを添付して送信する処理を前記コンピュータに行なわせることを特徴とする付記１１に記載の不正侵入対処プログラム。
（付記１４） 通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムであって、
前記第一のオペレーティングシステムによる管理の下で実行され、
前記データサーバへのアクセスを前記通信ネットワークを介して行なう処理と、
前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる処理と、
を該コンピュータに行なわせる不正侵入対処プログラム。
（付記１５） 通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させる

ことによって該コンピュータで構築される該データサーバに対する不正侵入に対処する不正侵入対処装置であって、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを前記第一のオペレーティングシステムによる管理の下で行なうアクセス手段と、
前記アクセスに対する前記データサーバからの応答が正常であるか異常であるかの判定を前記第一のオペレーティングシステムによる管理の下で行なう判定手段と、
前記応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータの取得を前記第一のオペレーティングシステムによる管理の下で行なうデータ取得手段と、
を有することを特徴とする不正侵入対処装置。

（付記１６） 通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する不正侵入対処装置であって、
前記コンピュータは、前記通信ネットワークを介して行なわれるデータの授受を管理するインタフェースを複数有し、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを前記第一のオペレーティングシステムによる管理の下で前記通信ネットワークを介して行なうアクセス手段と、
前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を前記第一のオペレーティングシステムによる管理の下で行なう判定手段と、
前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を前記第一のオペレーティングシステムによる管理の下で強制終了させる強制終了手段と、
を有することを特徴とする不正侵入対処装置。

（付記１７） 通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムを記録した記録媒体であって、
前記第一のオペレーティングシステムによる管理の下で該コンピュータで実行させることにより、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを行なう処理と、
前記アクセスに対する前記データサーバからの応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータの取得を行なう処理と、
を該コンピュータに行なわせることを特徴とする不正侵入対処プログラムを記録した記録媒体。

（付記１８） 通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムを記録した記録媒体であって、
前記第一のオペレーティングシステムによる管理の下で該コンピュータで実行させることにより、
前記データサーバへのアクセスを前記通信ネットワークを介して行なう処理と、

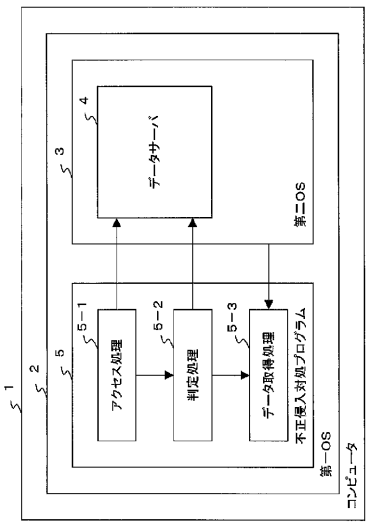
前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる処理と、
を該コンピュータに行なわせることを特徴とする不正侵入対処プログラムを記録した記録媒体。
（付記１９）　通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムを表現しており、搬送波に具現化されているコンピュータ・データ・シグナルであって、
前記第一のオペレーティングシステムによる管理の下で該コンピュータで実行させることにより、
前記アプリケーションプログラムの実行によって構築された前記データサーバへのアクセスを行なう処理と、
前記アクセスに対する前記データサーバからの応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記第二のオペレーティングシステムによって管理されているメモリに格納されているデータの取得を行なう処理と、
を該コンピュータに行なわせることを特徴とする不正侵入対処プログラムを表現しているコンピュータ・データ・シグナル。
（付記２０）　通信ネットワーク上でデータの公開を行なうデータサーバであって、コンピュータで実行される第一のオペレーティングシステムによる管理の下で実行される第二のオペレーティングシステムによる管理の下でアプリケーションプログラムを実行させることによって該コンピュータで構築される該データサーバに対する不正侵入に対処する処理を該コンピュータに行なわせる不正侵入対処プログラムを表現しており、搬送波に具現化されているコンピュータ・データ・シグナルであって、
前記第一のオペレーティングシステムによる管理の下で該コンピュータで実行させることにより、
前記データサーバへのアクセスを前記通信ネットワークを介して行なう処理と、
前記アクセスに対して前記データサーバから前記通信ネットワークを介して送られてくる応答が正常であるか異常であるかの判定を行なう処理と、
前記応答が異常であると判定したときに、前記アプリケーションプログラムの実行を管理している前記第二のオペレーティングシステムの実行を強制終了させる処理と、
を該コンピュータに行なわせることを特徴とする不正侵入対処プログラムを表現しているコンピュータ・データ・シグナル。
【００８５】
【発明の効果】
以上詳細に説明したように、本発明によれば、データサーバが構築されるコンピュータに残されている、データサーバへの不正侵入の痕跡を示す情報の取得が人手を介することなく行なえるようになり、あるいは、不正侵入されたデータサーバの動作を、人手を介することなく迅速に停止させることができるようになるという効果を奏する。
【図面の簡単な説明】
【図１】本発明の第一の原理構成を示す図である。
【図２】本発明の第二の原理構成を示す図である。
【図３】本発明を実施するＷｅｂサーバ装置のハードウェア構成を示す図である。
【図４】本発明を実施するＷｅｂサーバ装置の機能構成を示す図である。
【図５】不正侵入対処処理の処理内容を示すフローチャートである。
【図６】Ｗｅｂ文書データファイルの例を示す図である。

【図７】図６に示されているデータファイルの内容を示す図である。
【図８】改ざんされたＷｅｂ文書データファイルの例を示す図である。
【図９】図８に示されているデータファイルの内容を示す図である。
【図１０】乗っ取り改ざん対応処理の処理内容を示すフローチャートである。
【図１１】乗っ取り改ざん連絡処理の処理内容を示すフローチャートである。
【図１２】連絡先等設定ファイルのデータ例を示す図である。
【図１３】コンピュータで読み取ることの可能な記録媒体の例を示す図である。
【符号の説明】
１　コンピュータ
２　第一ＯＳ
３　第二ＯＳ
４　データサーバ
５　不正侵入対処プログラム
５－１　アクセス処理
５－２　判定処理
５－３　データ取得処理
５－４　強制終了処理
６　通信ネットワーク
１０　Ｗｅｂサーバ装置
１１　ＣＰＵ
１２　ＲＡＭ
１３　ＲＯＭ
１４　ＨＤＤ
１５　入力部
１６　出力部
１７　ＮＷインタフェースＡ
１８　ＮＷインタフェースＢ
１９　バス
２０　ホストＯＳ
２１　不正侵入対処プログラム
２１－１　比較監視部
２１－２　復旧処理部
２１－３　連絡処理部
２２　マスタＷｅｂ文書データ
２３　連絡先等設定ファイル
３０　ゲストＯＳ＿Ａ
３１　Ｗｅｂサーバａ
３２　Ｗｅｂ文書データａ
４０　ゲストＯＳ＿Ｂ
４１　Ｗｅｂサーバｂ
４２　Ｗｅｂ文書データｂ
５０　ハブＡ
６０　ハブＢ
７０　ルータＡ
８０　ルータＢ
９０　インターネット
１００１　コンピュータ
１００２　メモリ
１００３　可搬型記録媒体
１００４　通信回線

１００５　プログラムサーバ
１００６　記憶装置

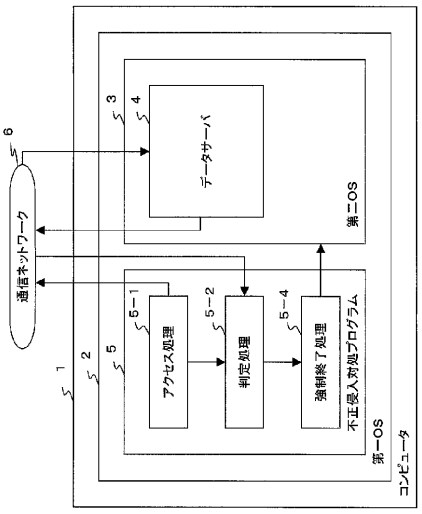
【図１】

本発明の第一の原理構成を示す図



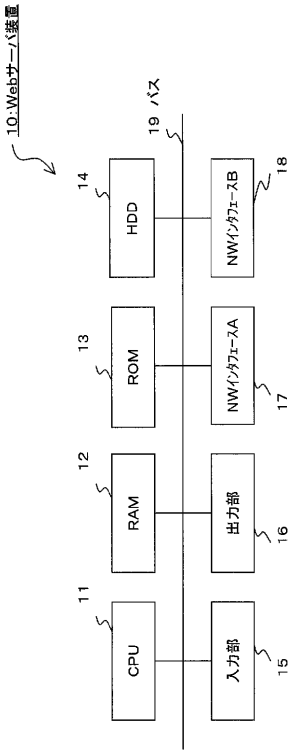

【図２】

本発明の第二の原理構成を示す図



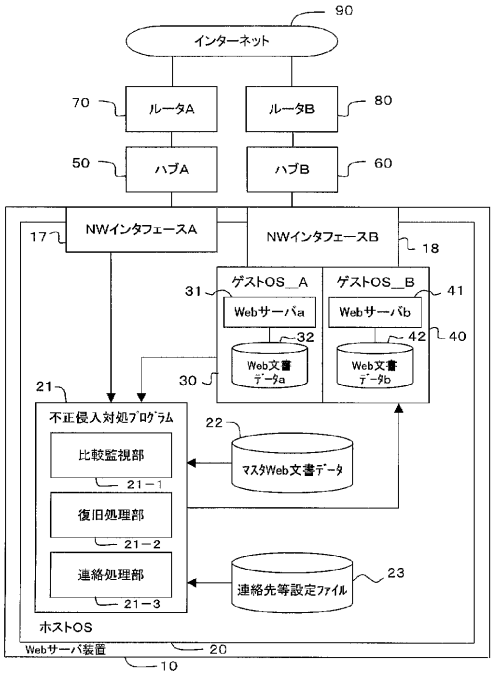
【図３】

本発明を実施するWebサーバ装置の
ハードウエア構成を示す図



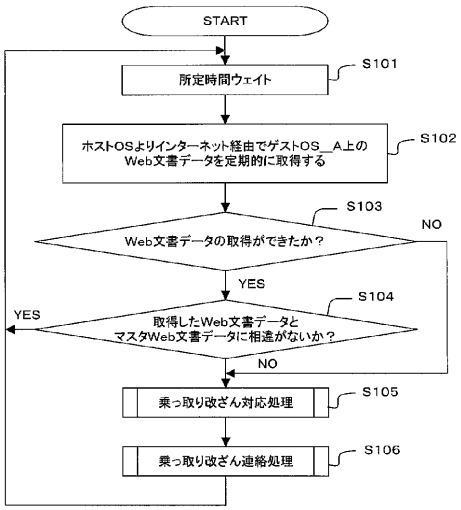

【図４】

本発明を実施するWebサーバ装置の機能構成を示す図




【図５】

不正侵入対処処理の処理内容を示すフローチャート




【図６】

Web文書データファイルの例を示す図

| path/filename | size | update |
|---|---|---|
| index. html | 91 | 2002. 01. 25. 11:29:00 |

【図７】

図6に示されているデータファイルの内容を示す図

```
<html>
<body>
<br><img SRC="title. gif" height=30 width=30>
Welcome!
</body>
</html>
```

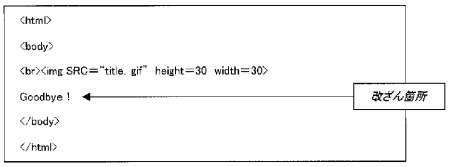
【図８】

改ざんされたWeb文書データファイルの例を示す図

| path/filename | size | update |
|---|---|---|
| index. html | 91 | 2002. 02. 09. 00:11:11 |

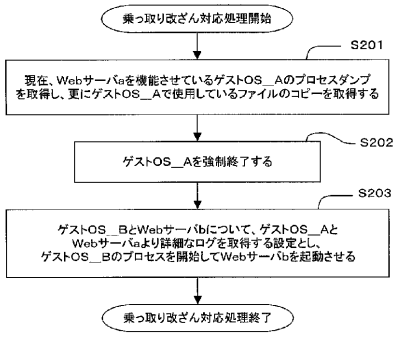
【図９】

図8に示されているデータファイルの内容を示す図



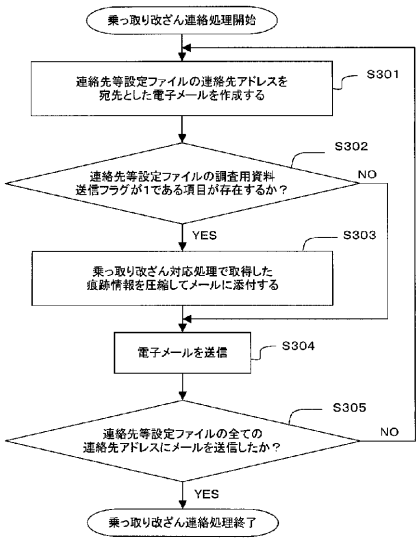

【図１０】

乗っ取り改ざん対応処理の処理内容を示すフローチャート




【図１１】

乗っ取り改ざん連絡処理の処理内容を示すフローチャート



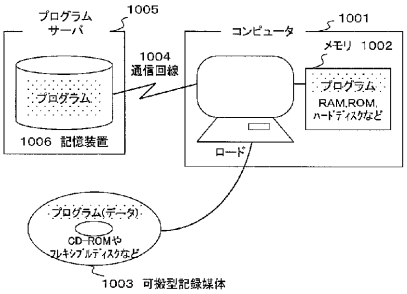

【図１２】

連絡先等設定ファイルのデータ例を示す図

| 連絡先アドレス | 調査用資料送信フラグ |
|---|---|
| admin@fijitsu.co.jp | 1 |
| 2ndadmin@fijitsu.co.jp | 0 |

【図１３】

コンピュータで読み取ることの可能な記録媒体の例を示す図



フロントページの続き

(56)参考文献 特開２００１－３３７８６４（ＪＰ，Ａ）
特開２００２－０３２２４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
G06F 11/34
G06F 13/00