(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2007-325275
(P2007-325275A)
(43)公開日　平成19年12月13日(2007.12.13)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	1/00	(2006.01)	H04N	1/00	107Z	5C062
H04N	1/44	(2006.01)	H04N	1/44		5C075
G09C	1/00	(2006.01)	G09C	1/00	660D	5J104

審査請求 未請求　請求項の数 12　ＯＬ　（全 14 頁）

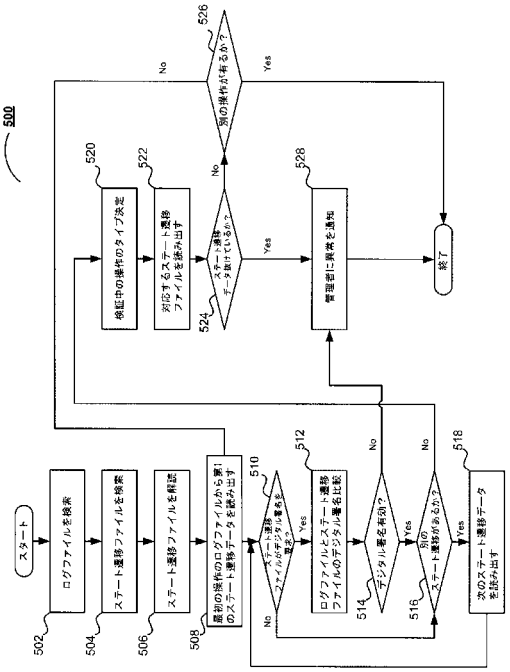
(21)出願番号　特願2007-147161 (P2007-147161)
(22)出願日　平成19年6月1日 (2007.6.1)
(31)優先権主張番号　11/446,910
(32)優先日　平成18年6月5日 (2006.6.5)
(33)優先権主張国　米国 (US)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(71)出願人　000003562
東芝テック株式会社
東京都品川区東五反田二丁目１７番２号
(74)代理人　110000235
特許業務法人　天城国際特許事務所
(72)発明者　ヤミ，サミール
アメリカ合衆国　カリフォルニア州　９２６０６　アーバイン　フラグストーン　２－３５８

最終頁に続く

(54)【発明の名称】画像処理装置の侵入検知システム及び方法

(57)【要約】
【課題】　画像処理装置に侵入した不正なアクセスを、画像処理装置で検知する。
【解決手段】　データ記憶装置１０８に、文書処理装置１０４の処理機能を定義するステート遷移データを暗号化してステート遷移ファイルとして保存する。文書処理装置１０４にアクセスされた操作のログファイルを、ステート遷移ファイルと比較する。ステート遷移ファイルに比べて、ログファイルにステート遷移データの抜けがある場合には、ログファイルが異常であり、侵入を検知する。
【選択図】図５



【特許請求の範囲】
【請求項１】
画像処理装置の処理機能のステート遷移を定義する実行可能コードを状態テーブルとして保存する記憶部と、
前記画像処理装置に実行中のステート遷移をモニタするためのモニタ部と、
前記モニタ部でモニタした前記ステート遷移を前記状態テーブルと比較する比較部と、
前記比較部による比較結果に従い、前記画像処理装置で前記実行中のステート遷移が許容不可能なステート遷移であることを表す出力を生成する生成部とを具備することを特徴とする画像処理装置の侵入検知システム。
【請求項２】
前記状態テーブルは、デジタル署名されることを特徴とする請求項１記載の画像処理装置の侵入検知システム。
【請求項３】
前記実行可能コードを暗号化して保存することを特徴とする請求項１又は請求項２記載の画像処理装置の侵入検知システム。
【請求項４】
前記比較部の比較結果が、前記モニタ部でモニタした前記ステート遷移のログファイルに記録されることを特徴とする請求項１乃至請求項３のいずれかに記載の画像処理装置の侵入検知システム。
【請求項５】
前記モニタ部でモニタした前記ステート遷移のログファイルへの変更中に許容不可能なステート遷移が生じることを特徴とする請求項１乃至請求項４のいずれかに記載の画像処理装置の侵入検知システム。
【請求項６】
署名が必要な前記実行可能コードのデジタル署名を生成して、前記比較部に送る署名生成部を更に有することを特徴とする請求項１記載の画像処理装置の侵入検知システム。
【請求項７】
画像処理装置の処理機能のステート遷移を定義する実行可能コードを状態テーブルとして保存するステップと、
前記画像処理装置に実行中のステート遷移をモニタするステップと、
前記モニタした前記ステート遷移を前記状態テーブルと比較するステップと、
前記比較するステップの比較結果に従い、前記画像処理装置で前記実行中のステート遷移が許容不可能なステート遷移であることを表す出力を生成するステップとを具備することを特徴とする画像処理装置の侵入検知方法。
【請求項８】
前記状態テーブルは、デジタル署名されることを特徴とする請求項７記載の画像処理装置の侵入検知方法。
【請求項９】
前記実行可能コードを暗号化して保存することを特徴とする請求項７又は請求項８記載の画像処理装置の侵入検知方法。
【請求項１０】
前記比較結果が、前記モニタした前記ステート遷移のログファイルに記録されることを特徴とする請求項７乃至請求項９のいずれかに記載の画像処理装置の侵入検知方法。
【請求項１１】
前記モニタした前記ステート遷移のログファイルへの変更中に許容不可能なステート遷移が生じることを特徴とする請求項７乃至請求項１０のいずれかに記載の画像処理装置の侵入検知方法。
【請求項１２】
前記モニタした前記ステート遷移を前記状態テーブルと比較するステップで使用するために、署名を必要とする前記実行可能コードのデジタル署名を生成するステップを更に有

することを特徴とする請求項７記載の画像処理装置の侵入検知方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はネットワーク等を介したデータ通信に係り、より詳細には画像処理装置への不正な侵入や改ざんをより確実に検知して、情報の保護を図る画像処理装置の侵入検知システム及び方法に関する。
【背景技術】
【０００２】
一般に文書処理装置等の画像処理装置では、情報の機密を保持し又不正な改ざん等から情報を保護するために、権限の無いユーザや不正侵入者が、装置やシステムにアクセスしたかどうかを検知できることが重要とされる。近年不正な侵入を検知するシステムとして、秘密キーを用い、或いはマシンの利用状況を検知して、ネットワークレベルで、不正な侵入を未然に検知するシステムがある。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、ネットワークレベルで不正な侵入者を検知するにもかかわらず、侵入検知システムを回避して、画像処理装置内に侵入し、或いは悪意のあることが判らないような不正なプログラムを画像処理装置に仕掛ける恐れがある。この様な不正な使用があった場合は、ネットワークレベルでは明らかな異常や侵入がないにもかかわらず、画像処理装置が損なわれてしまうおそれがある。例えば、文書処理装置の場合に権限の無いユーザが、保護されたプリント操作のパスワード検索要件を回避すれば、不正なプリント操作が可能となり、又データ伝送を不正に傍受すれば、プリント情報を侵入者に送信し或は後で又見るために保存することも可能となる。更により巧妙な侵入の場合には、侵入した形跡も残さずに、文書処理装置内の処理機能のステート遷移の状況を保存するステート遷移ファイルを改ざんしたりするおそれもある。
【０００４】
そこで本発明は上記課題を解決するものであり、不正な侵入者が、ネットワークレベルでの侵入検知システムをすり抜けた場合であっても、画像処理装置側で、不正な侵入や情報の傍受或いは改ざん等を検知することが可能であり、不正なアクセスにより画像形成装置を損なうことなく、画像処理装置の良好な稼動を保持することが出来る画像処理装置の侵入検知システム及び方法を提供することを目的とする。
【課題を解決するための手段】
【０００５】
本発明は上記課題を解決するための手段として、画像処理装置の処理機能のステート遷移を定義する実行可能コード状態テーブルとして保存する記憶部と、前記画像処理装置に実行中のステート遷移をモニタするためのモニタ部と、前記モニタ部でモニタした前記ステート遷移を前記状態テーブルと比較する比較部と、前記比較部による比較結果に従い、前記画像処理装置で前記実行中のステート遷移が許容不可能なステート遷移であることを表す出力を生成する生成部とを設けるものである。
【発明の効果】
【０００６】
本発明によれば、画像処理装置にアクセスのあった操作のステート遷移データを、画像処理装置にて利用可能なすべての処理機能の正規のステート遷移データと比較して、両者が違っていれば、画像処理装置への不正な侵入があったと検証する。従ってネットワークレベルでの侵入検知をすり抜けた不正アクセスであっても、画像処理装置側で検知することができる。また、ステート遷移ファイルを暗号化し、不正侵入時にステート遷移ファイルが改ざんされるのを防止して、ステート遷移ファイルの改ざんによる画像処理装置のシステムダウンを解消して、画像処理装置の有効稼動を得る。

【発明を実施するための最良の形態】
【０００７】
以下本発明の実施例を、図面を参照して説明する。図１は本発明の侵入検知システム１００を示す概略構成図である。侵入検知システム１００は、画像処理装置である少なくとも１台の文書処理装置１０４と、少なくとも１つのクライアント装置１１２を、分散処理環境を有する分散通信ネットワーク１０２で接続している。文書処理装置１０４と分散通信ネットワーク１０２は、通信リンク１１０を介して接続され、クライアント装置１１２と分散通信ネットワーク１０２は、通信リンク１１４を介して接続される。分散処理環境とは、分散通信ネットワーク１０２を介して、２台以上の電子装置間でデータを交換することができる環境のことである。
【０００８】
一般に分散通信ネットワーク１０２は、例えば、ローカル・エリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、パーソナルエリアネットワーク、仮想ネットワーク、イントラネット、インターネット、又はこれらの任意の組み合わせ等を含む。但しこれに限定されない。本実施例では、分散通信ネットワーク１０２は、例えば、トークンリング、８０２．１１（ｘ）、イーサネット（登録商標）、その他の有線又は無線データ通信機構などの、従来のデータ伝送機構によって例示されるような機構からなる。
【０００９】
文書処理装置１０４としては、多機能周辺装置(ＭＦＰ)がある。但し、これに限定されない。文書処理装置の各種文書処理機能としては、例えば、複写機能、プリント機能、スキャン機能、電子メール機能、文書管理機能、ファクシミリ機能等がある。又文書処理装置１０４は、Ｆｉｒｅｗｉｒｅドライブ、ＵＳＢドライブ、ＳＤ、ＭＭＣ、ＸＤ、コンパクトフラッシュ（登録商標）、メモリスティック等の各種携帯型記憶媒体を使用可能とするように装備される。又文書処理装置１０４は、ユーザとの直接対話を可能とするコントロールパネル上のタッチスクリーンインターフェースや液晶ディスプレイなどのユーザインターフェースを装備する。
【００１０】
通信リンク１１０、１１４は、ブルートゥース（Ｂｌｕｅｔｏｏｔｈ（登録商標））、ワイマックス（ＷｉＭａｘ）、８０２．１１ａ、８０２．１１ｂ、８０２．１１ｇ、８０２．１１（ｘ）、独自通信網、赤外線、光、公衆交換電話網、又は任意の無線データ伝送システムを含むがこれらに限らず、無線通信、或いは有線通信等での既知の任意の適切なデータ通信チャネルである。
【００１１】
文書処理装置１０４には、コントローラ１０６が動作可能に結合されている。コントローラ１０６は、任意のソフトウェア、ハードウェア又はこれらの組み合わせからなり、文書処理装置１０４に制御機能を提供する。コントローラ１０６は、文書処理装置１０４によってアクセスされた文書処理操作の履歴や内容を記録するステート遷移データを生成し保持させる等が可能である。更にコントローラ１０６は、後述する侵入検知時に、アクセスされたログファイルのステート遷移データと、正規のステート遷移ファイルのステート遷移データとを比較する比較部としての機能を有する。このためコントローラ１０６は、署名生成部にて、実行可能コード内の特定のデジタル署名を生成して、比較部に送る機能を有する。コントローラ１０６は文書処理装置１０４の内部に組み込んでも良いし、文書処理装置１０４の文書処理機構とは別に外部に設置しても良い。更にコントローラ１０６は、ログファイルのステート遷移データと、正規のステート遷移ファイルのステート遷移データとを比較した結果に基づいて、前記実行中のステート遷移が許容不可能なステート遷移であることを表す出力を生成する生成部として機能する。
【００１２】
記憶部であるデータ記憶装置１０８は、文書処理装置１０４上で実行可能な全ての文書処理機能のステート遷移を定義する実行可能コードを暗号化した状態テーブルであり、正規のステート遷移データのリスト又はテーブルである、ステート遷移ファイルを、実行可

能ファイルに保存する。更にモニタ部であるデータ記憶装置１０８は、実行済み或いは実行中の操作のステート遷移をモニタするために、文書処理装置１０４にアクセスした操作のステート遷移データのリスト又はテーブルであるログファイルを、アクセスファイルに保存する。データ記憶装置１０８は、ハードディスクドライブ、その他の磁気記憶装置、光学記憶装置、フラッシュメモリ素子、又はこれらの任意の組み合わせを含む任意の大容量記憶装置等である。但しこれに限定されない。データ記憶装置１０８は、図１に示すような独立の構成要素ではなく、例えば、内部ハードディスクドライブ等のように、文書処理装置１０４内部に組み込まれる内部記憶装置であっても良い。

【００１３】

クライアント装置１１２は、例えばラップトップコンピュータ等からなるが、これに限定されない。クライアント装置１１２は、文書処理操作を生成し、その操作を文書処理装置１０４に送信する。

【００１４】

次に図２に、侵入検知システム１００のコントローラ１０６および文書処理装置１０４のブロック図を示す。コントローラ１０６は、プロセッサ２０２、読み出し専用メモリ（ＲＯＭ）２０４、ランダム・アクセス・メモリ（ＲＡＭ）２０６、ストレージ・インターフェース２０８、ネットワーク・サブシステム２１０、ネットワーク・インターフェース２１４、ディスク２１６、無線インターフェース２１８を有している。プロセッサ２０２、読み出し専用メモリ２０４、ランダム・アクセス・メモリ２０６、ストレージ・インターフェース２０８、ネットワーク・インターフェース・サブシステム２１０はバス２１２で接続され、データ通信される。

【００１５】

プロセッサ２０２は、複数のプロセッサからなっても良く、後述する侵入検知のための各種機能の実施を制御する。

【００１６】

読み出し専用メモリ２０４は、ＢＩＯＳ機能、システム機能、システム構成データ、およびコントローラ１０６の操作に使用されるその他のルーチンまたはデータ等の静的データ又は固定のデータ又は指示のために使用される。

【００１７】

ランダム・アクセス・メモリ（ＲＡＭ）２０６は、ダイナミック・ランダム・アクセス・メモリ（ＤＲＡＭ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）、又はその他任意のアドレス書き込み可能なメモリ・システムから構成される。ランダム・アクセス・メモリ２０６は、プロセッサ２０２によって達成されるデータ取り扱いのための記憶領域及びアプリケーションに関するデータや指示のための記憶領域を提供する。

【００１８】

ストレージ・インターフェース２０８は、ディスクドライブ２１６等に、コントローラ１０６に関するデータを持久的に記憶し、大量または長期に記憶するための機能を提供する。ストレージ・インターフェース２０８は、ディスクドライブ２１６の他に例えば、光学ストレージ、テープドライブなどの任意の適切なアドレス可能な記憶装置や、シリアル・ストレージなどの大容量記憶装置等任意の記憶媒体を使用する。

【００１９】

ネットワーク・インターフェース・サブシステム２１０は、コントローラ１０６が他の装置と通信できるように、ネットワークからの入出力を適切に経路指定する。ネットワーク・インターフェース・サブシステム２１０は、例えば、イーサネット（登録商標）、トークンリング等の固定ネットワークまたは、有線ネットワークとのデータ通信のためのネットワーク・インターフェース・カード（ＮＩＣ)等のネットワーク・インターフェース２１４と接続される。ネットワーク・インターフェース・サブシステム２１０は、例えばワイファイ（ＷｉＦｉ）、その他、ワイマックス（ＷｉＭａｘ）、無線モデム、携帯ネットワーク等の無線通信システムを経由する無線通信のための無線インターフェース２１８と接続される。ネットワーク・インターフェース・サブシステム２１０は、任意のフィジ

カルまたはノンフィジカルなデータ転送レイヤまたはプロトコル・レイヤを利用する。例えばネットワーク・インターフェース２１４は、ローカル・エリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、またはそれらの組み合わせからなるフィジカルネットワーク２２０と相互に接続して、データを交換する。

【００２０】

バス２１２は、文書プロセッデジタル署名インターフェース２２２とデータ通信可能である。文書プロセッデジタル署名インターフェース２２２は、１つ又は複数の文書処理操作を実行するハードウェアである文書処理装置１０４との接続を提供する。文書処理装置１０４の文書処理操作には、コピーハードウェア２２４によって行われるコピー操作、スキャンハードウェア２２６によって行われるスキャン操作、プリントハードウェア２２８によって行われるプリント操作、及びファクシミリハードウェア２３０によって行われるファクシミリ通信操作等がある。コントローラ１０６の制御により各文書処理操作が実施される。

【００２１】

次に図３に示すコントローラ機能３００を用いて、侵入検知システム１００のコントローラ１０６による文書処理機能を説明する。図３は、図２に示すコントローラ１０６の機能を、ソフトウェア及びオペレーティングシステムに関連して示す説明図である。コントローラ機能３００は文書処理エンジン３０２、プリント機能部３０４、ファックス機能部３０６、スキャン機能部３０８、ジョブキュー３１２、ネットワークサービス機能部３１４、画像処理プロセッサ３１６及びジョブ解析部３１８を有する。

【００２２】

文書処理エンジン３０２は、プリント操作、コピー操作、ファクシミリ操作、及びスキャニング操作が可能である。これ等操作は多機能周辺装置（ＭＦＰ）により実施されることが多いがこれ等の操作機能を全て備えていなくても良く、一部の操作機能を実施するものであっても良い。

【００２３】

文書処理エンジン３０２は、ユーザインターフェース３１０に接続される。ユーザインターフェース３１０を使用してユーザ又は管理者は、文書処理エンジン３０２により制御される機能にアクセスすることができる。アクセスは、ローカルなインターフェースを介するか、リモートのシンクライアントまたはシッククライアントを介して、コントローラ１０６に対してなされる。

【００２４】

文書処理エンジン３０２は、プリント機能部３０４、ファックス機能部３０６、スキャン機能部３０８とデータ通信する。これらの装置は、文書情報のコピーやプリントに用いられ、プリント、ファクシミリ送受信、文書スキャンの実際の操作を容易にする。

【００２５】

ジョブキュー３１２は、プリンタ機能部３０４、ファックス通信機能部３０６及び画像走査機能部３０８とデータ通信する。画像走査機能部３０８とジョブキュー３１２とはビットマップ、ページ記述言語、ベクトル形式などの様々な画像形式が可能に接続される。

【００２６】

ジョブキュー３１２は、また、ネットワークサービス機能部３１４とデータ通信可能である。例えばジョブキュー３１２とネットワークサービス機能部３１４の間では、ジョブ制御、ステート遷移データ、又は電子文書データが通信される。

【００２７】

又コントローラ機能３００に対しては、任意のシンクライアントまたはシッククライアントであるクライアントネットワークサービス３２０を介して、ネットワークベースでアクセスするための、インターフェースが提供される。クライアントネットワークサービス３２０は、ウェブサービスアクセスは、ハイパーテキスト転送プロトコル、ファイル転送プロトコル、ユニフォームデータダイアグラムプロトコル、及びその他、任意の交換機構を介して行われる。また、ネットワークサービス機能部３１４は、ＦＴＰ、電子メール、

及びＴＥＬＮＥＴなどを介した通信のために、クライアントネットワークサービス３２０とのデータのやり取りを提供する。従って、コントローラ機能３００は、様々なネットワークアクセス機構を介した電子文書及びユーザ情報の入出力を容易にする。

【００２８】

又ジョブキュー３１２は、画像プロセッサ３１６とデータ通信可能にセットされる。画像プロセッサ３１６は、電子文書を、プリント機能部３０４或いは、ファックス機能部３０６などの操作機能と通信する形式に変換するためのラスタ画像処理部、ページ記述言語インタープリタ等の機構である。

【００２９】

更にジョブキュー３１２は、ジョブ解析部３１８とデータ通信する。ジョブ解析部３１８は、クライアント装置サービス３２２などの外部装置からプリントジョブ言語ファイルを受け取る。クライアント装置サービス３２２は、プリント機能部３０４、ファックス機能部３０６、その他コントローラ機能３００によって処理可能な電子文書等を入力する。ジョブ解析部３１８は、受信した電子文書ファイルを解析して、それを、コントローラ機能３００の該当する構成要素にて処理するために、ジョブキュー３１２に通信する。

【００３０】

上記侵入検知システム１００にて、データ記憶装置１０８に保存される全ての正規のステート遷移データは、拡張マークアップ言語ファイルで保存される。又、正規のステート遷移データは、不正な改ざんを防止するために暗号化される。更にステート遷移ファイルは、修正する権限を有するユーザだけにアクセスを限定するように設定される。又ステート遷移ファイルは、権限を有しない人による改ざんを防止するために、システム管理者によって指示され、認証のために要求される、特定のデジタル署名を、必要に応じて有する。更にデータ記憶装置１０８は、不正な侵入をモニタし検知するために、文書処理装置１０４にアクセスされたプロセスに関するログファイルを、データ記憶装置１０８内に有している。

【００３１】

ログファイルへのステート遷移データの書き込みは、文書処理装置１０４へのアクセスによるステート遷移データを受け取った後に、ステート遷移データに固有識別子を割り当てることにより行われる。ステート遷移データに固有識別子を割り当てた後、ステート遷移データにデジタル署名が必要であると指示されているかどうかが判定される。ステート遷移データにデジタル署名の必要が無い場合、アクセスされたステート遷移データは、アクセスされた操作に関するログファイルに記憶される。

【００３２】

ステート遷移データにデジタル署名が必要であると指示されている場合、アクセスされたステート遷移データに対して所定のデジタル署名が為された後に、デジタル署名とステート遷移データとが、ログファイルに記録される。このプロセスは、アクセスされた操作の全てのステート遷移データに実行されるまで繰り返される。

【００３３】

即ち、文書処理装置１０４にアクセスされる各種操作は、文書処理装置１０４で定義される実行形式のコードである、ステート遷移データを有すべきものであり、アクセスした操作の完了は、文書処理装置１０４で定義される実行形式のコードの実行の完了と一致し、その結果ログファイルが生成され、データ記憶装置１０８に記録される。即ち、文書処理装置１０４にアクセスされる一連の全ての操作はモニタされて、アクセスされた操作のステート遷移データは、データ記憶装置１０８のログファイルに保存される。

【００３４】

従って、権限の無い者による文書処理装置１０４への侵入の解析と検出は、文書処理装置１０４へのアクセスによる操作の実行中に生成されるログファイルを使用して行われる。ログファイルを解析して、アクセスの異常、即ち侵入の形跡を検知するために、コントローラ１０６、その他ハードウェア、ソフトウェア、或はこれらの組み合わせは、データ記憶装置１０８と連動して、ステート遷移ファイルとログファイルを検索する。これ等は

、文書処理装置１０４のコントローラ１０６を使用して行われるが、侵入検知のための検索或いは解析は、コントローラ１０６に限定されず、例えばデータ記憶装置１０８に接続される他の任意の管理装置等で実施することも可能である。

【００３５】

更にステート遷移ファイルは、権限の無い不正なアクセスによる改ざんを防ぐために暗号化されている。従って、コントローラ１０６は、ステート遷移ファイルに記憶された正規のステート遷移リスト又はテーブルにアクセスするためには先ずステート遷移ファイルを解読する必要がある。解析を行うため、コントローラ１０６は操作に関する暗号化された正規のステート遷移ファイルを解読した後、ステート遷移データをステート遷移ファイルから読み出すことが出来る。この様にして、ステート遷移ファイル内の正規のステート遷移データを一行ずつ検索する。最初の正規のステート遷移データを検索したら、コントローラ１０６は、正規のステート遷移データがデジタル署名を要求するものかどうかを判定する。デジタル署名が必要で無い場合、コントローラ１０６は、ステート遷移ファイルから次の正規のステート遷移データを検索し、続いてそのステート遷移データがデジタル署名を要求するかどうかを順次判定する。

【００３６】

ステート遷移データがデジタル署名を要求するものである場合、コントローラ１０６は、正規のステート遷移データのデジタル署名を生成して、アクセスされたステート遷移データに付与されたデジタル署名を、データ記憶装置１０８に記憶された正規のステート遷移データのデジタル署名と比較する。デジタル署名が一致しなければ、システム管理者にエラー通知を出力し、ログファイルに記録する。デジタル署名が一致したら、コントローラ１０６は、現在検証中の操作に関するログファイルに、まだ他にステート遷移データが残っているかどうかを判定する。まだ他のステート遷移データが残っていれば、次のステート遷移データを検索して、上記プロセスを繰り返す。ステート遷移データが残っていなければ、コントローラ１０６は、ログファイルから、アクセスされた操作のタイプ(コピー操作タイプ、プリント操作タイプ、ファックス操作タイプ等）を決定して、実行可能ファイルから、アクセスされた操作のタイプに対応するステート遷移ファイルの正規のステート遷移データをすべて読み出す。読み出された正規のステート遷移データに対して、ログファイルのステート遷移データが、例えば１つ或は複数のステップが抜けている等して、改ざんが判明した場合には、管理者に通知が送られ、ログファイルに記録される。この後、コントローラ１０６は、次の操作を検索して、同様に解析を続ける。

【００３７】

リアルタイムでアクセスの解析と不正な侵入を検知する際に、侵入検知システム１００は、コントローラ１０６、その他のソフトウェア、ハードウェア、ソフトウェア／ハードウェア組み合わせを使用して、ログファイルを継続的にモニタする。モニタは、文書処理装置１０４により実行される新規のアクセスの操作を実行した後に行われる。本実施例では侵入検知システム１００にて、コントローラ１０６をリアルタイムでモニタを行う構成要素として使用しているが、文書処理装置１０４とデータ通信可能であり、リアルタイムで侵入検知を等しく実行できる管理装置等を使用しても良い。

【００３８】

リアルタイムでの検証時、コントローラ１０６は、管理者等により設定された所定の時間が経過すると、アクセスファイルに記録されたログファイルを収集する。最後に検証されたアクセスの固有識別子が、ログファイルに含まれている。最後に検証された固有識別子を使用して、コントローラ１０６は、アクセスファイルを検索して、文書処理装置１０４にアクセスされ、実行される次の操作を探す。次の操作とは、固有識別子により時間順に実行される、次の操作のことである。コントローラ１０６は、アクセスファイルから次の操作のログファイルのステート遷移データを検索し、ステート遷移ファイルの正規のステート遷移データとの比較を行う。ログファイルとステート遷移ファイルのステート遷移データのデジタル署名が一致しないという判定であれば、それに基づいて前記実行中のステート遷移が許容不可能なステート遷移であることを表す出力であり、ログファイルが不

正な侵入であるとの出力通知が生成されて、例えば管理者に送られる。他方デジタル署名が有効な場合は、ログファイルとステート遷移ファイルとを比較して、両者のステート遷移データが一致していないかどうか判定する。１つ又は複数のステート遷移データが一致しないときは、その旨の通知が生成され、例えば、管理者に送られるか、或はログファイルに記録される。両者のステート遷移データが一致するとコントローラ１０６が判定したときは、次の操作である、現在アクセス中の操作が、最後に検証された操作のログファイルとしてアクセスファイルに保存される。次いで、侵入検知システム１００は元に戻って新しい操作を待機する。

【００３９】

次に図４のフローチャート４００を参照して、コントローラ１０６による、文書処理装置１０４にアクセスされる操作に関するステート遷移データの生成について説明する。文書処理装置１０４に任意の文書処理操作のアクセスが開始されると、コントローラ１０６は、前のステートから別のステートに遷移した旨を表すステート遷移データを受け取る（ステップ４０２）。次に、受け取ったステート遷移データに固有識別子を割り当てる（ステップ４０４）。ステート遷移データのデジタル署名判定を問い合わせる（ステップ４０６）。記憶装置に暗号化された形で記憶されたステート記憶ファイルの問い合わせは、先ず解読しなければならない。ステップ４０８でステート遷移データにデジタル署名するかを判定する。

【００４０】

ステップ４０８でステート遷移データにデジタル署名しないと判定したら、ステート遷移データをログファイルに保存する（ステップ４１０）。ステート遷移ファイルがデジタル署名される時は、ステップ４１２に進み、ステート遷移ファイルから取り出した指示に従って、ステート遷移データにデジタル署名する。次にデジタル署名されたステート遷移データをログファイルに保存する（ステップ４１４）。即ち、文書処理装置１０４に文書処理操作がアクセスされると、モニタのために、図４に示すフローに従い、アクセスを記録するステート遷移データが、デジタル署名されているかどうかに関係なく、全てログファイルに保存される。図４に従いログファイルを更新出来、その結果、アクセスファイル内には、順次多数のモニタデータが生成される。

【００４１】

次に図５のフローチャート５００を参照して、侵入検知方法について述べる。侵入検知をスタートして、先ずステップ５０２で、文書処理装置１０４へのアクセスのログファイルを検索する。ログファイルは、デジタル署名されたデータを含むものもある。次にステップ５０４で、データ記憶装置１０８から、ステート遷移ファイルを検索する。ステート遷移ファイルは、特定のデジタル署名されたデータを含む他に、権限の無いユーザによる改ざんからステート遷移ファイルを保護するために暗号化形式でデータ記憶装置１０８に保存される。適切な暗号化方法は、例えば、解読キーを有している。次に、ステップ５０６でステート遷移ファイルが解読され、コントローラ１０６による侵入検知のために準備される。

【００４２】

ステップ５０８で、アクセスファイル内の、最初の操作に対応するログファイルから第１のステート遷移データを読み出す。次にステップ５１０で、ステート遷移ファイルがデジタル署名を要求しているかどうか、即ち、検証中のステート遷移データにデジタル署名すべきかどうかを判定する。ステート遷移データにデジタル署名が必要であると判定された場合、ステップ５１２に進み、ログファイル内のデジタル署名と実行可能ファイル内のステート遷移ファイルのデジタル署名と比較する。ステップ５１４で、ログファイルのデジタル署名が有効かどうかを判定する。ステップ５１４でデジタル署名が有効で無いと判定された場合、ステップ５２８に進み、管理者にデジタル署名が有効で無い旨の通知が送られ、管理者に異常を通知する。この異常の通知は、例えば、ＭＦＰのコントロールパネル上のタッチスクリーンインターフェースや液晶ディスプレイに警告表示し或は、音声等で警告する。

【００４３】
ステップ５１４でデジタル署名が有効と判定された場合、ステップ５１６に進み、ログファイル内に別のステート遷移があるかどうか判定する。別のステート遷移データがログファイルに残っている時には、ステップ５１８に進み、ログファイルから次のステート遷移データを読み出す。ログファイル内の次のステート遷移データを読み出した後、ステップ５１０に戻り、次のステート遷移データにデジタル署名が必要かどうかを判定し、前述と同様に操作する。
【００４４】
一方ステップ５１６で、他のログファイルが残っていないと判定した場合は、ステップ５２０に進み、検証中の操作のタイプが決定される。即ち、文書処理装置１０４にて実行可能な文書処理機能のタイプ（コピー操作タイプ、プリント操作タイプ或は、ファクシミリ操作タイプ）に対して、文書処理機能のステート遷移を定義する実行可能コードが決定される。処理機能のタイプによって、必然的にステート遷移ファイル内にあるべき正規のステート遷移データが指定される。従ってコントローラ１０６は、次にステップ５２２で、アクセスされた処理機能に対応するステート遷移ファイルを実行可能ファイルから読み出す。次にステップ５２４で、アクセスのログファイルを検証して、ログファイルからステート遷移データが抜けていないかどうかを判断する。即ち、コントローラ１０６は、実行可能ファイルに記憶されていて、現在検証中の操作のタイプにあるはずのステート遷移ファイルを、検証中解析の操作に対応するログファイルと比較する。
【００４５】
１つ或は複数のステート遷移データが抜けている場合には、検証中のログファイルが異常であり、侵入の可能性を知らせる通知を管理者に送る（ステップ５２８）。検証中のログファイルにステート遷移データの抜けが無い場合は、侵入が無かったものと判断し、ステップ５２６に進み、別の操作のログファイルが在るか判定する。別の操作がある場合、ステップ５０８に戻り、次の操作の第１のステート遷移データをログファイルから読み出し、前述と同様に侵入検知される。ログファイル内に別の操作がもう残っていない場合、侵入検知操作を終了する。本実施例ではコントローラ１０６により侵入を解析し検知しているが、コントローラ１０６に限定されず、例えば管理装置、パーソナルコンピュータ等の処理装置によって実行することも可能である。
【００４６】
これにより、コントローラ１０６は、ネットワークレベルでの侵入検知をすり抜けて、文書処理装置１０４に侵入したアクセスのログファイルを、実行可能ファイルのステート遷移ファイルと比較して、ステート遷移データが抜けている場合には、検証中のログファイルが異常であり、侵入の可能性があったと検知できる。しかもステート遷移ファイル中のステート遷移データは、暗号化されているので、文書処理装置１０４に対して不正侵入があったとしてもステート遷移ファイルが改ざんされるのを防御できる。
【００４７】
次に図６のフローチャート６００を参照して、侵入検知をリアルタイムで行う方法について述べる。このフローチャートでは、コントローラ１０６や文書処理装置１０４等の侵入検知のための構成要素は、文書処理装置１０４が新しい操作を実行するのを待機する（ステップ６０２）。コントローラ１０６は、管理者等に指定された所定の時間を待機したら、ステップ６０４に進みログファイルを読み出す。但しこのリアルタイムでの侵入検知は、これに限らず、例えば、コントローラ１０６が、任意の文書処理操作の完了を検知し或いは、ログファイルに新たなステート遷移データが記録されたことを検知した場合に、ステップ６０４で、ログファイルを読み出すようにしても良い。
【００４８】
ログファイルを読み出した後、ステップ６０６に進み、最後に侵入の有無が検証された（最も最近検証された）操作の固有識別子をアクセスファイルから読み出す。固有識別子は、次に、最後に検証された操作に続く、アクセスファイル内の次の操作を決定する（ステップ６０８）。次の操作とは、文書処理装置１０４に文書処理操作を実行され、ログフ

ァイルに記録された操作の次に続く操作或いは、時間的に最も近い次の操作を指す。次に、ログファイルに記録されるデジタル署名を、ステート遷移ファイルに保存された特定のデジタル署名と比較する（ステップ６１０）。

【００４９】

前述のステップ５１４と同様にして、デジタル署名が有効かどうかを判定し（ステップ６１２）、デジタル署名が有効で無い場合、ステップ６２０に進み、管理者にデジタル署名が有効で無い旨が通知され、異常の検知が通知される。ステップ６１２でデジタル署名が有効な場合、ステップ６１４に進み、現在の操作タイプ対応する正規のステート遷移データをステート遷移ファイルから読み出す。ステート遷移ファイルの内容により示されるように、次にステップ６１６で、本来あるべきステート遷移データが、１つ又は複数、ログファイルから抜けていないかどうかを判断する。１つ或は複数のステート遷移データが抜けている場合、ステップ６２０に進み、ログファイルが異常であり、侵入の可能性があることを管理者に報告する。即ち、ステップ６１６で、ステート遷移データが抜けていると判断されると、ステップ６２０にて、リアルタイムでアクセス中、即ちログファイルへ変更中の操作が、許可不可能とされる。ステップ６１６で、ログファイルからステート遷移データが抜けていない場合は、ステップ６１８に進み、現在の操作が、検証済みの最後の操作としてログファイルに保存され、ログファイルが変更される。

【００５０】

この後フローはステップ６０２に戻り、コントローラ１０６は、文書処理装置１０４への新しい操作のアクセスを待つ。

【００５１】

これによりコントローラ１０６は、例えば現在の操作のログファイルについて、リアルタイムに、不正な侵入であるか否かを検証できる。従って管理者等は、文書処理装置１０４への不正な侵入検知後直ちに現在アクセス中の操作を不許可とする等の対策を講じることが可能となる。

【００５２】

この実施例によれば、不正な侵入や改ざんを検知する際の判断の基準とするために、文書処理装置１０４の全ての処理機能のステート遷移を定義する、暗号化した正規のステート遷移データのステート遷移ファイルをデータ記憶装置１０８に保存しておく。文書処理装置１０４にアクセスした操作のログファイルを、ステート遷移ファイルと比較して、ログファイルからステート遷移データが抜けている場合には、ログファイルが異常であり、侵入の可能性を検知することが出来る。従って、ネットワークレベルでの侵入検知をすり抜けて、文書処理装置１０４に不正な侵入があったとしても、文書処理装置１０４にて、不正な侵入を検知できる。更にステート遷移ファイルのステート遷移データを暗号化しているので、不正侵入があったとしても、正規のステート遷移データが改ざんされるのを防御でき、改ざんによる文書処理装置１０４のシステムダウンを防止して、文書処理装置１０４の良好な稼動を得ることが出来る。

【００５３】

尚本発明の侵入検知システムの構成は限定されず、クライアント装置は、ウェブ対応の任意の端末装置であり、例えば、コンピュータワークステーション、パーソナルコンピュータ、携帯情報端末、携帯電話、スマートフォン等であっても良いし、又クライアントの数も限定されない。

【００５４】

更に画像処理装置にて侵入検知を行うには、テート遷移を定義する実行可能コードを暗号化してなくても良いが、暗号化することにより、もしも画像処理装置に侵入があった場合でも、実行可能コードが改ざんされる恐れが低減される。

【００５５】

又本実施例では、侵入検知のための機能が侵入検知システムのコントローラ内に予め記録されている場合で説明をしたが、これに限らず、同様の機能のコンピュータプログラムをネットワーク等の伝達手段から侵入検知システム内にダウンロードしても良いし、同様

の機能を記録媒体に記憶させたものを、画像処理装置にインストールしても良い。記録媒体としては、ＣＤ－ＲＯＭ等の光学記録媒体或はフロッピー（登録商標）ディスク等の磁気記録媒体等、プログラムを記憶でき、且つクライアントが読み取り可能な記録媒体であれば、その形態はいずれの形態であっても良い。またこのように予めインストールやダウンロードにより得る機能は、クライアント内部のＯＳ（オペレーティング・システム）等と協動してその機能を実現させるものであっても良い。

【図面の簡単な説明】

【００５６】

【図１】本発明の実施例の侵入検知システムを示す概略ブロック図である。

【図２】本発明の実施例の文書処理装置及びコントローラの構成を示す概略ブロック図である。

【図３】本発明の実施例のコントローラ機能を示す概略説明図である。

【図４】本発明の実施例にてステート遷移データの生成を示すフローチャートである。

【図５】本発明の実施例にて侵入検知を示すフローチャートである。

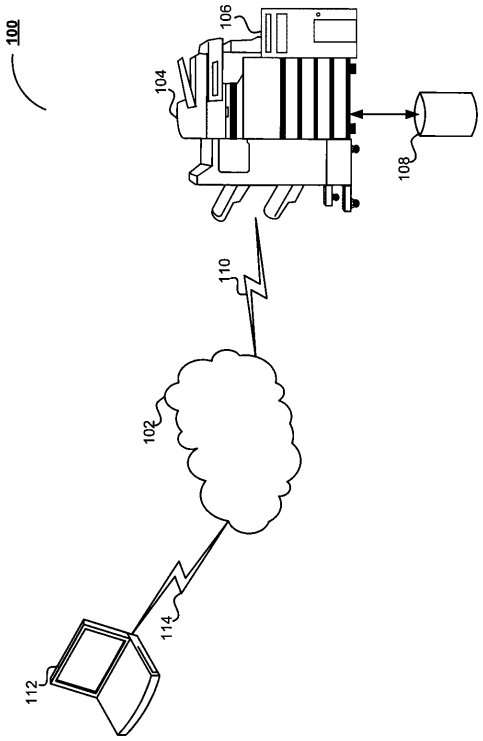
【図６】本発明の実施例にてリアルタイムでの侵入検知を示すフローチャートである。

【符号の説明】

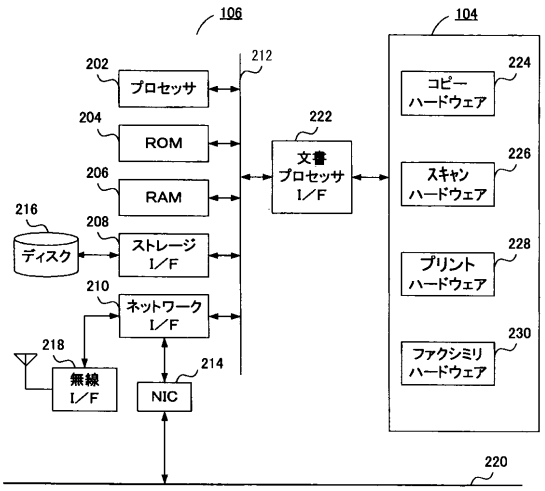
【００５７】

１００…侵入検知システム
１０２…分散通信ネットワーク
１０４…文書処理装置
１０６…コントローラ
１０８…データ記憶装置
１１０、１１４…通信リンク

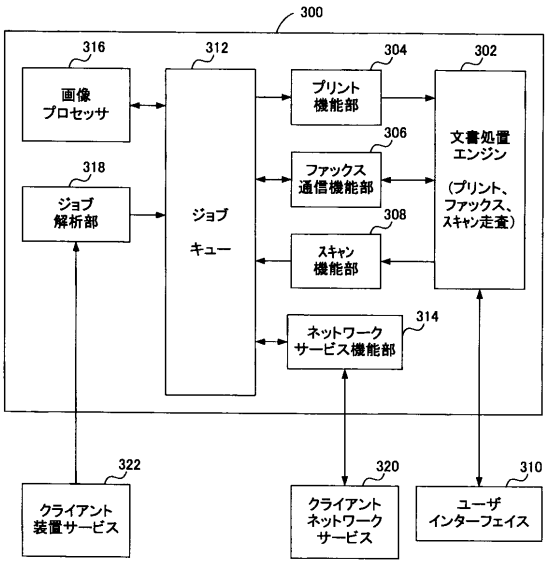
【図１】



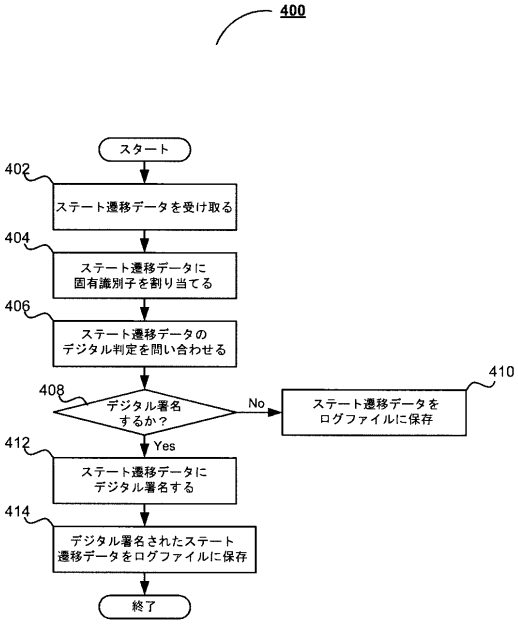
【図２】



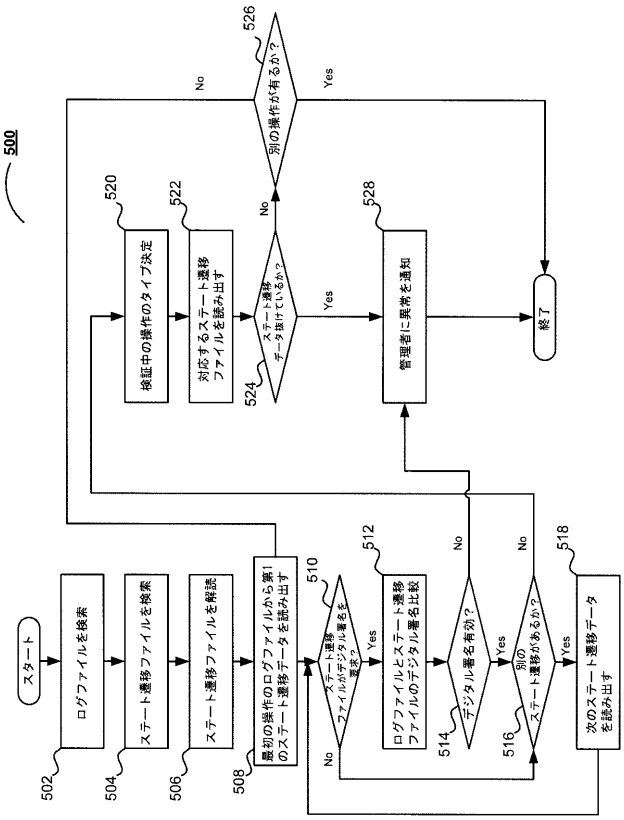
【図３】


300
316
画像
プロセッサ
318
ジョブ
解析部
312
ジョブ
キュー
304
プリント
機能部
306
ファックス
通信機能部
308
スキャン
機能部
314
ネットワーク
サービス機能部
302
文書処置
エンジン
(プリント、
ファックス、
スキャン走査)
322
クライアント
装置サービス
320
クライアント
ネットワーク
サービス
310
ユーザ
インターフェイス

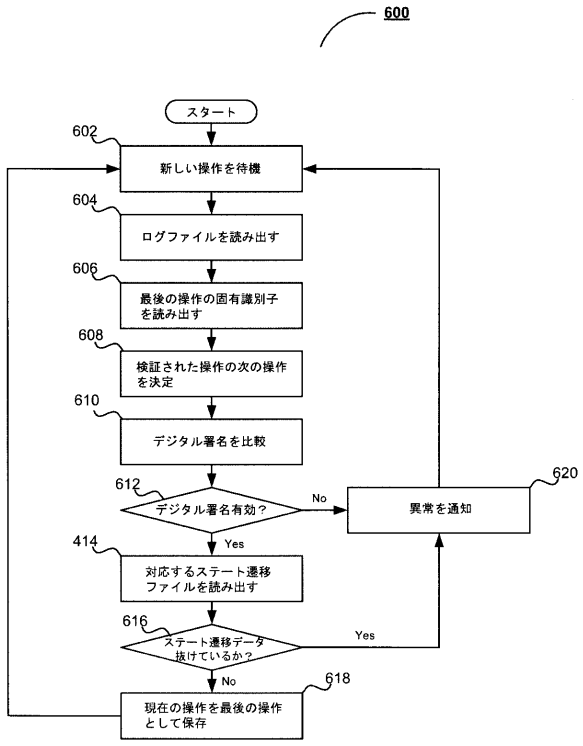
【図４】


400
スタート
402
ステート遷移データを受け取る
404
ステート遷移データに
固有識別子を割り当てる
406
ステート遷移データの
デジタル判定を問い合わせる
408
デジタル署名
するか？
No
410
ステート遷移データを
ログファイルに保存
Yes
412
ステート遷移データに
デジタル署名する
414
デジタル署名されたステート
遷移データをログファイルに保存
終了

【図５】


500
526
別の操作が有るか？
No
Yes
520
検証中の操作のタイプ決定
522
対応するステート遷移
ファイルを読み出す
ステート遷移
データ抜けているか？
524
528
管理者に異常を通知
終了
スタート
ログファイルを検索
502
ステート遷移ファイルを検索
504
ステート遷移ファイルを解読
506
最初の操作のログファイルから第1
のステート遷移データを読み出す
508
510
ステート遷移
ファイルがデジタル署名を
含む？
512
ログファイルとステート遷移
ファイルのデジタル署名比較
514
デジタル署名有効？
516
別の
ステート遷移があるか？
518
次のステート遷移データ
を読み出す

【図６】


600
スタート
602
新しい操作を待機
604
ログファイルを読み出す
606
最後の操作の固有識別子
を読み出す
608
検証された操作の次の操作
を決定
610
デジタル署名を比較
612
デジタル署名有効？
No
620
異常を通知
Yes
414
対応するステート遷移
ファイルを読み出す
616
ステート遷移データ
抜けているか？
Yes
No
618
現在の操作を最後の操作
として保存

フロントページの続き

(72)発明者　トラン，ピーター
アメリカ合衆国　カリフォルニア州　９２８４３　ガーデン　グローブ　シャーリー　ストリート　１３８０１－５６

Ｆターム(参考) 5C062 AA02 AA05 AA33 AA35 AB17 AB42 AC02 AC22 AC34 AF14
AF15
5C075 AB90 EE02 EE03
5J104 AA08 AA12 EA08 EA10 JA03 JA21 LA01 LA02 LA03 LA06
NA02 NA27 NA38 PA14