

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4651310号
(P4651310)

(45) 発行日 平成23年3月16日(2011.3.16)

(24) 登録日 平成22年12月24日(2010.12.24)

(51) Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F 12/14	560C	
G06Q 50/00	(2006.01)	G06F 17/60	108	
G06K 19/07	(2006.01)	G06K 19/00	H	
G06K 19/073	(2006.01)	G06K 19/00	P	

請求項の数 5 (全 20 頁)

(21) 出願番号	特願2004-170365 (P2004-170365)	(73) 特許権者	000005223 富士通株式会社
(22) 出願日	平成16年6月8日(2004.6.8)		神奈川県川崎市中原区上小田中4丁目1番1号
(65) 公開番号	特開2005-352600 (P2005-352600A)	(74) 代理人	100078868 弁理士 河野 登夫
(43) 公開日	平成17年12月22日(2005.12.22)	(72) 発明者	坂梨 利廣 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
審査請求日	平成18年11月16日(2006.11.16)	(72) 発明者	林 俊祐 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72) 発明者	三沢 伴恒 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 情報改竄検知システム、非接触型記録媒体、情報改竄検知方法及びコンピュータプログラム

(57) 【特許請求の範囲】

【請求項1】

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、複数の処理オブジェクトの実行完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知システムにおいて、

前記非接触型記録媒体は、

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得する手段と、
取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、

生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録する手段と

取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護する手段とを備え、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するよう構成してあることを特徴とする情報改竄検知システム。

【請求項2】

データを読み書きすることが可能なＩＣチップ及び無線でデータを送受信することが可能な無線通信手段を備え、複数の処理オブジェクトを実行する都度、順次パリティデータを生成して記録する非接触型記録媒体において、

各処理オブジェクトに関する情報を各処理オブジェクトの実行時に取得する手段と、
取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、

生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録する手段と

取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護する手段とを備え、

10

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトに対応するパリティデータを生成するよう構成してあることを特徴とする非接触型記録媒体。

【請求項 3】

所定の処理オブジェクトでパリティデータを生成した場合、該所定の処理オブジェクトより前の処理オブジェクトに関する情報の読出し及び書込みを禁止するよう構成してあることを特徴とする請求項 2 記載の非接触型記録媒体。

【請求項 4】

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、すべての処理オブジェクト完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知方法において、

20

前記非接触型記録媒体は、

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得し、
取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成し、

生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録し、

取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護し

30

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成することを特徴とする情報改竄検知方法。

【請求項 5】

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、すべての処理オブジェクトの実行完了時に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知するよう、非接触でデータを読み書きすることが可能な非接触型記録媒体を機能させる非接触型記録媒体で実行することが可能なコンピュータプログラムにおいて、

40

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得するステップと、

取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成するステップと、

生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録するステップと、

取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護するステップとを含み、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクト

50

より前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するようにしてあることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、複数の処理オブジェクトを有するアプリケーションで、各処理オブジェクトを実行する都度、正常に処理が行われた旨を示すパリティデータを生成してＩＣタグ等の非接触型記録媒体に書き込み、すべての処理オブジェクトの実行が完了した時点で記録されているパリティデータに基づいて、中途の処理オブジェクトでデータの改竄が行われたか否かを確認することができる情報改竄検知システム、非接触型記録媒体、情報改竄検知方法及びコンピュータプログラムに関する。

10

【背景技術】

【0002】

昨今、様々な生産工程、流通工程を経て商品が消費者の手許に届くことから、商品の品質の確保、模造品の排除等の観点から、商品の製造から廃棄までの履歴情報を管理する重要性が高まっている。一般に商品は、製造されてから廃棄されるまで複数の生産工程、流通工程を経由することから、商品毎に履歴情報を記憶することができる非接触型ＩＣタグを用い、各生産工程、流通工程を経由する都度、履歴情報を書き込むことで、商品毎のライフサイクルを管理する商品ライフサイクル管理システムが多々開発されている。

20

【0003】

非接触型ＩＣタグは、ネットワーク等の通信手段と接続されており、演算及び演算結果を記憶するＩＣチップを内蔵し、ＩＣタグに集約された膨大な情報を複数の管理者・複数の事業拠点で共有することができる。

【0004】

例えば、商品、荷物、車両等に、従来のバーコードと同様にＩＣタグを付与した状態で生産工程、流通工程等を流通又は移動させ、各処理工程に固定された無線通信用のアンテナ及び読み取り装置によって、必要なときに必要な情報の取り出し／書き換えを行うことが可能になる。

【0005】

30

これにより、該商品がどこから出荷され、どの配送ルートを通してどれだけの時間をかけて運ばれたのか、その履歴に関する情報をすべて非接触型ＩＣタグに記録することができ、商品毎のライフサイクルを容易に把握することが可能となる。

【0006】

上述のような商品ライフサイクル管理システムとして、例えば特許文献１には、非接触ＩＣタグが付された物品が、複数のステージを流通し、流通するステージ毎に秘密情報をＩＣタグに記録することが可能な非接触ＩＣタグを用いたアクセスシステムが開示されており、ＩＣタグに記録されている情報を、必要な者が必要な時に入手することができるよう構成されている。

【0007】

40

また、特許文献２には、ＩＣタグ（識別情報に限定したＩＤタグ）での情報の取り出し／書き換えが正常に行われたか否かを検証するための改竄検知符号を属性情報とともに付加し、商品の生産工程、流通工程における情報の改竄を検知することができる管理システムが開示されており、複数の工程を経由する場合におけるＩＣタグの記録情報の信頼性を高めることが可能となっている。

【特許文献１】特開２００１－３０７０５５号公報

【特許文献２】特開２００２－２４７６７号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

50

しかし、上述した従来の商品ライフサイクル管理システムでは、ＩＣタグに記録する秘密情報、あるいは改竄検知符号等は、各生産工程、流通工程毎に付与されており、各工程において正常な処理が行われたか否かを判断することはできても、複数の工程間の処理順序が正しいか否かを判断することができないという問題点があった。すなわち、本来Ａ、Ｂ、Ｃの順に処理を行う必要がある生産工程において、誤ってＡ、Ｃ、Ｂの順で処理を行った場合、ＩＣタグに記録されている情報からは、正しい順序で処理されたか否かを判断することができず、生産工程によっては規格外となっている商品でも、正常な商品として出荷されてしまうおそれが残されていた。

【０００９】

また、各工程で記録される情報が悪意ある第三者に漏洩した場合、各生産工程、流通工程毎に誤った情報を記録させることが容易となり、複数の工程を経由する場合におけるＩＣタグの記録情報の信頼性を維持することができないという問題点もあった。

【００１０】

すなわち、例えばある生産工程が正常に行われなかった場合に、記録すべきそれ以降の生産工程で正常に行われなかった生産工程を特定する手段がなく、特にブランドの信用が確立された商品等では、生産工程、物流工程のすべてに関係する業者の信用に関わる問題に発展する。

【００１１】

本発明は斯かる事情に鑑みてなされたものであり、複数の処理工程に対応する処理オブジェクトのどこで情報の改竄が行われて非接触型記録媒体に記録されたかを、改竄が行われた処理オブジェクト以降に実行する処理オブジェクトで検知することができる情報改竄検知システム、非接触型記録媒体、情報改竄検知方法及びコンピュータプログラム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】

【００１２】

上記目的を達成するために第１発明に係る情報改竄検知システムは、複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、複数の処理オブジェクトの実行完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知システムにおいて、前記非接触型記録媒体は、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得する手段と、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録する手段と、取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護する手段とを備え、所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するよう構成してあることを特徴とする。

【００１３】

第１発明に係る情報改竄検知システムでは、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報だけでなく、該処理オブジェクトより前に実行した他の処理オブジェクトで生成されたパリティデータを用いて、該処理オブジェクトのパリティデータを生成する。これにより、２番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正値と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【００１４】

10

20

30

40

50

また、第2発明に係る非接触型記録媒体は、データを読み書きすることが可能なICチップ及び無線でデータを送受信することが可能な無線通信手段を備え、複数の処理オブジェクトを実行する都度、順次パリティデータを生成して記録する非接触型記録媒体において、各処理オブジェクトに関する情報を各処理オブジェクトの実行時に取得する手段と、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録する手段と、取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護する手段とを備え、所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトに対応するパリティデータを生成するよう構成してあることを特徴とする。

10

【0015】

第2発明に係る非接触型記録媒体では、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報だけでなく、該処理オブジェクトより前に実行した他の処理オブジェクトで生成されたパリティデータを用いて、該処理オブジェクトのパリティデータを生成する。これにより、2番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正値と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

20

【0016】

また、第3発明に係る非接触型記録媒体は、第2発明において、所定の処理オブジェクトでパリティデータを生成した場合、該所定の処理オブジェクトより前の処理オブジェクトに関する情報の読み出し及び書き込みを禁止するよう構成してあることを特徴とする。

【0017】

第3発明に係る非接触型記録媒体では、処理オブジェクトでパリティデータを生成した場合、該処理オブジェクトより前に実行した処理オブジェクトに関する情報については、非接触型記録媒体からの読み出し及び情報を更新するための書き込みを禁止する。これにより、任意の処理オブジェクトでは、非接触型記録媒体から該処理オブジェクトより前に実行した処理オブジェクトで生成したパリティデータしか読出すことができず、既に行った処理オブジェクトについて新たにパリティデータを生成することを未然に防止することが可能となる。

30

【0018】

また、第4発明に係る情報改竄検知方法は、複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、すべての処理オブジェクト完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知方法において、前記非接触型記録媒体は、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得し、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成し、生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録し、取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護し、所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成することを特徴とする。

40

【0019】

第4発明に係る情報改竄検知方法では、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報だけでなく、該処理オブジェクトより前に実行した他の処理オブジェ

50

クトで生成されたパリティデータを用いて、該処理オブジェクトのパリティデータを生成する。これにより、2番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正值と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【0020】

また、第5発明に係るコンピュータプログラムは、複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、すべての処理オブジェクトの実行完了時に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知するよう、非接触でデータを読み書きすることが可能な非接触型記録媒体を機能させる非接触型記録媒体で実行することが可能なコンピュータプログラムにおいて、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得するステップと、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成するステップと、生成したパリティデータを、処理オブジェクトの識別情報に対応付けて記録するステップと、取得した各処理オブジェクトに関する情報を第三者が読み出し不可となるように保護するステップとを含み、所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するようにしてあることを特徴とする。

【0021】

第5発明に係るコンピュータプログラムでは、各処理オブジェクトの実行時に、該処理オブジェクトに関する情報だけでなく、該処理オブジェクトより前に実行した他の処理オブジェクトで生成されたパリティデータを用いて、該処理オブジェクトのパリティデータを生成する。これにより、2番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正值と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【発明の効果】

【0022】

第1発明、第2発明、第4発明及び第5発明によれば、2番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正值と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【0023】

第3発明によれば、任意の処理オブジェクトでは、非接触型記録媒体から該処理オブジェクトより前に実行した処理オブジェクトで生成したパリティデータしか読出すことができず、既に行した処理オブジェクトについて新たにパリティデータを生成することを未然に防止することが可能となる。

【発明を実施するための最良の形態】

【0024】

10

20

30

40

50

(実施の形態1)

以下、本発明の実施の形態1に係る情報改竄検知システムについて図面に基づいて具体的に説明する。図1は、本発明の実施の形態1に係る情報改竄検知システムの構成を示すブロック図である。本実施の形態1では、地理的に離れた4つの工場を経由して、非接触型記録媒体であるICタグ4を付した商品を製造する。すなわち、4つの工場がそれぞれ処理オブジェクトに相当し、1つの処理オブジェクトの実行が完了した後、ICタグ4を付した商品を次の工場へと移送し、順次処理オブジェクトを実行する。本社に備えた中央装置1と、4つの工場に備えた端末装置2、2、・・・とは、インターネット3等の通信手段を介して相互にデータを送受信することが可能に接続されており、各工場に備えた端末装置2、2、・・・とICタグ4とは、非接触でデータを送受信することが可能となっている。なお、工場の本数は4つに限定されるものではなく、中央装置1も本社に設置されていることに限定されるものではない。

10

【0025】

中央装置1は、各工場の端末装置2、2、・・・がICタグ4から読み取ったデータ、及び各処理オブジェクトで発生する情報を集約し、パリティデータの値に基づいて、各処理オブジェクトにおいて正常に実行されているか否かを検証する。

【0026】

図2は、本発明の実施の形態1に係る情報改竄検知システムの中央装置1の構成を示すブロック図である。中央装置1は、少なくとも、CPU(中央演算装置)11、記憶手段12、RAM13、インターネット3等の外部の通信手段と接続する通信インタフェース14、入力手段15、出力手段16及びDVD、CD等の可搬型記録媒体18を用いる補助記憶手段17で構成される。

20

【0027】

CPU11は、内部バス19を介して中央装置1の上述したようなハードウェア各部と接続されており、上述したハードウェア各部を制御するとともに、記憶手段12に記憶されている処理プログラム、例えば各処理オブジェクトに関する情報に基づいて生成したパリティデータが正しいか否かを検証するプログラム等に従って、種々のソフトウェアの機能を実行する。

【0028】

記憶手段12は、内蔵される固定型記憶装置(ハードディスク)、ROM等で構成され、通信インタフェース14を介した外部のコンピュータ、又はDVD、CD-ROM等の可搬型記録媒体18から取得した、中央装置1として機能させるために必要な処理プログラムを記憶している。記憶手段12は、処理プログラムだけではなく、インターネット3等のネットワークを介して接続してある端末装置2、2、・・・を識別する情報に対応付けて、処理オブジェクトの実行完了時に生成されるべきパリティ値を記憶してある。

30

【0029】

RAM13は、DRAM等で構成され、ソフトウェアの実行時に発生する一時的なデータを記憶する。通信インタフェース14は内部バス19に接続されており、インターネット3等と通信することができるよう接続することにより、処理に必要とされるデータを送受信する。

40

【0030】

入力手段15は、画面上に表示された単語を選択するマウス等のポインティングデバイス、又は画面上でテキストデータを打鍵により入力するキーボード等である。出力手段16は、画像を表示出力する液晶表示装置(LCD)、表示ディスプレイ(CRT)等の表示装置である。

【0031】

補助記憶手段17は、CD、DVD等の可搬型記録媒体18を用い、記憶手段12へ、CPU11が処理するプログラム、データ等をダウンロードする。また、CPU11が処理したデータをバックアップすべく書き込むことも可能である。

【0032】

50

図3は、本発明の実施の形態1に係る情報改竄検知システムの端末装置2の構成を示すブロック図である。端末装置2は、少なくとも、CPU(中央演算装置)21、記憶手段22、RAM23、インターネット3等の外部の通信手段と接続する通信インタフェース24、入力手段25、出力手段26、及び非接触型記録媒体であるICタグ4とデータを送受信することができるICタグリーダ/ライタ27で構成される。

【0033】

CPU21は、内部バス28を介して端末装置2の上述したようなハードウェア各部と接続されており、上述したハードウェア各部を制御するとともに、記憶手段22に記憶されている処理プログラム、例えば非接触型記録媒体であるICタグ4から読み取ったデータに基づいて新たにパリティデータを算出し、ICタグ4へ書き込むプログラム等に従って、種々のソフトウェア的機能を実行する。

10

【0034】

記憶手段22は、内蔵される固定型記憶装置(ハードディスク)、ROM等で構成され、通信インタフェース24を介した外部のコンピュータ、又はDVD、CD-ROM等の可搬型記録媒体から取得した、端末装置2として機能させるために必要な処理プログラムを記憶している。記憶手段22は、処理プログラムだけではなく、ICタグ4がパリティデータを算出するのに必要な処理オブジェクトに関する情報、例えば製品を識別する情報、加工時間、加工工場を識別する情報、工程番号等を記憶してある。

【0035】

RAM23は、DRAM等で構成され、ソフトウェアの実行時に発生する一時的なデータを記憶する。通信インタフェース24は内部バス28に接続されており、インターネット3等と通信することができるよう接続することにより、処理に必要とされるデータを送受信する。

20

【0036】

入力手段25は、画面上に表示された単語を選択するマウス等のポインティングデバイス、又は画面上でテキストデータを打鍵により入力するキーボード等である。出力手段26は、画像を表示出力する液晶表示装置(LCD)、表示ディスプレイ(CRT)等の表示装置である。

【0037】

ICタグリーダ/ライタ27は、非接触型記録媒体であるICタグ4と無線で通信を行い、ICタグ4に対して、記憶手段22に記憶してある処理オブジェクトに関する情報を送信して書き込み、ICタグ4で算出されて記録されているパリティデータを読み出して記憶手段22に記憶する。

30

【0038】

図4は、本発明の実施の形態1に係る情報改竄検知システムで用いるICタグ4の構成を示すブロック図である。ICタグ4は、少なくとも、ICチップ41及び無線通信手段42を備えており、ICチップ41は、演算部411、記憶部412、電源整流部413、及び送受信部414を含んでいる。無線通信手段42はICチップ41の送受信部414と接続してあるコイル状のアンテナ421であり、アンテナ421を介してデータを送受信する。

40

【0039】

アンテナ421が、ICタグリーダ/ライタ27からの電波信号を受信した場合、アンテナ421のアンテナ線がコイル状であることから共振作用により起電力が発生する。発生した起電力によりICチップ41が起動し、記憶部412に記憶されている情報を信号化するとともに、送受信部414から受信した信号に基づいて演算部411で演算処理を実行し、演算結果を記憶部412へ記憶する。演算部411は、記憶部412に記憶した演算結果を、送受信部414を介して、アンテナ421からICタグリーダ/ライタ27へ送信する。

【0040】

図5は、本発明の実施の形態1に係る情報改竄検知システムで用いるICタグ4のIC

50

チップ41の処理手順を示すフローチャートである。ICタグ4を端末装置2のICタグリーダー/ライタ27に接近させた場合、ICチップ41は誘導起電力により起動し、ICタグリーダー/ライタ27から送信されてきた処理オブジェクトに関する情報を受け取る(ステップS501)。ICチップ41が受け取る処理オブジェクトに関する情報は、例えば製品を識別する情報、加工時間、加工工場を識別する情報、工程番号等を含む。

【0041】

ICチップ41は、記憶してある既に実行が完了している処理オブジェクトで算出したパリティデータを読み出し(ステップS502)、読み出したパリティデータと、ICタグリーダー/ライタ27から受け取った処理オブジェクトに関する情報とに基づいて、新たにパリティデータを算出する(ステップS503)。

10

【0042】

本実施の形態1では、処理オブジェクト毎に端末装置2を設けている。各処理オブジェクトの実行が完了した時点で、作業者は、ICタグ4を端末装置2のICタグリーダー/ライタ27に接近させる。ICタグ4は、ICタグリーダー/ライタ27を介して、ICタグリーダー/ライタ27を備えた端末装置2に対応する処理オブジェクトに関する情報を取得し、記憶してある既に実行が完了している処理オブジェクトのパリティデータとともに、該処理オブジェクトのパリティデータを算出する。

【0043】

図6は、本発明の実施の形態1に係る情報改竄検知システムで用いるパリティデータ算出方法の説明図である。最初の処理オブジェクト1の実行時には、処理オブジェクト1に関する情報 D_1 に基づいて、パリティデータ P_1 を処理オブジェクト1に関する情報 D_1 の関数 $f(D_1)$ として算出する。

20

【0044】

2番目の処理オブジェクト2の実行時には、処理オブジェクト2に関する情報 D_2 と、既に算出してあるパリティデータ P_1 とを用いて、処理オブジェクト2のパリティデータ P_2 を算出する。すなわち、パリティデータ P_2 は、処理オブジェクト2に関する情報 D_2 とパリティデータ P_1 の関数 $f(P_1, D_2)$ として算出する。

【0045】

以下、4つの処理オブジェクトの実行が完了するまで、順次同様の手順でパリティデータを算出する。一般に、 n 番目(n は自然数)の処理オブジェクト n の実行時には、処理オブジェクト n に関する情報 D_n と、既に算出してあるパリティデータ P_1, P_2, \dots, P_{n-1} とを用いて、処理オブジェクト n のパリティデータ P_n を算出する。すなわち、パリティデータ P_n は、(数1)に示すように、処理オブジェクト n に関する情報 D_n とパリティデータ P_1, P_2, \dots, P_{n-1} の関数 $f(P_1, P_2, \dots, P_{n-1}, D_n)$ として算出する。

30

【0046】

(数1)

$$P_n = f(P_1, P_2, \dots, P_{n-1}, D_n)$$

【0047】

ICチップ41は、算出したパリティデータを処理オブジェクトを識別する情報と対応付けて記憶し(ステップS504)、記憶してあるパリティデータを端末装置2へ送信する(ステップS505)。

40

【0048】

該処理オブジェクトに関する情報は、ICタグ4を入手した第三者が読出すことができないように、読出し不可となるよう設定する(ステップS506)。図6では、ハッチングをかけている部分が、第三者による読出しが不可となるよう保護している領域を示している。第三者が読み出すことができないようにする方法は、特に限定されるものではなく、セキュリティロックをかける方法であっても良いし、ICチップ41から消去する方法であっても良い。

【0049】

50

このようにすることで、ICタグ4を不正に入手した第三者は、パリティデータを算出しようと試みた場合であっても、各処理オブジェクトに関する情報を取得することができず、正しいパリティデータを算出することができないことから、データの改竄等の不正行為を未然に防止することが可能となる。

【0050】

ICタグ4から算出したパリティデータを受信した端末装置2のCPU21は、パリティデータを記憶手段22に記憶し、通信インタフェース24を介して中央装置1へ送信する。中央装置1へ送信するタイミングは特に限定されるものではなく、例えば中央装置1からの取得要求信号を受信したタイミングであっても良いし、一定時間間隔で中央装置1に対して送信するものであっても良い。

10

【0051】

図7は、本発明の実施の形態1に係る情報改竄検知システムの中央装置1のCPU11の処理手順を示すフローチャートである。中央装置1のCPU11は、各処理オブジェクトにつき、順次、適正に実行が完了した場合に算出されるべきパリティデータの適正値を事前に算出し、記憶手段12に記憶しておく(ステップS701)。

【0052】

図8は、中央装置1の記憶手段12に記憶するパリティデータのデータ構成の例示図である。図8に示すように、処理オブジェクトの実行を順次完了する都度、算出したパリティデータを処理オブジェクトを識別する情報、例えば処理オブジェクト番号に対応付けて記憶しておく。

20

【0053】

CPU11は、最後の処理オブジェクトの実行が完了した時点で、端末装置2から送信された最後のパリティデータを取得する(ステップS702)。そして、CPU11は、事前に算出して記憶手段12に記憶してあるパリティデータの適正値と、取得したパリティデータとが一致しているか否かを判断する(ステップS703)。

【0054】

CPU11が両者が一致していると判断した場合(ステップS703: YES)、処理オブジェクトは適正に実行されたものと判断し、処理を終了する。

【0055】

CPU11が両者が一致していないと判断した場合(ステップS703: NO)、CPU11は端末装置2から、前回パリティデータを取得した処理オブジェクトの直前の処理オブジェクトの実行完了時のパリティデータを取得し(ステップS704)、記憶手段12に記憶してあるパリティデータの適正値と、取得したパリティデータとが一致しているか否かを判断する(ステップS705)。

30

【0056】

CPU11が両者が一致していると判断した場合(ステップS705: YES)、適正値と一致するパリティデータを取得した処理オブジェクトの次に実行した処理オブジェクトで不正な処理が実行されたものと判断し、該処理オブジェクトを識別する情報を出力手段16へ出力する(ステップS706)。CPU11が両者が一致していないと判断した場合(ステップS705: NO)、CPU11は、ステップS704へ戻す。

40

【0057】

以下、同様にパリティデータの比較処理を行うことにより、どの処理オブジェクトで不正な処理が実行されたか、特定することができ、出力手段16への出力によって確認することが可能となる。

【0058】

以上のように本実施の形態1によれば、2番目に実行する処理オブジェクト以降の処理オブジェクトは、それより前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正値と異

50

なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【0059】

(実施の形態2)

以下、本発明の実施の形態2に係る情報改竄検知システムについて図面に基づいて具体的に説明する。実施の形態2に係る情報改竄検知システムの構成は実施の形態1と同様であることから、同一の符号を付することで詳細な説明は省略する。本実施の形態2は、パリティデータの生成方法が実施の形態1と相違する。

【0060】

図9は、本発明の実施の形態2に係る情報改竄検知システムで用いるICタグ4のICチップ41の処理手順を示すフローチャートである。ICタグ4を端末装置2のICタグリーダー/ライター27に接近させた場合、ICチップ41は誘導起電力により起動し、ICタグリーダー/ライター27から送信されてきた処理オブジェクトに関する情報を受け取る(ステップS901)。ICチップ41が受け取る処理オブジェクトに関する情報は、例えば製品を識別する情報、加工時間、加工工場を識別する情報、工程番号等を含む。

10

【0061】

ICチップ41は、記憶してある既に実行が完了している処理オブジェクトで算出したパリティデータのうち、直前に実行した処理オブジェクトで算出したパリティデータのみを読み出し(ステップS902)、読み出したパリティデータと、ICタグリーダー/ライター27から受け取った処理オブジェクトに関する情報とに基づいて、新たにパリティデータを算出する(ステップS903)。

20

【0062】

本実施の形態2でも、処理オブジェクト毎に端末装置2を設けている。各処理オブジェクトの実行が完了した時点で、作業者は、ICタグ4を端末装置2のICタグリーダー/ライター27に接近させる。ICタグ4は、ICタグリーダー/ライター27を介して、ICタグリーダー/ライター27を備えた端末装置2に対応する処理オブジェクトに関する情報を取得し、記憶してある既に実行が完了している処理オブジェクトのうち、直前に算出したパリティデータ、すなわち直前に実行した処理オブジェクトで算出したパリティデータとともに、該処理オブジェクトのパリティデータを算出する。

30

【0063】

図10は、本発明の実施の形態2に係る情報改竄検知システムで用いるパリティデータ算出方法の説明図である。最初の処理オブジェクト1の実行時には、処理オブジェクト1に関する情報 D_1 に基づいて、パリティデータ P_1 を処理オブジェクトに関する情報 D_1 の関数 $f(D_1)$ として算出する。

【0064】

2番目の処理オブジェクト2の実行時には、処理オブジェクト2に関する情報 D_2 と、既に算出してあるパリティデータ P_1 とを用いて、処理オブジェクト2のパリティデータ P_2 を算出する。すなわち、パリティデータ P_2 は、処理オブジェクト2に関する情報 D_2 とパリティデータ P_1 の関数 $f(P_1, D_2)$ として算出する。

【0065】

3番目の処理オブジェクト3の実行時には、処理オブジェクト3に関する情報 D_3 と、既に算出してあるパリティデータのうち、直前に算出したパリティデータ P_2 とを用いて、処理オブジェクト3のパリティデータ P_3 を算出する。すなわち、パリティデータ P_3 は、処理オブジェクト3に関する情報 D_3 とパリティデータ P_2 の関数 $f(P_2, D_3)$ として算出する。

40

【0066】

以下、4つの処理オブジェクトの実行が完了するまで、順次同様の手順でパリティデータを算出する。一般に、 n 番目(n は自然数)の処理オブジェクト n の実行時には、処理オブジェクト n に関する情報 D_n と、既に算出してあるパリティデータ P_1 、 P_2 、 \dots 、 P_{n-1} のうち、直前に実行した処理オブジェクト($n-1$)で算出したパリティデータ P

50

$n-1$ を用いて、処理オブジェクト n のパリティデータ P_n を算出する。すなわち、パリティデータ P_n は、(数2)に示すように、処理オブジェクト n に関する情報 D_n とパリティデータ P_{n-1} の関数 $f(P_{n-1}, D_n)$ として算出する。

【0067】

(数2)

$$P_n = f(P_{n-1}, D_n)$$

【0068】

ICチップ41は、算出したパリティデータを処理オブジェクトを識別する情報と対応付けて記憶し(ステップS904)、記憶してあるパリティデータを端末装置2へ送信する(ステップS905)。

10

【0069】

該処理オブジェクトに関する情報は、ICタグ4を入手した第三者が読出すことができないように、読出し不可となるよう設定する(ステップS906)。同様に、直前に実行した処理オブジェクトより前に実行した処理オブジェクトで算出したパリティデータについても、ICタグ4を入手した第三者が読出すことができないように、読出し不可となるよう設定する(ステップS907)。

【0070】

図10では、ハッチングをかけている部分が、第三者による読出しが不可となるよう保護している領域を示している。実施の形態1とは異なり、既に実行が完了している処理オブジェクトに関する情報に加えて、既に実行が完了している処理オブジェクトで算出したパリティデータも、第三者による読出しができないよう設定する。第三者が読み出すことができないようにする方法は、特に限定されるものではなく、セキュリティロックをかける方法であっても良いし、ICチップ41から消去する方法であっても良い。

20

【0071】

このようにすることで、ICタグ4を不正に入手した第三者は、パリティデータを算出しようとした場合であっても、各処理オブジェクトに関する情報だけでなく、既に実行された処理オブジェクトで算出したパリティデータも取得することができず、正しいパリティデータを算出することができないことから、データの改竄等の不正行為を未然に防止することが可能となる。

【0072】

30

ICタグ4から算出したパリティデータを受信した端末装置2のCPU21は、パリティデータを記憶手段22に記憶し、通信インタフェース24を介して中央装置1へ送信する。中央装置1へ送信するタイミングは特に限定されるものではなく、例えば中央装置1からの取得要求信号を受信したタイミングであっても良いし、一定時間間隔で中央装置1に対して送信するものであっても良い。

【0073】

図11は、本発明の実施の形態2に係る情報改竄検知システムの中央装置1のCPU11の処理手順を示すフローチャートである。中央装置1のCPU11は、各処理オブジェクトにつき、順次、適正に実行が完了した場合に算出されるべきパリティデータの適正値を事前に算出し、記憶手段12に記憶しておく(ステップS1101)。なお、中央装置1の記憶手段12に記憶するパリティデータのデータ構成は、実施の形態1と同様、処理オブジェクトの実行を順次完了する都度、算出したパリティデータを処理オブジェクトを識別する情報、例えば処理オブジェクト番号に対応付けて記憶しておく。

40

【0074】

CPU11は、最後の処理オブジェクトの実行が完了した時点で、端末装置2から送信された最後のパリティデータを取得する(ステップS1102)。そして、CPU11は、事前に算出して記憶手段12に記憶してあるパリティデータの適正値と、取得したパリティデータとが一致しているか否かを判断する(ステップS1103)。

【0075】

CPU11が両者が一致していると判断した場合(ステップS1103: YES)、処

50

理オブジェクトは適正に実行されたものと判断し、処理を終了する。

【 0 0 7 6 】

C P U 1 1 が両者が一致していないと判断した場合（ステップ S 1 1 0 3 : N O ）、C P U 1 1 は端末装置 2 から、前回パリティデータを取得した処理オブジェクトの直前の処理オブジェクトの実行完了時のパリティデータを取得し（ステップ S 1 1 0 4 ）、記憶手段 1 2 に記憶してあるパリティデータの適正值と、取得したパリティデータとが一致しているか否かを判断する（ステップ S 1 1 0 5 ）。

【 0 0 7 7 】

C P U 1 1 が両者が一致していると判断した場合（ステップ S 1 1 0 5 : Y E S ）、適正值と一致するパリティデータを取得した処理オブジェクトの次に実行した処理オブジェクトで不正な処理が実行されたものと判断し、該処理オブジェクトを識別する情報を出力手段 1 6 へ出力する（ステップ S 1 1 0 6 ）。C P U 1 1 が両者が一致していないと判断した場合（ステップ S 1 1 0 5 : N O ）、C P U 1 1 は、ステップ S 1 1 0 4 へ戻す。

【 0 0 7 8 】

以下、同様にパリティデータの比較処理を行うことにより、どの処理オブジェクトで不正な処理が実行されたか、特定することができ、出力手段 1 6 への出力によって確認することが可能となる。

【 0 0 7 9 】

以上のように本実施の形態 2 によれば、2 番目に実行する処理オブジェクト以降の処理オブジェクトは、その直前に実行した処理オブジェクトで生成したパリティデータを参照して新たなパリティデータを生成することから、中途の処理オブジェクトに対応する不正なパリティデータを生成することが困難であるとともに、パリティデータが不正に置換された場合、次に実行される処理オブジェクトで生成されるパリティデータが適正值と異なっていることを検知することで、正常な処理が実行されていない処理オブジェクトを確実に特定することが可能となる。

【 0 0 8 0 】

なお、上述した実施の形態 1 及び 2 では、1 つの処理オブジェクトの次に 1 つの処理オブジェクトを実行し、また次の 1 つの処理オブジェクトを実行するといった順次処理を行う場合について説明しているが、複数の処理オブジェクトの実行完了後に 1 つの処理オブジェクトを実行する処理工程、あるいは 1 つの処理オブジェクトの実行完了後に複数の処理オブジェクトを実行する処理工程等、多様な処理工程においても同様の効果が期待できる。

【 0 0 8 1 】

以下、付記する。

【 0 0 8 2 】

（付記 1 ）

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、複数の処理オブジェクトの実行完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知システムにおいて、

前記非接触型記録媒体は、

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得する手段と、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、

生成したパリティデータを記録する手段とを備え、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するよう構成してあることを特徴とする情報改竄検知システム。

10

20

30

40

50

【 0 0 8 3 】

(付記 2)

前記非接触型記録媒体は、所定の処理オブジェクトでパリティデータを生成した場合、該所定の処理オブジェクトより前の処理オブジェクトに関する情報の読出し及び書込みを禁止するよう構成してあることを特徴とする付記 1 記載の情報改竄検知システム。

【 0 0 8 4 】

(付記 3)

前記非接触型記録媒体は、所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトの直前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトに対応するパリティデータを生成するよう構成してあることを特徴とする付記 1 又は 2 記載の情報改竄検知システム。

10

【 0 0 8 5 】

(付記 4)

前記非接触型記録媒体は、データを読み書きすることが可能な IC チップ及び無線でデータを送受信することが可能な無線通信手段を備えた IC タグであることを特徴とする付記 1 乃至 3 のいずれか 1 つに記載の情報改竄検知システム。

【 0 0 8 6 】

(付記 5)

データを読み書きすることが可能な IC チップ及び無線でデータを送受信することが可能な無線通信手段を備え、複数の処理オブジェクトを実行する都度、順次パリティデータを生成して記録する非接触型記録媒体において、

20

各処理オブジェクトに関する情報を各処理オブジェクトの実行時に取得する手段と、取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成する手段と、

生成したパリティデータを記録する手段とを備え、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトに対応するパリティデータを生成するよう構成してあることを特徴とする非接触型記録媒体。

30

【 0 0 8 7 】

(付記 6)

所定の処理オブジェクトでパリティデータを生成した場合、該所定の処理オブジェクトより前の処理オブジェクトに関する情報の読出し及び書込みを禁止するよう構成してあることを特徴とする付記 5 記載の非接触型記録媒体。

【 0 0 8 8 】

(付記 7)

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトの直前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトに対応するパリティデータを生成するよう構成してあることを特徴とする付記 5 又は 6 記載の非接触型記録媒体。

40

【 0 0 8 9 】

(付記 8)

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、非接触でデータを読み書きすることが可能な非接触型記録媒体に記録し、すべての処理オブジェクト完了時に前記非接触型記録媒体に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知する情報改竄検知方法において、

前記非接触型記録媒体は、

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得し、

50

取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成し、

生成したパリティデータを記録し、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成することを特徴とする情報改竄検知方法。

【 0 0 9 0 】

(付 記 9)

複数の処理オブジェクトを実行する都度、順次、パリティデータを生成し、すべての処理オブジェクトの実行完了時に記録されているパリティデータに基づいて、途中の処理オブジェクトに関する情報が改竄されているか否かを検知するよう、非接触でデータを読み書きすることが可能な非接触型記録媒体を機能させる非接触型記録媒体で実行することが可能なコンピュータプログラムにおいて、

10

各処理オブジェクトの実行時に、該処理オブジェクトに関する情報を取得するステップと、

取得した各処理オブジェクトに関する情報に基づいて、各処理オブジェクト毎にパリティデータを生成するステップと、

生成したパリティデータを記録するステップとを含み、

所定の処理オブジェクトでパリティデータを生成する場合、該所定の処理オブジェクトより前の処理オブジェクトで生成されたパリティデータ及び前記所定の処理オブジェクトに関する情報に基づいて、前記所定の処理オブジェクトのパリティデータを生成するようにしてあることを特徴とするコンピュータプログラム。

20

【 図 面 の 簡 単 な 説 明 】

【 0 0 9 1 】

【 図 1 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム の 構 成 を 示 す ブ ロ ッ ク 図 で あ る。

【 図 2 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム の 中 央 装 置 の 構 成 を 示 す ブ ロ ッ ク 図 で あ る。

【 図 3 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム の 端 末 装 置 の 構 成 を 示 す ブ ロ ッ ク 図 で あ る。

30

【 図 4 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム で 用 い る I C タ グ の 構 成 を 示 す ブ ロ ッ ク 図 で あ る。

【 図 5 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム で 用 い る I C タ グ の I C チ ッ プ の 処 理 手 順 を 示 す フ ロ ー チ ャ ー ト で あ る。

【 図 6 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム で 用 い る パ リ テ ィ デ ー タ 算 出 方 法 の 説 明 図 で あ る。

【 図 7 】 本 発 明 の 実 施 の 形 態 1 に 係 る 情 報 改 竄 検 知 シ ス テ ム の 中 央 装 置 の C P U の 処 理 手 順 を 示 す フ ロ ー チ ャ ー ト で あ る。

【 図 8 】 中 央 装 置 の 記 憶 手 段 に 記 憶 す る パ リ テ ィ デ ー タ の デ ー タ 構 成 の 例 示 図 で あ る。

40

【 図 9 】 本 発 明 の 実 施 の 形 態 2 に 係 る 情 報 改 竄 検 知 シ ス テ ム で 用 い る I C タ グ の I C チ ッ プ の 処 理 手 順 を 示 す フ ロ ー チ ャ ー ト で あ る。

【 図 1 0 】 本 発 明 の 実 施 の 形 態 2 に 係 る 情 報 改 竄 検 知 シ ス テ ム で 用 い る パ リ テ ィ デ ー タ 算 出 方 法 の 説 明 図 で あ る。

【 図 1 1 】 本 発 明 の 実 施 の 形 態 2 に 係 る 情 報 改 竄 検 知 シ ス テ ム の 中 央 装 置 の C P U の 処 理 手 順 を 示 す フ ロ ー チ ャ ー ト で あ る。

【 符 号 の 説 明 】

【 0 0 9 2 】

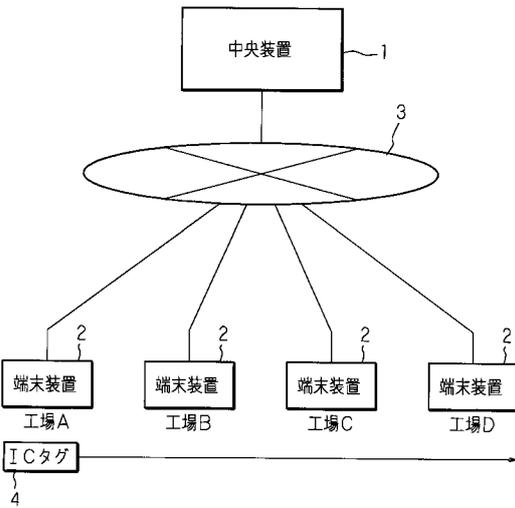
- 1 中央装置
- 2 端末装置

50

- 3 インターネット
- 4 ICタグ
- 11、21 CPU
- 12、22 記憶手段
- 13、23 RAM
- 14、24 通信インターフェース
- 15、25 入力手段
- 16、26 出力手段
- 17 補助記憶手段
- 27 ICタグリーダー/ライター
- 41 ICチップ
- 42 無線通信手段

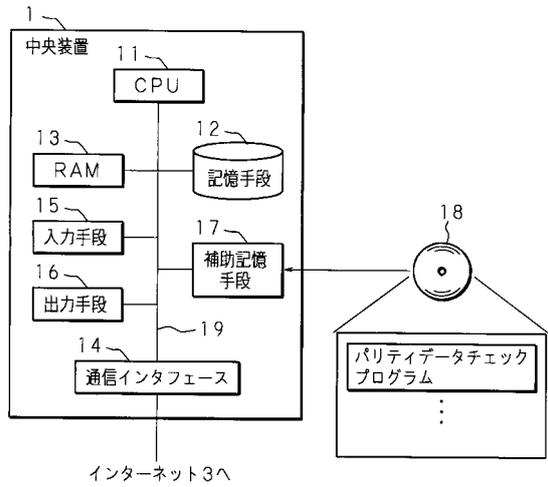
【図1】

本発明の実施の形態1に係る情報改竄検知システムの構成を示すブロック図



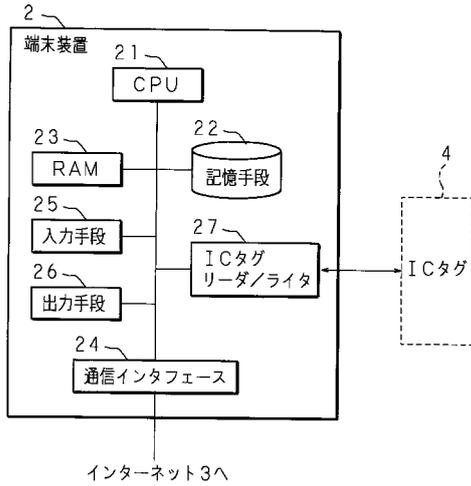
【図2】

本発明の実施の形態1に係る情報改竄検知システムの中央装置の構成を示すブロック図



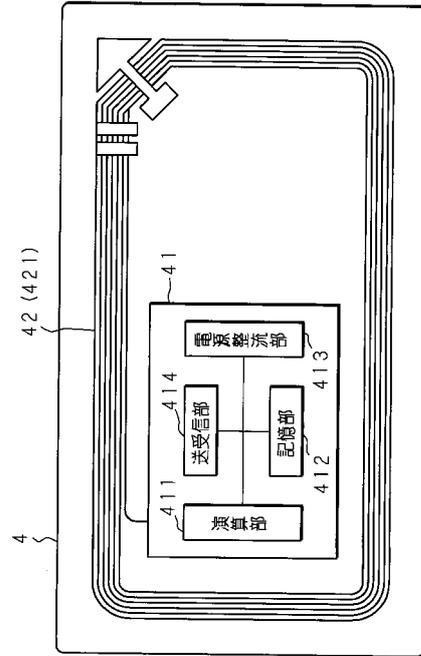
【図3】

本発明の実施の形態1に係る情報改竄検知システムの端末装置の構成を示すブロック図



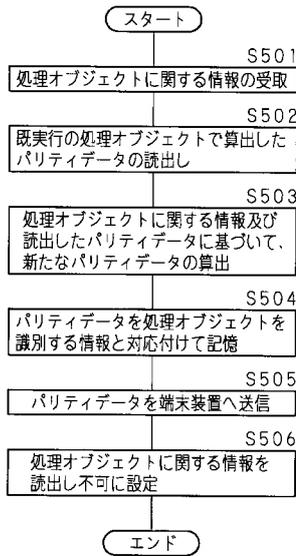
【図4】

本発明の実施の形態1に係る情報改竄検知システムで用いるICタグの構成を示すブロック図



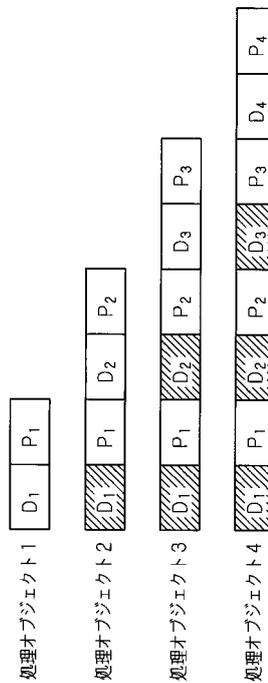
【図5】

本発明の実施の形態1に係る情報改竄検知システムで用いるICタグのICチップの処理手順を示すフローチャート



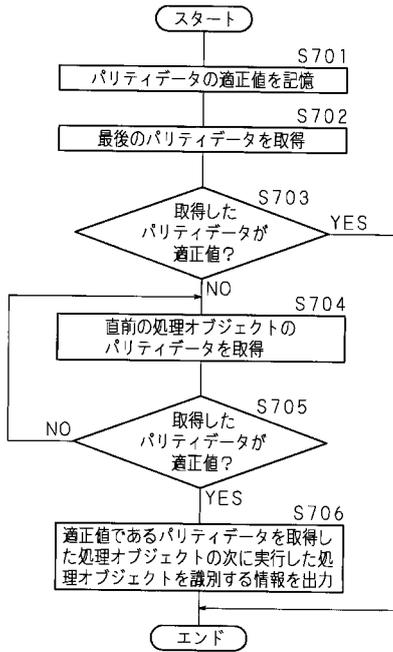
【図6】

本発明の実施の形態1に係る情報改竄検知システムで用いるパリティデータ算出方法の説明図



【図 7】

本発明の実施の形態 1 に係る情報改竄検知システムの中央装置の CPU の処理手順を示すフローチャート



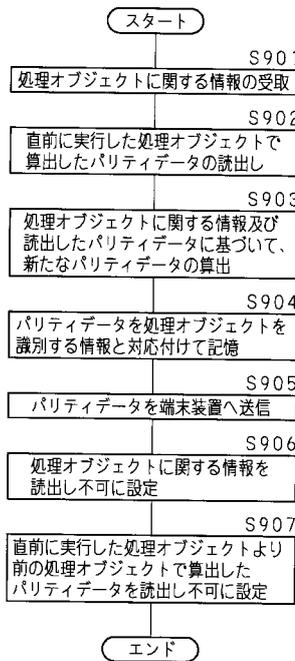
【図 8】

中央装置の記憶手段に記憶するパリティデータのデータ構成の例示図

処理オブジェクト番号	1	2	3	4
パリティデータ	P ₁	P ₂	P ₃	P ₄

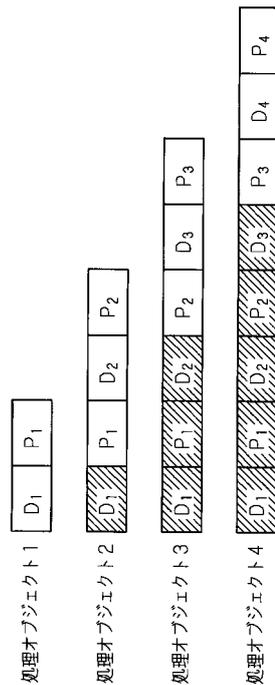
【図 9】

本発明の実施の形態 2 に係る情報改竄検知システムで用いる IC タグの IC チップの処理手順を示すフローチャート



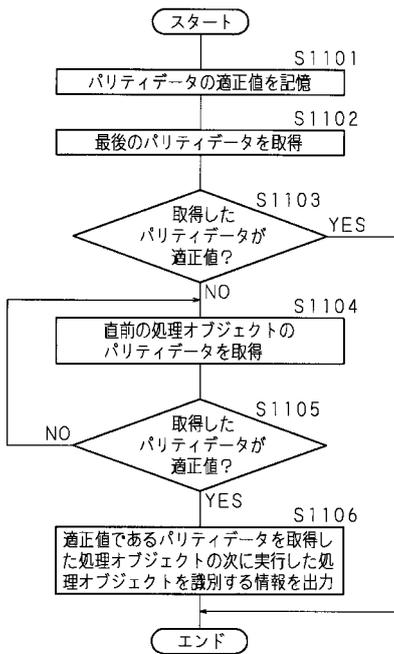
【図 10】

本発明の実施の形態 2 に係る情報改竄検知システムで用いるパリティデータ算出方法の説明図



【図 11】

本発明の実施の形態2に係る情報改竄検知システムの中央装置のCPUの処理手順を示すフローチャート



フロントページの続き

審査官 高橋 克

- (56)参考文献 特開2001-307055(JP,A)
特開2002-082834(JP,A)
特開平10-283263(JP,A)
特開2002-024767(JP,A)
特開2004-043143(JP,A)
特開2005-063039(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/24
G06K 19/07
G06K 19/073
G06Q 50/00