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

特許第6072584号
(P6072584)

(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.		F I		
G06F 21/50	(2013.01)	G06F	21/50	
G06F 21/57	(2013.01)	G06F	21/57	320
G06F 21/64	(2013.01)	G06F	21/64	
G06F 9/445	(2006.01)	G06F	9/06	610L
G06F 13/00	(2006.01)	G06F	13/00	530B

請求項の数 5　(全 22 頁)

(21)出願番号　特願2013-67634(P2013-67634)
(22)出願日　平成25年3月27日(2013.3.27)
(65)公開番号　特開2014-191658(P2014-191658A)
(43)公開日　平成26年10月6日(2014.10.6)
審査請求日　平成28年1月8日(2016.1.8)

(73)特許権者　598057291
株式会社富士通エフサス
神奈川県川崎市中原区中丸子１３番地２
(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　100089118
弁理士　酒井　宏明
(72)発明者　伊藤　昌彦
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内
(72)発明者　浅沼　広樹
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内

最終頁に続く

(54)【発明の名称】サーバ装置およびプログラム管理方法

(57)【特許請求の範囲】
【請求項１】
自装置にインストールされているプログラムを管理テーブルで管理する管理部と、
自装置へのプログラムのインストールおよび自装置にインストールされているプログラムの更新の際に、前記インストールの処理および前記更新の処理をおこなうとともに、前記インストールの処理および前記更新の処理に応じて前記管理部が管理するプログラムの管理情報を更新する更新部と、
前記更新部による更新後のプログラムおよび前記管理テーブルのハッシュ値を算出し、算出した前記ハッシュ値を、外部装置へ送信するとともに、自装置に記憶するハッシュ値処理部と
を有することを特徴とするサーバ装置。
【請求項２】
自装置の記憶部に格納されているファイルのうち、実行可能なプログラムの属性を有するファイルを抽出する抽出部と、
前記抽出部により抽出された前記ファイルと、前記管理部により前記管理テーブルで管理されるプログラムとを比較し、前記ファイルが前記管理部により前記管理テーブルで管理されているプログラムに含まれるか否かを判定する判定部と
をさらに有し、
前記ハッシュ値処理部は、前記判定部により前記ファイルが前記管理部により前記管理テーブルで管理されているプログラムに含まれないと判定された場合に、前記ファイルに

基づくハッシュ値を算出し、算出した前記ハッシュ値を外部装置へ送信する
ことを特徴とする請求項１に記載のサーバ装置。
【請求項３】
前記ハッシュ値は、前記サーバ装置に搭載されたＴＰＭチップにより算出され、前記ＴＰＭチップにより確保された記憶領域に格納される
ことを特徴とする請求項１または２に記載のサーバ装置。
【請求項４】
コンピュータが実行するプログラム管理方法であって、
前記コンピュータにインストールされているプログラムを管理部にて管理テーブルで管理し、
前記コンピュータへのプログラムのインストールおよび自装置にインストールされているプログラムの更新の際に、前記インストールの処理および前記更新の処理をおこなうとともに、前記インストールの処理および前記更新の処理に応じて、前記管理部が管理するプログラムの情報を更新し、
更新後の前記プログラムおよび前記管理テーブルのハッシュ値を算出し、算出した前記ハッシュ値を、外部装置へ送信するとともに、自装置に記憶する
各処理を含むことを特徴とするプログラム管理方法。
【請求項５】
前記コンピュータの記憶部に格納されているファイルのうち、実行可能なプログラムの属性を有するファイルを抽出し、
抽出された前記ファイルと、前記管理部により前記管理テーブルで管理されるプログラムとを比較し、前記ファイルが前記管理部により前記管理テーブルで管理されているプログラムに含まれるか否かを判定し、
前記ファイルが前記管理部により前記管理テーブルで管理されているプログラムに含まれないと判定された場合に、前記ファイルに基づくハッシュ値を、前記コンピュータに搭載されたＴＰＭチップにより算出し、算出した前記ハッシュ値を外部装置へ送信し、
前記ハッシュ値を前記ＴＰＭチップにより確保された記憶領域に格納する
処理をさらに含むことを特徴とする請求項４に記載のプログラム管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバ装置などに関する。
【背景技術】
【０００２】
従来から、電気機器が管理する情報の非改竄証明のために、電気機器が管理する情報のハッシュ値をサーバ装置が管理し、電気機器が管理する情報に基づいて算出したハッシュ値と、サーバ装置が管理するハッシュ値とを比較する技術がある。非改竄証明とは、情報が真性であることを証左に基づき証明することである。この技術によれば、電気機器が管理する情報に基づいて算出したハッシュ値と、サーバ装置が管理するハッシュ値とが一致する場合に、電気機器が管理する情報が改竄された可能性がないと判定する。一方、電気機器が管理する情報に基づいて算出したハッシュ値と、サーバ装置が管理するハッシュ値とが一致しない場合に、電気機器が管理する情報が改竄された可能性があると判定する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００９－２３０４５７号公報
【非特許文献】
【０００４】
【非特許文献１】富士通株式会社　「Systemwalker　IT　Change　Manager　V14g」
【発明の概要】

【発明が解決しようとする課題】
【０００５】
しかしながら、上述の従来技術では、非改竄性証明に関し、サーバ装置自体が信頼に値するか否かが明確でないため、たとえサーバ装置が、電気機器が管理する情報が改竄されていないと判定しても、その信憑性を保証することはできない。
【０００６】
開示技術の実施形態の一例では、上述の問題に鑑み、非改竄性証明に関するサーバ装置の信頼性を高めることを目的とする。
【課題を解決するための手段】
【０００７】
開示技術の実施形態の一例では、サーバ装置は、管理部、更新部を有する。管理部は、自装置にインストールされているプログラムを管理する。更新部は、自装置へのプログラムのインストールおよび自装置にインストールされているプログラムの更新の際に、インストールの処理および更新の処理をおこなう。さらに、管理部は、インストールの処理および更新の処理に応じて管理部が管理するプログラムの管理情報を更新する。
【発明の効果】
【０００８】
開示技術の実施形態の一例によれば、非改竄性証明に関するサーバ装置の信頼性を高める。
【図面の簡単な説明】
【０００９】
【図１】図１は、実施形態にかかるシステム構成を示す図である。
【図２】図２は、実施形態にかかるＰ－ＥＭＡサーバの構成を示すブロック図である。
【図３】図３は、Ｐ－ＥＭＡサーバが有するポリシーテーブルを示す図である。
【図４】図４は、Ｐ－ＥＭＡサーバが有するペアリングテーブルを示す図である。
【図５】図５は、Ｐ－ＥＭＡサーバが有するプログラム管理テーブルを示す図である。
【図６】図６は、Ｐ－ＥＭＡサーバが有するファイル群を示す図である。
【図７】図７は、Ｐ－ＥＭＡサーバが有するハッシュ値ログを示す図である。
【図８】図８は、Ｐ－ＥＭＡサーバが有するペアリングテーブル更新ログを示す図である。
【図９】図９は、Ｐ－ＥＭＡサーバが有するアクセスログを示す図である。
【図１０】図１０は、Ｐ－ＥＭＡサーバが有するプログラム更新ログを示す図である。
【図１１】図１１は、Ｐ－ＥＭＡサーバが有するプログラム動作ログを示す図である。
【図１２】図１２は、Ｐ－ＥＭＡサーバで実行されるハッシュ値ログのハッシュ値算出処理を示すフローチャートである。
【図１３】図１３は、Ｐ－ＥＭＡサーバで実行されるペアリングテーブル更新ログのハッシュ値算出処理を示すフローチャートである。
【図１４】図１４は、Ｐ－ＥＭＡサーバで実行されるアクセスログのハッシュ値算出処理を示すフローチャートである。
【図１５】図１５は、Ｐ－ＥＭＡサーバで実行されるプログラム管理テーブル更新ログのハッシュ値算出処理を示すフローチャートである。
【図１６】図１６は、Ｐ－ＥＭＡサーバで実行されるプログラム実行ログのハッシュ値算出処理を示すフローチャートである。
【図１７】図１７は、Ｐ－ＥＭＡサーバで実行される不正プログラム検出処理を示すフローチャートである。
【図１８】図１８は、実施形態にかかるＨ－ＥＭＡサーバの構成を示すブロック図である。
【図１９】図１９は、Ｈ－ＥＭＡサーバが有するポリシーテーブルを示す図である。
【図２０】図２０は、Ｈ－ＥＭＡサーバで実行されるＰ－ＥＭＡサーバ監査処理を示すフローチャートである。

【発明を実施するための形態】
【００１０】
以下に、開示技術の実施形態の一例を、図面に基づいて説明する。なお、以下の実施例は、一例を示すに過ぎず、開示技術を限定するものではない。また、以下の実施例は、矛盾しない範囲で適宜組合せてもよい。
【００１１】
（システム構成）
図１は、実施形態にかかるシステム構成を示す図である。図１に示すように、実施形態にかかるシステム１は、保守サーバ１００Ａ、保守端末２００Ａ－１～２００Ａ－ｘ、・・・、保守サーバ１００Ｎ、保守端末２００Ｎ－１～２００Ｎ－ｙ、Ｐ－ＥＭＡサーバ３００、Ｈ－ＥＭＡサーバ４００を有する。保守サーバ１００Ａ、保守端末２００Ａ－１～２００Ａ－ｘ、・・・、保守サーバ１００Ｎ、保守端末２００Ｎ－１～２００Ｎ－ｙ、Ｐ－ＥＭＡサーバ３００は、公衆網もしくは閉域網であるネットワーク２を介して接続される。Ｐ－ＥＭＡサーバ３００と、Ｈ－ＥＭＡサーバ４００は、通信可能にケーブルもしくはネットワークを介して接続される。
【００１２】
システム１において、１つの保守サーバ１００Ａと、複数の保守端末２００Ａ－１～２００Ａ－ｘが１つの装置グループをなし、１つの保守サーバ１００Ｎと、複数の保守端末２００Ｎ－１～１００Ｎ－ｙが１つの装置グループをなす。なお、１つの装置グループに含まれる保守サーバおよび保守端末の数は、システム１の構成要件にしたがった任意の数である。そして、システム１における装置グループの数も、システム１の構成要件にしたがった任意の数である。
【００１３】
そして、保守サーバ１００Ａは、ＴＰＭ（Trusted Platform Module）チップ１０Ａを有する。保守端末２００Ａ－１～２００Ａ－ｘは、ＴＰＭチップ２０Ａ－１～２０Ａ－ｘをそれぞれ有する。同様に、保守サーバ１００Ｎは、ＴＰＭチップ１０Ｎを有する。保守端末２００Ｎ－１～２００Ｎ－ｘは、ＴＰＭチップ２０Ｎ－１～２０Ｎ－ｙをそれぞれ有する。
【００１４】
なお、以下では、保守サーバ１００Ａ～１００Ｎを総称する場合には、保守サーバ１００と称する。また、保守端末２００Ａ－１～２００Ａ－ｘ、・・・、保守端末２００Ｎ－１～２００Ｎ－ｙを総称する場合には、保守端末２００と称する。また、保守サーバ１００が有するＴＰＭチップをＴＰＭチップ１０と総称し、保守端末２００が有するＴＰＭチップをＴＰＭチップ２０と総称する。
【００１５】
なお、図示はしないが、ネットワーク２には、保守サーバ１００および保守端末２００と暗号化通信をおこなうための鍵を管理するＣＡ（Certificate Authority）サーバが接続されている。
【００１６】
保守端末２００は、保守の対象となる電気機器（図示せず）に接続される、保守作業員が利用する端末装置である。電気機器は、例えば、パーソナルコンピュータ、サーバコンピュータ、プリンタ、ネットワーク機器、外部ストレージ、携帯電話、スマートフォン、冷蔵庫、洗濯機、テレビ、ステレオコンポ、医療機器、工作機器などである。保守作業員は、電気機器が設置される作業現場に到着した後に、電気機器と保守端末２００を接続する。保守端末２００は、電気機器と接続されると、電気機器が有するエージェントから、電気機器の構成情報や電気機器で発生した障害の情報など、電気機器の動作にかかる各種情報を取得し、保守サーバ１００へ送信する。保守サーバは、保守端末から送られてくる保守端末と電気機器との間のすべての通信内容を含む通信履歴と、保守端末と保守サーバとの間のすべての通信内容を含む通信履歴を保存するとともに、それぞれの通信履歴のハッシュ値を計算して保守サーバ内に保存して、または保存せずに、それぞれのハッシュ値

をＰ－ＥＭＡサーバ３００に送信する。このハッシュ値には通信履歴に関する属性情報、例えば通信機器対の名称、通信機器ＩＤ、通信時刻等が付随してもよい。Ｐ－ＥＭＡサーバ３００は、保守サーバから送付されてきたハッシュ値をその属性情報とともに保存する。また、このハッシュ値とそれに付随する属性情報は電子署名を付してもよい。

【００１７】

Ｐ－ＥＭＡとは、Private（もしくはPersonal）－Environment Management Authorityの略である。Ｐ－ＥＭＡサーバ３００は、保守サーバ１００に蓄積されている上記通信履歴の真正性の担保と保守サーバ１００の動作の正当性を担保するための機能を有する装置である。Ｐ－ＥＭＡサーバ３００は、この機能を提供するために、私的機関等により設置、管理される。Ｐ－ＥＭＡサーバ３００は、例えば、業界ごとに設置されてもよい。

【００１８】

Ｈ－ＥＭＡとは、Hyper－Environment Management Authorityの略である。Ｈ－ＥＭＡサーバ４００は、システム監査体系において、Ｐ－ＥＭＡサーバ３００の上位に位置づけられる。Ｈ－ＥＭＡサーバ４００は、Ｐ－ＥＭＡサーバ３００から受信した電気機器の動作にかかる各種情報を管理し、その真正性を監査するための機能を有する装置である。Ｈ－ＥＭＡサーバ４００は、Ｐ－ＥＭＡサーバ３００に蓄積されたハッシュ値等やＰ－ＥＭＡサーバ３００の動作状況を管理し、Ｐ－ＥＭＡサーバの動作の正当性を担保する機能を提供するために、公的機関または、準公的機関等により設置、管理される。

【００１９】

なお、上述のＰ－ＥＭＡサーバ３００およびＨ－ＥＭＡサーバ４００は、特許第４８１８６６４号に開示される環境管理局に類するものである。Ｐ－ＥＭＡサーバ３００およびＨ－ＥＭＡサーバ４００は、ＴＰＭチップを局内に含む。Ｐ－ＥＭＡサーバ３００およびＨ－ＥＭＡサーバ４００は、例えば、保守サーバ１００Ａや保守端末２００Ａ－１のような管理対象電子機器に組み込まれているソフトウェアやハードウェアの正規品情報を管理し、必要に応じ保守サーバ１００Ａや保守端末２００Ａ－１等の監査を行う機能を有する。なお、保守サーバ１００Ａや保守端末２００Ａ－１等の認証にかかる行為は従来技術であるＰＫＩシステムに従う。その際に、署名鍵管理等については、ＩＥＴＦ　ＲＦＣ５７９２／５７９３に開示されているＴＣＧ技術を応用してもよい。

【００２０】

ところで、図１に示す保守サーバ１００、保守端末２００、Ｐ－ＥＭＡサーバ３００、Ｈ－ＥＭＡサーバ４００は、ＴＣＧ（Trusted Computing Group）技術を利用して、セキュアにデータ通信を実行することを前提とする。実施形態で利用するＴＣＧ技術の一例について説明する。インターネットに接続される端末、デバイスは常にセキュリティの脅威に曝され、ウィルス、スパイウェア、その他悪質なスクリプト、不正アクセスなどにより、プラットフォームを構成するソフトウェア構造に予期せぬ改変が加えられる場合がある。このようなリスクに対して、ＴＣＧでは、プラットフォームの信頼性を保障することにより、安全なコンピューティング環境を実現する。ここで、プラットフォームとは、ハードウェア、ＯＳ、アプリケーションなどを示す。

【００２１】

例えば、ソフトウェアの改竄という脅威に対して、従来のソフトウェアのみに依存するセキュリティ対策には限界がある。このため、ＴＣＧでは、ＴＰＭチップをプラットフォームに埋め込み、かかるＴＰＭチップを信頼のルートとして、改竄が極めて困難な、信頼できるコンピューティング環境を構築している。また、ＴＰＭチップを利用することで、ハードウェアベースのデータおよび証明書の保護、安全な暗号処理環境の実現ができる。

【００２２】

次に、ＴＰＭチップについて説明する。ＴＰＭチップは、電子機器にバインドされるバードウェアのチップであり、耐タンパー性を持つ。ＴＰＭチップは電子機器から取り外しができないように、電子機器の主要な構成パーツに物理的にバインドされる。例えば、電子機器の構成パーツは、マザーボードなどに対応する。ＴＰＭチップは、実装される機能、メモリ領域、プロセッサのパワーを極力抑えて動作するように設計されているため、低

コストで製造でき、様々な電気機器やプラットフォームに適用できる。

【００２３】

例えば、ＴＰＭの機能には、ＲＳＡ（Rivest Shamir Adleman）秘密鍵を生成および保管する機能、ＲＳＡ秘密鍵による署名、暗号化、復号する機能が含まれる。ＲＳＡでは、秘密鍵と公開鍵とのペアを作成する。また、ＴＰＭの機能には、ＳＨＡ－１（Secure Hash Algorithm 1）のハッシュ値を算出する機能、電気機器の環境情報を保持する機能が含まれる。ＴＰＭは、バインドされた電気機器が起動した時点で、ＢＩＯＳ（Basic Input/Output System）、ＯＳ（Operating System）ローダ、ＯＳカーネルへのブートプロセスにおけるソフトウェアコードを計測する。そして、ＴＰＭは、計測したソフトウェアコードをハッシュ化して、ＴＰＭ内部のレジスタに登録する。また、ＴＰＭは、バインドされた電子機器のハードウェアの情報を収集し、ハードウェアの情報をハッシュ化して、ＴＰＭ内部のレジスタに登録する。

【００２４】

ＴＣＧでは、上位のアプリケーションやライブラリからハードウェアデバイスであるＴＰＭチップを利用するためソフトウェアスタックとソフトウェアインターフェースを規定する。このソフトウェアスタックはＴＳＳ（TCG Software Stack）と呼ばれ、リソースが制限されるＴＰＭチップの機能を保管するソフトウェアモジュールから構成されている。電子機器のアプリケーションは、ＴＳＳの提供するインターフェースを利用して、上述したＴＰＭチップの機能にアクセスすることができる。

【００２５】

（Ｐ－ＥＭＡサーバの構成）

図２は、実施形態にかかるＰ－ＥＭＡサーバの構成を示すブロック図である。図２に示すように、実施形態にかかるＰ－ＥＭＡサーバ３００は、通信部３１０、入力部３２０、表示部３３０、インターフェース部３４０、ＴＰＭチップ３５０、記憶部３６０、制御部３７０を有する。Ｐ－ＥＭＡサーバ３００が有する各構成要素は、バス３８０によって相互に接続される。

【００２６】

通信部３１０は、ネットワーク２を介して保守サーバ１００、保守端末２００と通信をおこなう。また、通信部３１０は、Ｈ－ＥＭＡサーバ４００と通信をおこなう。入力部３２０は、Ｐ－ＥＭＡサーバ３００への各種情報の入力を受け付ける入力装置であり、例えば、キーボード、マウス、タッチパネルなどである。表示部３３０は、制御部３７０から出力される各種情報を表示する表示装置であり、例えば、液晶ディスプレイなどである。インターフェース部３４０は、Ｈ－ＥＭＡサーバ４００と接続するためのインターフェースである。

【００２７】

ＴＰＭチップ３５０は、上述したＴＣＧ技術に準拠するＴＰＭチップであり、後述するように、制御部３７０と協働して動作し、保守サーバ１００および保守端末２００との通信の安全性を保証する。例えば、ＴＰＭチップ３５０は、制御部３７０の各部からの要求に応じて、情報のハッシュ値算出（ハッシュ化）や、ＴＰＭチップにより暗号化された情報を復号する。

【００２８】

記憶部３６０は、ポリシーテーブル３６１ａ、ハッシュ値ログ３６２ｂ、ペアリングテーブル３６３ａ、ペアリングテーブル更新ログ３６３ｂ、アクセスログ３６４ｂを有する。また、記憶部３６０は、プログラム管理テーブル３６５ａ、プログラム更新ログ３６５ｂ、ファイル群３６６、プログラム動作ログ３６７ｂ、ＴＰＭ拡張保護領域３６８、一時テーブル３６９を有する。ＴＰＭ拡張保護領域３６８は、ＴＰＭチップ３５０により記憶部３６０内に確保された領域であり、ＴＰＭチップ３５０のみがアクセス可能な領域である。記憶部３６０は、例えば、ハードディスク装置、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ（Flash Memory）などの半導体メモリ素子などの記憶装置である。記憶部３６０が有する各種情報の詳細は、後述する。な

お、以降、ＴＰＭチップ内の領域および上記ＴＰＭ拡張保護領域３６８をＴＰＭチップにより確保された領域と呼ぶ。

【００２９】

制御部３７０は、ハッシュ値ログ送受信部３７１、テーブル更新部３７２、アクセス監視部３７３、プログラム更新部３７４、プログラム実行監視部３７５、不正プログラム検出部３７６を有する。制御部３７０は、後述するポリシーテーブル３６１ａに記述されたポリシーにしたがい動作する。制御部３７０は、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）などの集積装置である。または、制御部３７０は、例えば、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）などの電子回路である。

【００３０】

ハッシュ値ログ送受信部３７１は、保守サーバ１００（もしくは保守端末２００）から受信した、ＴＰＭチップ１０（もしくはＴＰＭチップ２０）によりそれぞれハッシュ値が算出されて付加された各種情報、例えば、電気機器の動作にかかる各種情報を受信する。保守サーバ１００（もしくは保守端末２００）から受信した、ハッシュ値が算出されて付加された各種情報、例えば、電気機器の動作にかかる各種情報を、ハッシュ値ログと呼ぶ。そして、ハッシュ値ログ送受信部３７１は、記憶部３６０のハッシュ値ログ３６２ｂにハッシュ値ログを記憶させる。ハッシュ値ログは、ハッシュ値を算出する基礎になる基礎情報と、基礎情報に基づいて算出されたハッシュ値を含む。ハッシュ値ログ送受信部３７１は、送信元である保守サーバ１００もしくは保守端末２００の識別情報と、ハッシュ値ログと対応付けて、１件ずつハッシュ値ログ３６２ｂに記憶させる。なお、このハッシュ値の算出にあたっては、適宜ポリシーを定め、そのポリシーにしたがって実行する。

【００３１】

また、ハッシュ値ログ送受信部３７１は、ＴＰＭチップ３５０により、ハッシュ値ログ３６２ｂに記憶させた、例えばｎ（ｎは自然数）件のハッシュ値ログを単位として、ｎ件のハッシュ値ログに基づくハッシュ値をさらに算出する。そして、ハッシュ値ログ送受信部３７１は、まとめたｎ件のハッシュ値ログに基づくハッシュ値を、ｎ件のハッシュ値ログとともに、Ｈ－ＥＭＡサーバ４００へ送信する。

【００３２】

なお、ｎ件のハッシュ値ログのまとめ方は、ハッシュ値ログの送信元の保守サーバ１００および保守端末２００の組合せにおいて、例えば、ハッシュ値ログのタイムスタンプの順序でｎ件ずつのハッシュ値ログをまとめる。すなわち、ハッシュ値ログ送受信部３７１は、保守対象の電気機器に接続される保守端末２００および保守端末２００を管理する保守サーバ１００の組合せごとに、ハッシュ値ログのタイムスタンプの順序でｎ件ずつのハッシュ値ログをまとめる。言い換えると、Ｐ－ＥＭＡサーバ３００には、時刻の経過に応じて、保守サーバ１００、保守端末２００から受信したハッシュ値ログが蓄積されていく。ハッシュ値ログ送受信部３７１は、ｎ件のハッシュ値ログが蓄積されたタイミングで、ＴＰＭチップ３５０によりｎ件のハッシュ値ログのハッシュ値を算出し、算出したハッシュ値をＨ－ＥＭＡサーバ４００へ送信する。これにより、保守対象の電気機器のいずれのグループ単位のいずれの時刻のハッシュ値ログに不正が含まれるかが、Ｈ－ＥＭＡサーバ４００で特定できる。

【００３３】

テーブル更新部３７２は、ペアリングテーブル３６３ａの初期書き込み、書き換えをおこなう。ペアリングテーブル３６３ａの初期書き込み、書き換えの指示は、入力部３２０や、保守サーバ１００などから入力される。ペアリングテーブル３６３ａは、後述するように、保守サーバ１００と、保守端末２００との対応付けを管理するテーブルである。そして、テーブル更新部３７２は、ペアリングテーブル３６３ａの初期書き込み、書き換えの都度、最新のペアリングテーブル３６３ａに基づくハッシュ値を算出し、最新のペアリングテーブル３６３ａとともにペアリングテーブル更新ログ３６３ｂに記憶させる。そして、テーブル更新部３７２は、最新のペアリングテーブルに基づくハッシュ値を、Ｈ－Ｅ

ＭＡサーバ４００へ送信する。なお、テーブル更新部３７２は、以上の処理を、Ｐ－ＥＭＡサーバ３００の起動時、再起動時にもおこなう。

【００３４】

アクセス監視部３７３は、ネットワーク２を介した外部装置からＰ－ＥＭＡサーバ３００へのアクセスを監視する。そして、アクセス監視部３７３は、ネットワーク２を介した外部装置からＰ－ＥＭＡサーバ３００へのアクセスの監視結果を、アクセスコントロールログとしてアクセスログ３６４ｂに記憶させる。例えば、アクセス監視部３７３は、Ｐ－ＥＭＡサーバ３００へ接続が許可された保守サーバ１００以外かつ保守端末２００以外のその他の装置からのアクセスに対してアクセス不可としたことを、アクセスコントロールログとしてアクセスログ３６４ｂに記憶させる。そして、アクセス監視部３７３は、ＴＰＭチップ３５０により、アクセスログ３６４ｂに記憶させたアクセスコントロールログのハッシュ値を算出する。そして、アクセス監視部３７３は、アクセスログ３６４ｂにおいて、アクセスログ３６４ｂに記憶させたアクセスコントロールログに算出したハッシュ値を対応付けて記憶させるとともに、算出したハッシュ値をＨ－ＥＭＡサーバ４００へ送信する。

【００３５】

プログラム更新部３７４は、Ｐ－ＥＭＡサーバ３００で動作する全てのプログラムの初期インストール、更新をおこなう。Ｐ－ＥＭＡサーバ３００で動作するプログラムの初期インストール、更新は、プログラム更新部３７４以外はおこなうことができない。以下、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、ハッシュ値ログ送受信部３７１としてコンピュータを機能させるプログラム、テーブル更新部３７２としてコンピュータを機能させるプログラムを含む。また、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、アクセス監視部３７３としてコンピュータを機能させるプログラム、プログラム更新部３７４としてコンピュータを機能させるプログラムを含む。また、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、プログラム実行監視部３７５としてコンピュータを機能させるプログラム、不正プログラム検出部３７６としてコンピュータを機能させるプログラムを含む。

【００３６】

なお、Ｐ－ＥＭＡサーバ３００で動作するプログラムの初期インストール、更新の指示は、入力部３２０などから入力される。あるいは、Ｐ－ＥＭＡサーバ３００で動作するプログラムの初期インストール、更新の指示は、ネットワーク２を介した外部の信頼できる装置から受信してもよい。Ｐ－ＥＭＡサーバ３００で動作する全てのプログラムは、プログラム管理テーブル３６５ａにより管理される。プログラム管理テーブル３６５ａは、後述するように、プログラムの識別情報、インストール日時、初期バージョン、最終更新日時、最新バージョンを対応付けて管理するテーブルである。

【００３７】

そして、プログラム更新部３７４は、Ｐ－ＥＭＡサーバ３００で動作するプログラムの初期インストール、更新の都度、プログラム管理テーブル３６５ａを書き換える。そして、プログラム更新部３７４は、更新前のプログラムデータをプログラム更新ログ３６５ｂに記憶させる。そして、プログラム更新部３７４は、ＴＰＭチップ３５０により、更新後のプログラムデータに基づくハッシュ値を算出し、更新後のプログラムデータとともにプログラム更新ログ３６５ｂに記憶させる。そして、プログラム更新部３７４は、更新後のプログラムデータに基づくハッシュ値を、更新後のプログラムデータとともにＨ－ＥＭＡサーバ４００へ送信する。また、プログラム更新部３７４は、ＴＰＭチップ３５０により、初期インストール、更新の都度、更新後のプログラム管理テーブル３６５ａに基づくハッシュ値を算出し、更新後のプログラム管理テーブル３６５ａとともにＨ－ＥＭＡ４００へ送信する。また、プログラム更新部３７４は、更新後のプログラムデータおよび更新後のプログラム管理テーブル３６５ａに基づくハッシュ値を、ＴＰＭチップ３５０により、ＴＰＭ拡張保護領域３６８に記憶させる。

【００３８】

プログラム実行監視部３７５は、Ｐ－ＥＭＡサーバ３００で動作する全てのプログラムの実行を監視する。なお、上述したように、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、ハッシュ値ログ送受信部３７１としてコンピュータを機能させるプログラム、テーブル更新部３７２としてコンピュータを機能させるプログラムを含む。また、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、アクセス監視部３７３としてコンピュータを機能させるプログラム、プログラム更新部３７４としてコンピュータを機能させるプログラムを含む。また、Ｐ－ＥＭＡサーバ３００で動作するプログラムは、プログラム実行監視部３７５としてコンピュータを機能させるプログラム、不正プログラム検出部３７６としてコンピュータを機能させるプログラムを含む。

【００３９】

プログラム実行監視部３７５は、Ｐ－ＥＭＡサーバ３００で動作する全てのプログラムの実行にともなう動作ログを取得し、後述するプログラム動作ログ３６７ｂに記憶させる。プログラム実行監視部３７５は、プログラムの実行にともなう動作ログとして、プログラムの識別情報、動作内容、動作日時を含む１件の動作ログごとに、動作ログに基づくハッシュ値を算出し、動作ログに対応付けてプログラム動作ログ３６７ｂに記憶させる。そして、プログラム実行監視部３７５は、各動作ログに基づく各ハッシュ値をＨ－ＥＭＡサーバ４００へ送信する。なお、プログラム実行監視部３７５は、動作ログごとにハッシュ値を算出し、Ｈ－ＥＭＡサーバ４００へ送信することとしてもよい。あるいは、プログラム実行監視部３７５は、プログラム単位もしくは動作日時単位で複数の動作ログをまとめ、まとめた動作ログの単位でハッシュ値を算出し、Ｈ－ＥＭＡサーバ４００へ送信することとしてもよい。

【００４０】

不正プログラム検出部３７６は、Ｐ－ＥＭＡサーバ３００の起動時もしくは予め定められた周期により、Ｐ－ＥＭＡサーバ３００内に存在するファイル群３６６のファイルの属性をチェックする。そして、不正プログラム検出部３７６は、Ｐ－ＥＭＡサーバ３００内に存在するファイルのうち、実行可能な属性を有するファイルを抽出する。そして、不正プログラム検出部３７６は、抽出した実行可能な属性を有するファイルのうち、Ｐ－ＥＭＡサーバ３００上で動作するＯＳ以外およびミドルウェアのファイル以外のファイルの一覧を一時テーブル３６９に展開する。

【００４１】

そして、不正プログラム検出部３７６は、一時テーブル３６９に含まれるファイルが、プログラム管理テーブル３６５ａに登録されているか否かを判定する。そして、不正プログラム検出部３７６は、一時テーブル３６９に含まれるファイル（プログラム）のうち、プログラム管理テーブル３６５ａに登録されていないプログラムが存在する場合には、次の動作をおこなう。すなわち、不正プログラム検出部３７６は、ポリシーテーブル３６１ａに記述されたポリシーにしたがい、例えば、表示部３３０から警告などを出力したり、Ｐ－ＥＭＡサーバ３００を停止したりする。なお、不正プログラム検出部３７６は、生成した一時テーブル３６９に基づくハッシュ値を算出し、一時テーブル３６９とともにＨ－ＥＭＡサーバ４００へ送信する。

【００４２】

（Ｐ－ＥＭＡサーバが有するポリシーテーブル）

図３は、Ｐ－ＥＭＡサーバが有するポリシーテーブルを示す図である。Ｐ－ＥＭＡサーバ３００が有するポリシーテーブル３６１ａは、Ｐ－ＥＭＡサーバ３００の動作ポリシーを記述する。ポリシーテーブル３６１ａは、例えば、「ハッシュ値ログのハッシュ値を算出するデータ数の単位」が“ｎ件”であるとは、「ｎ件のハッシュ値ログごとにハッシュ値ログをとりまとめ、とりまとめたハッシュ値ログに基づいてハッシュ値を算出する」ことを指す。

【００４３】

また、ポリシーテーブル３６１ａは、「ペアリングテーブル更新ログの保存期間」、「ペアリングテーブル更新ログのハッシュ値算出サイクル」、「アクセスログの保存期間」

などのポリシーが記述されている。Ｐ－ＥＭＡサーバ３００は、ポリシーテーブル３６１ａに記述されたこれらのポリシーにしたがい、各処理をおこなう。なお、各ログのハッシュ値算出サイクルは、時間単位、日単位、週単位、月単位など、任意の時間を設定できる。また、ポリシーテーブル３６１ａに記述される各ログの保存期間は、Ｐ－ＥＭＡサーバ３００のポリシーテーブル３６１ａに記述される、対応する各ログの保存期間以上である。つまり、同一のログは、Ｐ－ＥＭＡサーバ３００よりも、Ｈ－ＥＭＡサーバ４００がより長く保存する。

【００４４】

（Ｐ－ＥＭＡサーバが有するペアリングテーブル）

図４は、Ｐ－ＥＭＡサーバが有するペアリングテーブルを示す図である。ペアリングテーブル３６３ａは、保守サーバ１００と、保守端末２００との対応付けを記憶する。図４に示すように、例えば、「ＡＡＡ」の保守サーバ１００には、「Ａ００１」、「Ａ００２」、・・・の保守端末２００が対応付けられている。すなわち、「ＡＡＡ」の保守サーバ１００および「Ａ００１」、「Ａ００２」、・・・の保守端末２００は、１組の管理単位を構成する。つまり、「Ａ００１」、「Ａ００２」、・・・の保守端末２００は、各保守端末２００が対象とする電気機器の動作にかかる各種情報を、「ＡＡＡ」の保守サーバ１００へ送信することになる。

【００４５】

（Ｐ－ＥＭＡサーバが有するプログラム管理テーブル）

図５は、Ｐ－ＥＭＡサーバが有するプログラム管理テーブルを示す図である。図５に示すように、プログラム管理テーブル３６５ａは、各プログラムの識別情報に、当該プログラムの（初期）インストール日時、当該プログラムの初期バージョン、当該プログラムの最終更新日時、当該プログラムの最新バージョンを対応付けて管理する。図５を参照すると、例えば、「プログラム（の識別情報）」が“ＰＥ１”のプログラムは、「インストール日時」が“y1/m1/d1/h1/mm1/s1”であることが分かる。また、例えば、「プログラム（の識別情報）」が“ＰＥ１”のプログラムは、「初期バージョン」が“Ｖ１”であり、「最終更新日時」が“Y1/M1/D1/H1/MM1/S1”であり、「最新バージョン」が「Ｖ３」であることが分かる。

【００４６】

（Ｐ－ＥＭＡサーバが有するファイル群）

図６は、Ｐ－ＥＭＡサーバが有するファイル群を示す図である。ファイル群３６６は、Ｐ－ＥＭＡサーバ３００が保持する全てのファイルを示す。図６によれば、Ｐ－ＥＭＡサーバ３００は、例えば、“Ｆ１”、“Ｆ２”、・・・のファイルを有することが分かる。なお、ファイル群３６６は、階層形式でファイルが保持され、例えば、実行形式の属性を有するファイルは、特定の階層をたどった先の特定のパスで示される格納領域に保持される。

【００４７】

（Ｐ－ＥＭＡサーバが有するハッシュ値ログ）

図７は、Ｐ－ＥＭＡサーバが有するハッシュ値ログを示す図である。図７に示すように、ハッシュ値ログ３６２ｂは、ハッシュ値および算出日時を少なくとも含む各ハッシュ値ログを含むとともに、ｎ件のハッシュ値ログをまとめたデータに基づき算出されたハッシュ値を対応付けて記憶する。なお、図７には図示しないが、ハッシュ値ログ３６２ｂにおいて、各ハッシュ値ログは、当該ハッシュ値ログの送信元の装置の識別情報とともに記憶されてもよい。または、ポリシーテーブル３６１ａに記述されるポリシーにしたがい、保守サーバ１００および保守端末２００の装置グループごとに、ｎ件のハッシュ値ログをまとめ、まとめたデータに基づき算出されたハッシュ値を対応付けて記憶することとしてもよい。

【００４８】

（Ｐ－ＥＭＡサーバが有するペアリングテーブル更新ログ）

図８は、Ｐ－ＥＭＡサーバが有するペアリングテーブル更新ログを示す図である。ペア

リングテーブル更新ログ３６３ｂは、ペアリングテーブル３６３ａが新規作成、レコードの新規追加、レコード更新される都度に、更新前のペアリングテーブル３６３ａのデータを待避する。そして、ペアリングテーブル更新ログ３６３ｂは、待避した更新前のペアリングテーブル３６３ａのデータに、更新後のペアリングテーブル３６３ａのデータに基づくハッシュ値を対応付けて記憶する。なお、ペアリングテーブル３６３ａの新規作成時には、「更新前テーブルデータ」は“－（Null）”であり、「更新日時」は“新規作成日時”となる。例えば、図８に示すように、「更新日時」が“Y3/M3/D3/H3/MM3/S3”のペアリングテーブル３６３ａの「更新前テーブルデータ」は“ペアリングテーブルデータ１”である。また、“ペアリングテーブルデータ１”に基づく「ハッシュ値」は、“ペアリングテーブルハッシュ値１”である。

【００４９】

（Ｐ－ＥＭＡサーバが有するアクセスログ）

図９は、Ｐ－ＥＭＡサーバが有するアクセスログを示す図である。アクセスログ３６４ｂは、ネットワーク２を介して外部の装置からアクセスがあった場合に、アクセスの識別情報に、アクセス日時、アクセス内容および対応アクション、ハッシュ値を対応付けて記憶する。図９によれば、アクセスログ３６４ｂは、アクセスログとして、例えば、「アクセス」が“アクセス１”のアクセスが、「アクセス日時」が“y5/m5/d5/h5/mm5/s5”にあったことを示す。そして、“アクセス１”のアクセスに対する「アクセス内容および対応アクション」が“保守サーバＸからのアクセス→ブロック”を含むことを示す。そして、“アクセス１”のアクセスログに基づく「ハッシュ値」として“アクセスハッシュ値１”が算出され、“アクセス１”のアクセスログに対応付けて記憶される。なお、「アクセス内容および対応アクション」は、ポリシーテーブル３６１ａに記述されるポリシーにしたがって、アクセスが許可されない外部の装置からのアクセスをブロックし、アクセスが許可された外部の装置からのアクセスのみを許可するなどを含む。

【００５０】

（Ｐ－ＥＭＡサーバが有するプログラム更新ログ）

図１０は、Ｐ－ＥＭＡサーバが有するプログラム更新ログを示す図である。プログラム更新ログ３６５ｂは、Ｐ－ＥＭＡサーバ３００で動作するプログラムが更新される都度に、更新前のプログラムのデータおよび更新前のプログラム管理テーブル３６５ａのデータを待避する。そして、プログラム更新ログ３６５ｂは、更新後のプログラムのデータに基づくハッシュ値および更新後のプログラム管理テーブル３６５ａのデータに基づくハッシュ値を対応付けて記憶する。例えば、図１０に示すように、「更新日時」が“Y5/M5/D5/H5/MM5/S5”の「更新前プログラム」が“更新前プログラムデータ１”であり、「更新後プログラム」が“更新後プログラムデータ１”であり、「更新前プログラム管理テーブルデータ」が“更新前プログラム管理テーブルデータ１”であるプログラム更新ログを含む。また、「更新前プログラム」が“更新前プログラムデータ１”、「更新後プログラム」が“更新後プログラムデータ１”であるプログラム更新ログに基づく「ハッシュ値」は、“更新後プログラムデータハッシュ値１”である。また、「更新前プログラム管理テーブルデータ」が“更新前プログラムデータ１”である更新ログに対応する更新後プログラム管理テーブル３６５ａに基づく「ハッシュ値」は、“更新後プログラム管理テーブルデータハッシュ値１”である。

【００５１】

（Ｐ－ＥＭＡサーバが有するプログラム動作ログ）

図１１は、Ｐ－ＥＭＡサーバが有するプログラム動作ログを示す図である。プログラム動作ログ３６７ｂは、Ｐ－ＥＭＡサーバ３００でプログラムが動作する都度に、プログラムの識別情報、動作内容、動作日時を対応付けて含むプログラム動作ログを記憶する。そして、各プログラム動作ログのデータに基づくハッシュ値を対応付けて記憶する。例えば、図１１に示すように、「プログラム」“ＰＥ１”が「動作内容」“起動”を「動作日時」“y7/m7/d7/h7/mm7/s7”におこなったことを示すプログラム動作ログを記憶する。そして、プログラム動作ログ３６７ｂは、「プログラム」、「動作内容」、「動作日時」を含

むプログラム動作ログに基づく「ハッシュ値」は、“プログラム動作ログハッシュ値１”である。

【００５２】

（Ｐ－ＥＭＡサーバで実行されるハッシュ値ログのハッシュ値算出処理）

図１２は、Ｐ－ＥＭＡサーバで実行されるハッシュ値ログのハッシュ値算出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０のハッシュ値ログ送受信部３７１は、ハッシュ値ログのハッシュ値算出タイミングであるか否かを判定する（ステップＳ１１）。例えば、ハッシュ値ログのハッシュ値算出タイミングは、保守サーバ１００または保守端末２００から受信したハッシュ値ログがｎ（ｎは自然数）件に達したか否かなどである。ハッシュ値ログのハッシュ値算出タイミングであると判定した場合（ステップＳ１１Ｙｅｓ）、ハッシュ値ログ送受信部３７１は、ステップＳ１２へ処理を移す。一方、ハッシュ値ログのハッシュ値算出タイミングでないと判定した場合（ステップＳ１１Ｎｏ）、ハッシュ値ログ送受信部３７１は、ステップＳ１１を繰り返す。

【００５３】

ステップＳ１２では、ハッシュ値ログ送受信部３７１は、ｎ件のハッシュ値ログのハッシュ値を算出する。そして、ハッシュ値ログ送受信部３７１は、算出したハッシュ値を、算出の基礎となったハッシュ値ログに対応付けてハッシュ値ログ３６２ｂに記憶させるとともに、算出したハッシュ値をＨ－ＥＭＡサーバ４００へ送信する（ステップＳ１３）。ステップＳ１３の処理が終了すると、ハッシュ値ログ送受信部３７１は、処理を終了する。

【００５４】

（Ｐ－ＥＭＡサーバで実行されるペアリングテーブル更新ログのハッシュ値算出処理）

図１３は、Ｐ－ＥＭＡサーバで実行されるペアリングテーブル更新ログのハッシュ値算出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０のテーブル更新部３７２は、ペアリングテーブル更新ログ３６３ｂにおいて、更新前のペアリングテーブル３６３ａを待避させる（ステップＳ２１）。そして、テーブル更新部３７２は、ペアリングテーブル３６３ａを更新する（ステップＳ２２）。

【００５５】

そして、テーブル更新部３７２は、更新後のペアリングテーブル３６３ａのハッシュ値を算出する。そして、テーブル更新部３７２は、算出したハッシュ値を、算出の基礎となった更新前のペアリングテーブル３６３ａに対応付けてペアリングテーブル更新ログ３６３ｂに記憶させる（ステップＳ２３）。そして、テーブル更新部３７２は、算出したハッシュ値をＨ－ＥＭＡサーバ４００へ送信する（ステップＳ２４）。ステップＳ２４の処理が終了すると、テーブル更新部３７２は、処理を終了する。

【００５６】

（Ｐ－ＥＭＡサーバで実行されるアクセスログのハッシュ値算出処理）

図１４は、Ｐ－ＥＭＡサーバで実行されるアクセスログのハッシュ値算出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０のアクセス監視部３７３は、アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスがあるか否かを判定する（ステップＳ３１）。アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスがある場合（ステップＳ３１Ｙｅｓ）、アクセス監視部３７３は、ステップＳ３２へ処理を移す。一方、アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスがない場合（ステップＳ３１Ｎｏ）、アクセス監視部３７３は、ステップＳ３１を繰り返す。

【００５７】

なお、アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスがない場合（ステップＳ３１Ｎｏ）は、アクセスが許可されない外部の装置からのアクセスがなった場合も含む。この場合も、アクセス監視部３７３は、図９に示すアクセスログ３６４ｂに、「アクセス」、「アクセス日時」、「アクセス内容および対応アクション」、「ハッシュ値」を記憶させる。この場合、「アクセス内容および対応アクション」は、

“アクセスが許可されない外部の装置からのアクセス→ブロック”という内容になる。

【００５８】

ステップＳ３２では、アクセス監視部３７３は、アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスのログをアクセスログ３６４ｂに記憶させる。そして、アクセス監視部３７３は、アクセスが許可された保守サーバ１００もしくは保守端末２００からのアクセスのログに基づくハッシュ値を算出し、算出の基礎となったアクセスのログに対応付けてアクセスログ３６４ｂに記憶させる（ステップＳ３３）。そして、アクセス監視部３７３は、算出したハッシュ値をＨ－ＥＭＡサーバ４００へ送信する（ステップＳ３４）。ステップＳ３４が終了すると、アクセス監視部３７３は、処理を終了する。

【００５９】

（Ｐ－ＥＭＡサーバで実行されるプログラム管理テーブル更新ログのハッシュ値算出処理）

図１５は、Ｐ－ＥＭＡサーバで実行されるプログラム管理テーブル更新ログのハッシュ値算出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０のプログラム更新部３７４は、更新前の該当プログラムをプログラム更新ログ３６５ｂに待避させる（ステップＳ４１）。そして、プログラム更新部３７４は、該当プログラムおよびプログラム管理テーブル３６５ａの該当プログラム部分を更新する（ステップＳ４２）。そして、プログラム更新部３７４は、ＴＰＭチップ３５０により、更新後の該当プログラムおよびプログラム管理テーブルのハッシュ値を算出する（ステップＳ４３）。そして、プログラム更新部３７４は、算出した更新後の該当プログラムおよびプログラム管理テーブルのハッシュ値を、Ｈ－ＥＭＡサーバ４００へ送信する（ステップＳ４４）。そして、プログラム更新部３７４は、ＴＰＭチップ３５０により、算出した更新後の該当プログラムおよびプログラム管理テーブルのハッシュ値を、ＴＰＭ拡張保護領域３６８に記憶させる（ステップＳ４５）。ステップＳ４５の処理が終了すると、プログラム更新部３７４は、処理を終了する。

【００６０】

なお、ＴＰＭ拡張保護領域３６８に記憶された更新後のプログラムおよびプログラム管理テーブルのハッシュ値は、Ｐ－ＥＭＡサーバ３００の再起動時もしくは所定周期で、プログラムおよびプログラム管理テーブルの真正性を確認するために、参照される。

【００６１】

（Ｐ－ＥＭＡサーバで実行されるプログラム実行ログのハッシュ値算出処理）

図１６は、Ｐ－ＥＭＡサーバで実行されるプログラム実行ログのハッシュ値算出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０のプログラム実行監視部３７５は、Ｐ－ＥＭＡサーバ３００で実行中のプログラムの実行ログを取得し、プログラム動作ログ３７６ｂに記憶させる（ステップＳ５１）。そして、プログラム実行監視部３７５は、プログラムの実行ログごとに当該プログラムの実行ログに基づくハッシュ値を算出する。そして、プログラム実行監視部３７５は、プログラムの実行ログに基づくハッシュ値を、算出の基礎となったプログラムの実行ログに対応付けてプログラム動作ログ３６７ｂに記憶させる（ステップＳ５２）。そして、プログラム実行監視部３７５は、算出したプログラムの実行ログに基づくハッシュ値を、Ｈ－ＥＭＡサーバ４００へ送信する（ステップＳ５３）。ステップＳ５３の処理が終了すると、プログラム実行監視部３７５は、処理を終了する。

【００６２】

（Ｐ－ＥＭＡサーバで実行される不正プログラム検出処理）

図１７は、Ｐ－ＥＭＡサーバで実行される不正プログラム検出処理を示すフローチャートである。先ず、Ｐ－ＥＭＡサーバ３００の制御部３７０の不正プログラム検出部３７６は、Ｐ－ＥＭＡサーバ３００内の全てのファイルの属性をチェックする（ステップＳ６１）。そして、不正プログラム検出部３７６は、Ｐ－ＥＭＡサーバ３００内のファイルのうち、実行属性を持つファイルを一時テーブル３６９に記憶させる（ステップＳ６２）。そ

して、不正プログラム検出部３７６は、一時テーブル３６９に記憶される実行属性を持つファイルのうち、Ｐ－ＥＭＡサーバ３００のＯＳおよびミドルウェアのファイルを除外する（ステップＳ６３）。そして、不正プログラム検出部３７６は、ＯＳおよびミドルウェアのファイルを除外された実行属性を持つファイルが記憶される一時テーブル３６９と、プログラム管理テーブル３６５ａとを比較する（ステップＳ６４）。

【００６３】

そして、ＯＳおよびミドルウェアのファイルを除外した実行属性を持つファイルが記憶される一時テーブル３６９と、プログラム管理テーブル３６５ａとの内容が一致する場合（ステップＳ６５Ｙｅｓ）、不正プログラム検出部３７６は、処理を終了する。一方、ＯＳおよびミドルウェアのファイルを除外した実行属性を持つファイルが記憶される一時テーブル３６９と、プログラム管理テーブル３６５ａとの内容が一致しない場合（ステップＳ６５Ｎｏ）、不正プログラム検出部３７６は、ステップＳ６６へ処理を移す。

【００６４】

ステップＳ６６では、不正プログラム検出部３７６は、一時テーブル３６９に存在し、かつ、プログラム管理テーブル３６５ａに存在しないプログラムの動作ログをプログラム動作ログ３６７ｂから取得して保存する。そして、不正プログラム検出部３７６は、ステップＳ６６で取得した、一時テーブル３６９に存在し、かつ、プログラム管理テーブル３６５ａに存在しないプログラムの動作ログに基づくハッシュ値を算出する（ステップＳ６７）。そして、不正プログラム検出部３７６は、一時テーブル３６９の内容に基づくハッシュ値を算出する（ステップＳ６８）。そして、不正プログラム検出部３７６は、ステップＳ６７およびステップＳ６８で算出した各ハッシュ値を、Ｈ－ＥＭＡサーバ４００へ送信する（ステップＳ６９）。

【００６５】

（Ｈ－ＥＭＡサーバの構成）

図１９は、実施形態にかかるＨ－ＥＭＡサーバの構成を示すブロック図である。図１８に示すように、実施形態にかかるＨ－ＥＭＡサーバ４００は、入力部４２０、表示部４３０、インターフェース部４４０、ＴＰＭチップ４５０、記憶部４６０、制御部４７０を有する。Ｈ－ＥＭＡサーバ４００が有する各構成要素は、バス４８０によって相互に接続される。入力部４２０、表示部４３０は、Ｐ－ＥＭＡサーバ３００の入力部３２０、表示部３３０と同様の機能を有する。インターフェース部４４０は、Ｐ－ＥＭＡサーバ３００と接続するためのインターフェースである。

【００６６】

ＴＰＭチップ４５０は、Ｐ－ＥＭＡサーバ３００のＴＰＭチップ３５０と同様であり、後述するように、制御部４７０と協働して動作し、Ｐ－ＥＭＡサーバ３００との通信の安全性を保証する。例えば、ＴＰＭチップ４５０は、制御部４７０の各部からの要求に応じて、情報のハッシュ値算出（ハッシュ化）や、ＴＰＭチップにより暗号化された情報を復号する。

【００６７】

記憶部４６０は、ポリシーテーブル４６１、ハッシュ値ログのハッシュ値４６２、ペアリングテーブル更新ログのハッシュ値４６３を有する。また、記憶部４６０は、アクセスログのハッシュ値４６４、プログラム管理テーブル更新ログのハッシュ値４６５、プログラム動作ログのハッシュ値４６６、一時テーブルのハッシュ値４６７を有する。ポリシーテーブル４６１については、後述する。記憶部４６０は、例えば、ハードディスク装置、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ（Flash Memory）などの半導体メモリ素子などの記憶装置である。

【００６８】

制御部４７０は、ハッシュ値送受信部４７１、監査処理実行部４７２を有する。制御部４７０は、ポリシーテーブル４６１に記述されたポリシーにしたがい動作する。制御部４７０は、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）などの集積装置である。または、制御部４７０は

、例えば、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）などの電子回路である。

【００６９】

ハッシュ値送受信部４７１は、Ｐ－ＥＭＡサーバ３００から受信した、ＴＰＭチップ３５０によりハッシュ値が算出されて付加された各種情報を受信し、記憶部４６０に記憶させる。各種情報は、ハッシュ値ログ３６２ｂのハッシュ値、ペアリングテーブル更新ログ３６３ｂのハッシュ値である。また、各種情報は、アクセスログ３６４ｂのハッシュ値、プログラム更新ログ３６５ｂのハッシュ値、プログラム動作ログ３６７ｂのハッシュ値、一時テーブル３６９のハッシュ値である。

【００７０】

ハッシュ値ログ３６２ｂのハッシュ値は、ハッシュ値ログのハッシュ値４６２に記憶される。また、ペアリングテーブル更新ログ３６３ｂのハッシュ値は、ペアリングテーブル更新ログのハッシュ値４６３に記憶される。また、アクセスログ３６４ｂのハッシュ値は、アクセスログのハッシュ値４６４に記憶される。また、プログラム更新ログ３６５ｂのハッシュ値は、プログラム更新ログのハッシュ値４６５に記憶される。また、プログラム動作ログ３６７ｂのハッシュ値は、プログラム動作ログのハッシュ値４６６に記憶される。また、一時テーブル３６９のハッシュ値は、一時テーブルのハッシュ値４６７に記憶される。

【００７１】

監査処理実行部４７２は、後述する監査処理を実行し、ポリシーテーブル４６１に記述されるポリシーに沿って、監査結果に応じたアクションを実行する。

【００７２】

（Ｈ－ＥＭＡサーバが有するポリシーテーブル）

図１９は、Ｈ－ＥＭＡサーバが有するポリシーテーブルを示す図である。ポリシーテーブル４６１は、Ｈ－ＥＭＡサーバ４００の動作ポリシーを記述する。ポリシーテーブル４６１は、例えば、「ハッシュ値不一致の場合のアクション」が“Ｐ－ＥＭＡサーバ停止”であるとは、具体的には、次の処理を指す。図１７のステップＳ６５でＮｏとなり、ステップＳ６９で、Ｐ－ＥＭＡサーバ３００から、一時テーブル３６９に存在し、かつ、プログラム管理テーブル３６５ａに存在しないプログラムの動作ログおよび一時テーブル３６９に基づくハッシュ値が送信されたとする。この場合に、Ｐ－ＥＭＡサーバ３００の非改竄性が保証できないとして、Ｐ－ＥＭＡサーバ３００を停止させることを指す。そのほか、ポリシーテーブル４６１は、図１９に示すように、「ハッシュ値ログのハッシュ値の保存期間」、「ペアリングテーブル更新ログハッシュ値の保存期間」など、Ｐ－ＥＭＡサーバ３００から受信した各ハッシュ値の保存期間などの規定が記述される。

【００７３】

同様に、ハッシュ値ログのハッシュ値４６２、ペアリングテーブル更新ログのハッシュ値４６３、アクセスログのハッシュ値４６４は、Ｐ－ＥＭＡサーバ３００から送信され、記憶するハッシュ値である。また、プログラム更新ログのハッシュ値４６５、プログラム動作ログのハッシュ値４６６、一時テーブルのハッシュ値４６７は、Ｐ－ＥＭＡサーバ３００から送信され、記憶するハッシュ値である。

【００７４】

（Ｈ－ＥＭＡサーバで実行されるＰ－ＥＭＡサーバ監査処理）

図２０は、Ｈ－ＥＭＡサーバで実行されるＰ－ＥＭＡサーバ監査処理を示すフローチャートである。先ず、Ｈ－ＥＭＡサーバ４００の監査処理実行部４７２は、Ｐ－ＥＭＡサーバ３００の監査対象のハッシュ値を決定する（ステップＳ７１）。そして、監査処理実行部４７２は、Ｐ－ＥＭＡサーバ３００から、監査対象の該当部分のハッシュ値を取得する（ステップＳ７２）。そして、監査処理実行部４７２は、自装置であるＨ－ＥＭＡサーバ４００が記憶するハッシュ値と、Ｐ－ＥＭＡサーバ３００から取得したハッシュ値とが一致するか否かを判定する（ステップＳ７３）。自装置であるＨ－ＥＭＡサーバ４００が記憶するハッシュ値と、Ｐ－ＥＭＡサーバ３００から取得したハッシュ値とが一致する場合

（ステップＳ７３Ｙｅｓ）、監査処理実行部４７２は、監査異常なしとして、処理を終了する。

【００７５】

一方、自装置であるＨ－ＥＭＡサーバ４００が記憶するハッシュ値と、Ｐ－ＥＭＡサーバ３００から取得したハッシュ値とが一致しない場合（ステップＳ７３Ｎｏ）、監査処理実行部４７２は、監査異常ありとする。例えば、監査処理実行部４７２は、ポリシーテーブル４６１の規定にしたがい、Ｐ－ＥＭＡサーバ３００に対して、稼働停止を指示する（ステップＳ７４）。つまり、Ｐ－ＥＭＡサーバ３００から、Ｐ－ＥＭＡの権限を剥奪する。ステップＳ７４の処理が終了すると、監査処理実行部４７２は、処理を終了する。なお、ステップＳ７４の処理は、一例を示すに過ぎず、例えば、ポリシーテーブル４６１に、Ｐ－ＥＭＡ３００の設置現場へ向かい、原因調査をおこなう指示を出力するポリシーが記述されているならば、その旨の指示を表示部４３０から出力することになる。つまり、ステップＳ７４の処理は、ポリシーテーブル４６１に記述されている規定内容に応じたものになる。

【００７６】

以上の実施形態によれば、Ｐ－ＥＭＡサーバ３００からＨ－ＥＭＡサーバ４００へ送信されるハッシュ値は、ハッシュ値の算出基礎となるログとともに送信されることとした。しかし、ハッシュ値の算出基礎となるログを識別する情報であれば、いずれの情報であってもよい。ハッシュ値の算出基礎となるログを識別する情報が、ハッシュ値とともにＨ－ＥＭＡサーバ４００へ送信されることによっても、Ｐ－ＥＭＡサーバ３００が保持するログの監査をおこなうことができる。

【００７７】

また、Ｐ－ＥＭＡサーバ３００からＨ－ＥＭＡサーバ４００へ送信されるハッシュ値は、各ログの１件ごとに基づくハッシュ値であってもよい。または、Ｐ－ＥＭＡサーバ３００からＨ－ＥＭＡサーバ４００へ送信されるハッシュ値は、装置グループ、日時、各ログの内容もしくは種別などに基づきとりまとめた各ログの複数ごとに基づくハッシュ値であってもよい。

【００７８】

（実施形態による効果）

以上の実施形態によれば、例えば、Ｐ－ＥＭＡサーバ３００は、保守サーバ１００や保守端末２００から受信したハッシュ値ログを蓄積し、蓄積したログをポリシーにしたがってまとめた情報に基づくハッシュ値を算出する。また、例えば、Ｐ－ＥＭＡサーバ３００は、自装置へのアクセスログ、プログラムの実行ログ、プログラムの更新ログを蓄積し、蓄積したログに基づきハッシュ値を算出する。そして、例えば、Ｐ－ＥＭＡサーバ３００は、算出したハッシュ値を、Ｈ－ＥＭＡサーバ４００へ保管させる。これにより、例えば、Ｈ－ＥＭＡサーバ４００は、自装置が保管するハッシュ値に基づきＰ－ＥＭＡサーバ３００を何時でも監査でき、Ｐ－ＥＭＡサーバ３００の非改竄性を担保することができる。

【００７９】

また、例えば、Ｐ－ＥＭＡサーバ３００は、自装置で動作するプログラムのインストールおよび更新を、専用の更新プログラムでのみ実施可能とする。このため、例えば、Ｐ－ＥＭＡサーバ３００は、意図しない不正なプログラムがインストールされたり、意図しないプログラムの更新がなされたりすることを防止でき、自装置で動作するプログラムの正当性を確保できる。

【００８０】

さらに、例えば、Ｐ－ＥＭＡサーバ３００は、自装置で動作するプログラムを管理テーブルで管理し、プログラムのインストールおよび更新の都度、管理テーブルを更新する。また、例えば、Ｐ－ＥＭＡサーバ３００は、専用の更新プログラムでプログラムのインストールおよび更新をおこなう際には、動作ログを蓄積する。そして、例えば、Ｐ－ＥＭＡサーバ３００は、管理テーブルの変更履歴をログとして蓄積し、専用の更新プログラムの動作ログとともに、ハッシュ値を算出する。そして、例えば、Ｐ－ＥＭＡサーバ３００は

、算出したハッシュ値を、Ｈ－ＥＭＡサーバ４００へ保管させる。これにより、例えば、Ｈ－ＥＭＡサーバ４００は、自装置が保管するハッシュ値に基づきＰ－ＥＭＡサーバ３００で動作するプログラムに関して何時でも監査でき、Ｐ－ＥＭＡサーバ３００のプログラムの非改竄性をより強く担保することができる。

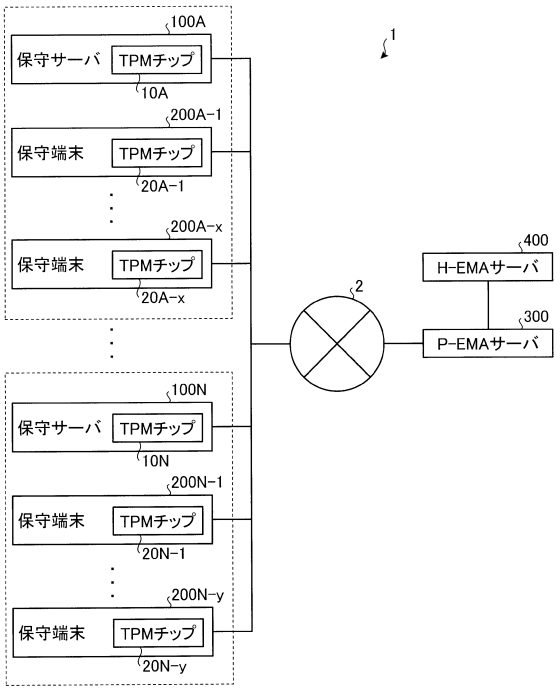
【符号の説明】

【００８１】

１　システム
１００Ａ、・・・、１００Ｎ　保守サーバ
２００Ａ－１、・・・、２００Ａ－ｘ、２００Ｎ－１、・・・、２００Ｎ－ｙ　保守端末
３００　Ｐ－ＥＭＡサーバ
３１０　通信部
３２０　入力部
３３０　表示部
３４０　インターフェース部
３５０　ＴＰＭチップ
３６０　記憶部
３６１ａ　ポリシーテーブル
３６２ｂ　ハッシュ値ログ
３６３ａ　ペアリングテーブル
３６３ｂ　ペアリングテーブル更新ログ
３６４ｂ　アクセスログ
３６５ａ　プログラム管理テーブル
３６５ｂ　プログラム更新ログ
３６６　ファイル群
３６７ｂ　プログラム動作ログ
３６８　ＴＰＭ拡張保護領域
３６９　一時テーブル
３７０　制御部
３７１　ハッシュ値ログ送受信部
３７２　テーブル更新部
３７３　アクセス監視部
３７４　プログラム更新部
３７５　プログラム実行監視部
３７６　不正プログラム検出部
４００　Ｈ－ＥＭＡサーバ
４２０　入力部
４３０　表示部
４４０　インターフェース部
４５０　ＴＰＭチップ
４６０　記憶部
４６１　ポリシーテーブル
４６２　ハッシュ値ログのハッシュ値
４６３　ペアリングテーブル更新ログのハッシュ値
４６４　アクセスログのハッシュ値
４６５　プログラム更新ログのハッシュ値
４６６　プログラム動作ログのハッシュ値
４６７　一時テーブルのハッシュ値
４７０　制御部
４７１　ハッシュ値送受信部
４７２　監査処理実行部

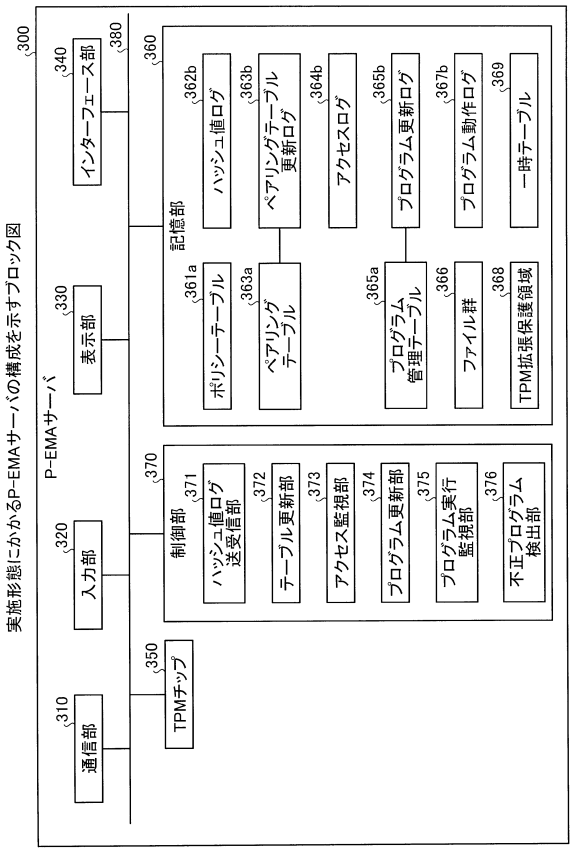
【図１】

実施形態にかかるシステム構成を示す図



【図２】

実施形態にかかるP-EMAサーバの構成を示すブロック図



【図３】

P-EMAサーバが有するポリシーテーブルを示す図

361a

ポリシー	n件
ハッシュ値ログのハッシュ値を算出するデータ数の単位	X1日
ペアリングテーブル更新ログの保存期間	X2日
ペアリングテーブル更新ログのハッシュ値算出サイクル	X3日
アクセスログの保存期間	X4日
アクセスログのハッシュ値算出サイクル	X5日
プログラム管理テーブルログの保存期間	X6日
プログラム管理テーブルログのハッシュ値算出サイクル	X7日
プログラム実行ログの保存期間	X8日
プログラム実行ログのハッシュ値算出サイクル	X9日
・ ・ ・	・ ・ ・

【図４】

P-EMAサーバが有するペアリングテーブルを示す図

363a

保守サーバ	保守端末
AAA	A001
	A002
	・ ・ ・
BBB	B001
	B002
	・ ・ ・
・ ・ ・	・ ・ ・

【図５】

P-EMAサーバが有するプログラム管理テーブルを示す図

365a

プログラム	インストール日時	初期バージョン	最終更新日時	最新バージョン
PE1	y1/m1/d1/h1/mm1/s1	V1	Y1/M1/D1/H1/MM1/S1	V3
PE2	y2/m2/d2/h2/mm2/s2	V2	Y2/M2/D2/H2/MM2/S2	V4
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図６】

P-EMAサーバが有するファイル群を示す図

366

ファイル
F1
F2
・ ・ ・

【図７】

P-EMAサーバが有するハッシュ値ログを示す図

362b

ハッシュ値ログ		ハッシュ値
ハッシュ値	算出日時	
ハッシュ値1	y3/m3/d3/h3/mm3/s3	ハッシュ値H1
ハッシュ値2	y4/m4/d4/h4/mm4/s4	
・ ・ ・	・ ・ ・	
ハッシュ値n	・・・	
・ ・ ・	・ ・ ・	・ ・ ・

【図８】

P-EMAサーバが有するペアリングテーブル更新ログを示す図

363b

更新日時	更新前テーブルデータ	ハッシュ値
Y3/M3/D3/H3/MM3/S3	ペアリングテーブルデータ1	ペアリングテーブルハッシュ値1
Y4/M4/D4/H4/MM4/S4	ペアリングテーブルデータ2	ペアリングテーブルハッシュ値2
・ ・ ・	・ ・ ・	・ ・ ・

【図９】

P-EMAサーバが有するアクセスログを示す図

364b

アクセス	アクセス日時	アクセス内容および 対応アクション	ハッシュ値
アクセス1	y5/m5/d5/h5/mm5/s5	保守サーバXからのアクセス →ブロック	アクセスハッシュ値1
アクセス2	y6/m6/d6/h6/mm6/s6	保守端末Xからのアクセス →許可	アクセスハッシュ値2
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図１０】

P-EMAサーバが有するプログラム更新ログを示す図

365b

更新日時	更新前プログラムデータ	更新後プログラムデータ	ハッシュ値	更新前プログラム管理テーブルデータ	更新後プログラム管理テーブルデータ	ハッシュ値
Y5/M5/D5/H5/MM5/S5	更新前プログラムデータ1	更新後プログラムデータ1	更新後プログラムデータハッシュ値1	更新前プログラム管理テーブルデータ1	更新後プログラム管理テーブルデータハッシュ値1	・・・
Y6/M6/D6/H6/MM6/S6	更新前プログラムデータ2	更新後プログラムデータ2	更新後プログラムデータハッシュ値2	更新前プログラム管理テーブルデータ2	更新後プログラム管理テーブルデータハッシュ値2	・・・
・・・	・・・	・・・	・・・	・・・	・・・	・・・

【図１１】

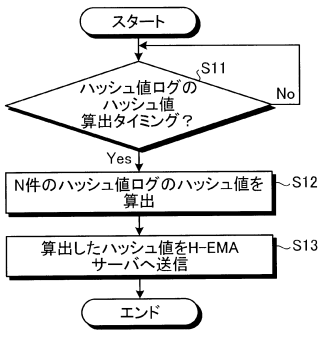
P-EMAサーバが有するプログラム動作ログを示す図

367b

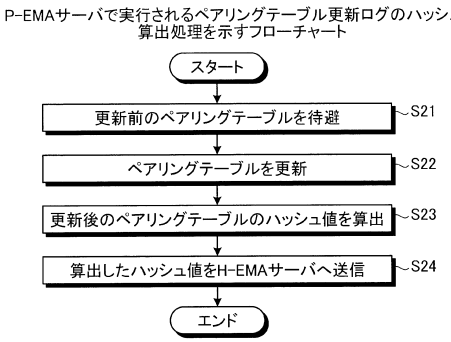
プログラム動作ログ			ハッシュ値
プログラム	動作内容	動作日時	
PE1	起動	y7/m7/d7/h7/mm7/s7	プログラム動作ログ ハッシュ値1
PE2	データ2を受信	y8/m8/d8/h8/mm8/s8	プログラム動作ログ ハッシュ値2
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
PEx	終了	・・・	プログラム動作ログ ハッシュ値x
・ ・ ・	・ ・ ・	・ ・ ・	・・・

【図１２】

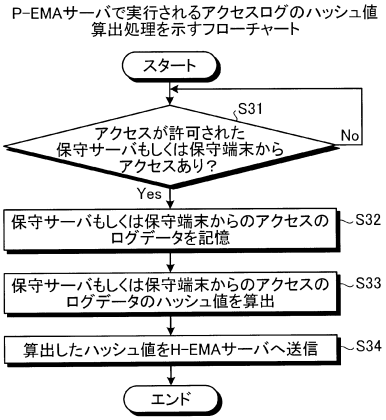
P-EMAサーバで実行されるハッシュ値ログのハッシュ値算出処理を示すフローチャート



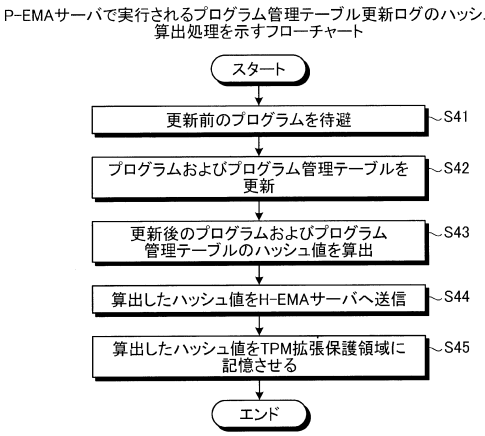
【図１３】



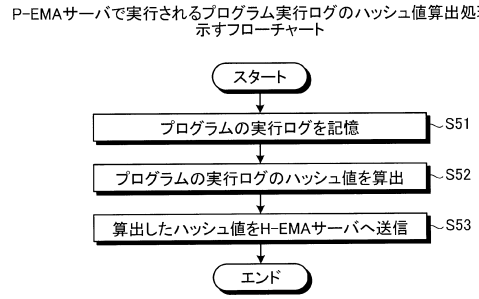
【図１４】



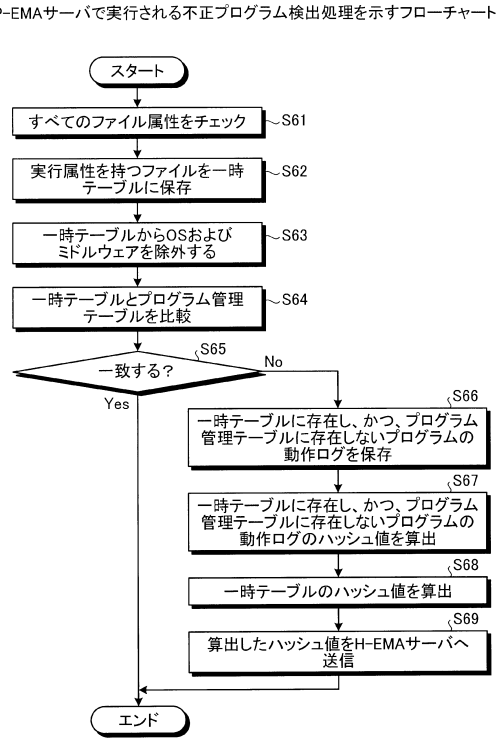
【図１５】



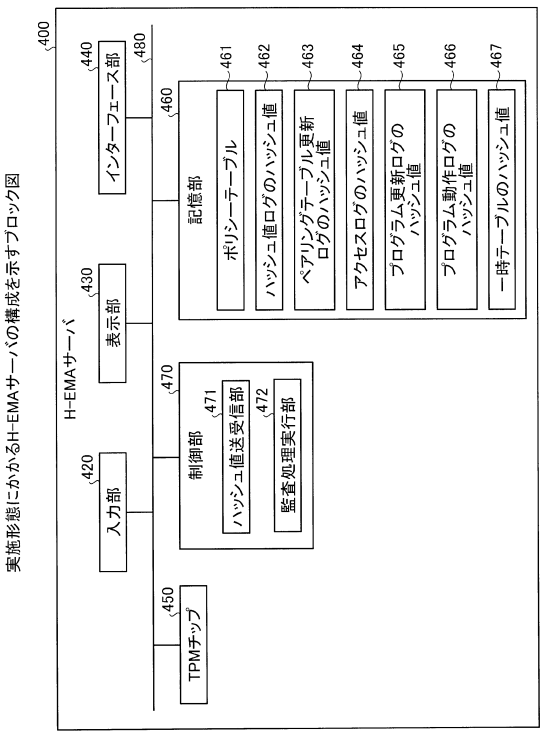
【図１６】



【図１７】



【図１８】



【図１９】

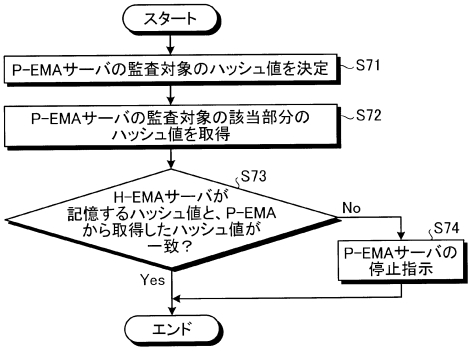
H-EMAサーバが有するポリシーテーブルを示す図

461

ポリシー	
ハッシュ値不一致の場合のアクション	P-EMAサーバ停止指示
ハッシュ値ログのハッシュ値の保存期間	Y1日
ペアリングテーブル更新ログのハッシュ値の保存期間	Y2日
アクセスログハッシュ値の保存期間	Y3日
アクセスログのハッシュ値の保存期間	Y4日
プログラム管理テーブルログハッシュ値の保存期間	Y5日
プログラム実行ログハッシュ値の保存期間	Y6日
・ ・ ・	・ ・ ・

【図２０】

H-EMAサーバで実行されるP-EMAサーバ監査処理を示すフローチャート



フロントページの続き

(72)発明者　今野　淳
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内
(72)発明者　小谷　誠剛
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　藤野　明夫
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

審査官　戸島　弘詩

(56)参考文献　特開平０３－２３３６２９（ＪＰ，Ａ）
特開２００８－２１７５３３（ＪＰ，Ａ）
特開２００９－１２９２２０（ＪＰ，Ａ）
特開平０９－２８８５７７（ＪＰ，Ａ）
特開２００３－８５０４６（ＪＰ，Ａ）
伊藤　幸夫，Ｌｉｎｕｘ逆引き大全　５５５の極意　コマンド編［第２版］，株式会社秀和システム，２０１１年　3月２９日，第1版，５９１，１２３，１２６頁
中井　奨，ウイルス対策もクラウドの時代，日経コンピュータ，日本，日経ＢＰ社，２００８年１２月　1日，ｎｏ．７１８，２０頁
早川　薫，プラットフォーム部分認証，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１１年　7月２１日，Ｖｏｌ．１１１，Ｎｏ．１６３，２０～２１頁
江川　友寿，ＩａａＳ環境における安全な帯域外リモート管理機構，情報処理学会研究報告　２０１２（平成２４）年度（３）　［ＣＤ－ＲＯＭ］，日本，一般社団法人情報処理学会，２０１２年１０月１５日，４頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００，１３／００，９／４４５
Ｈ０４Ｌ９／００
Ｇ０９Ｃ１／００