(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2011-108167
(P2011-108167A)
(43)公開日　平成23年6月2日(2011.6.2)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 9/445	(2006.01)	G06F	9/06	610K	5B276
G06F 11/00	(2006.01)	G06F	9/06	630B	5B376
G06F 21/22	(2006.01)	G06F	9/06	610Q	
		G06F	9/06	660J	

審査請求 未請求　請求項の数 6　OL　（全 24 頁）

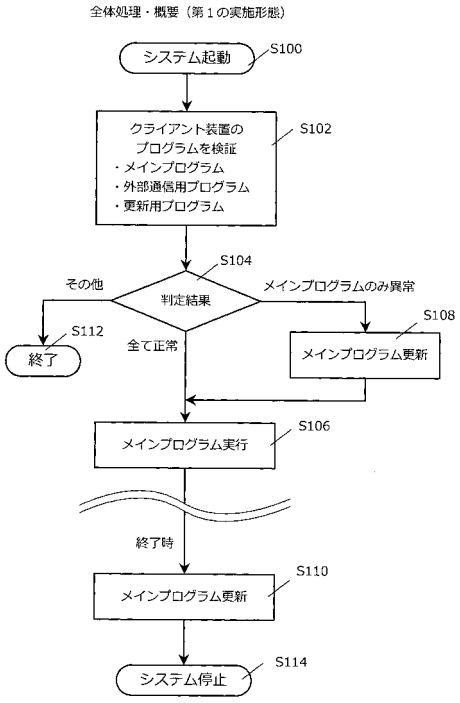
(21)出願番号　特願2009-265150 (P2009-265150)
(22)出願日　平成21年11月20日 (2009.11.20)

(71)出願人　502087460
株式会社トヨタＩＴ開発センター
東京都港区赤坂６丁目６番２０号
(71)出願人　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100100549
弁理士　川口　嘉之
(74)代理人　100106622
弁理士　和久田　純一
(74)代理人　100085006
弁理士　世良　和信
(74)代理人　100089244
弁理士　遠山　勉

最終頁に続く

(54)【発明の名称】コンピューターシステム

(57)【要約】
【課題】システム停止時のソフトウェアリモート更新と、システム起動時のプログラムの正当性検査を行うシステムにおいて、更新処理が失敗した場合でもプログラムを安全に普及可能なコンピューターシステムを提供する。
【解決手段】コンピューターシステムは、メインプログラムと、メインプログラムを更新するための更新用プログラムと、外部と通信するための外部通信用プログラムを有するクライアント装置と、クライアント装置のプログラムが正常か否かを検査するとともに、更新用プログラムを配布するサーバ装置から構成される。システム終了時に更新用プログラムによってメインプログラムの更新を行う。システム起動時は、上記３つのプログラムのダイジェスト値をサーバ装置に送信し、全てが正常の場合はメインプログラムを実行し、メインプログラムのみ異常の場合はメインプログラムの更新処理を実行し、それ以外の場合は処理を停止する。
【選択図】図４



【特許請求の範囲】
【請求項１】
互いに通信可能なサーバ装置と複数のクライアント装置とから構成され、
前記クライアント装置は、
プロセッサと、
メインプログラム、前記メインプログラムを更新するための更新用プログラム、サーバ装置および他のクライアント装置と通信を行うための外部通信用プログラムを記憶する記憶手段と、
を有し、
前記サーバ装置は、
クライアント装置が記憶しているメインプログラムを記憶する現在プログラム記憶部と、
クライアント装置に配布すべき最新版のメインプログラムを記憶する更新プログラム記憶部と、
クライアント装置に最新版のメインプログラムを配布する更新プログラム管理部と、
クライアント装置と通信を行うための外部通信部と、
を有し、
クライアント装置が前記更新用プログラムを実行することにより、最新版のメインプログラムをサーバ装置から取得して、前記記憶手段内のメインプログラムを更新するコンピューターシステムであって、
前記クライアント装置は、前記メインプログラム、前記更新用プログラムおよび前記外部通信用プログラムのダイジェスト値を求めるための、耐タンパ性デバイスで構成されたコード測定部をさらに有し、
前記サーバ装置は、各クライアント装置について、メインプログラム、更新用プログラムおよび外部通信用プログラムの正しいダイジェスト値を記憶する正常状態記憶部をさらに有し、
クライアント装置は、起動時に、メインプログラム、更新用プログラムおよび外部通信用プログラムのダイジェスト値をコード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から受信した３つのダイジェスト値それぞれが正しいか否か判定し、
クライアント装置は、前記３つのハッシュの全てが正しい場合はメインプログラムを実行し、メインプログラムのダイジェスト値のみが異常の場合は更新用プログラムによってメインプログラムの更新を実行し、それ以外の場合は起動処理を終了する
ことを特徴とするコンピューターシステム。
【請求項２】
メインプログラムのダイジェスト値のみが異常であって更新用プログラムによってメインプログラムの更新を実行するときに、
サーバ装置の更新プログラム管理部は、更新プログラム記憶部に最新版のメインプログラムが存在する場合は当該メインプログラムをクライアント装置に配布し、更新プログラム記憶部に最新版のメインプログラムが存在しない場合は、現在プログラム記憶部内のメインプログラムをクライアント装置に配布する
ことを特徴とする請求項１に記載のコンピューターシステム。
【請求項３】
前記サーバ装置は、クライアント装置から受信した前記３つのダイジェスト値の全てが正しい場合は、前記コンピューターシステム内で共通の暗号鍵をクライアント装置に送信し、
前記クライアント装置は、メインプログラム実行後にサーバ装置または他のクライアント装置と通信する場合は前記暗号鍵を用いた通信を行い、他のクライアント装置からの通信に前記暗号鍵が用いられていない場合は当該通信を無視する
ことを特徴とする請求項１または２に記載のコンピューターシステム。

【請求項４】
互いに通信可能なサーバ装置と複数のクライアント装置とから構成され、
前記クライアント装置は、
プロセッサと、
メインプログラム、前記メインプログラムを更新するための更新用プログラム、サーバ装置、他のクライアント装置と通信を行うための外部通信用プログラム、および、前記更新用プログラムによる前記メインプログラムの更新処理を実行中であるか否かを示すフラグを記憶する記憶手段と、
を有し、
前記サーバ装置は、
クライアント装置が記憶しているメインプログラムを記憶する現在プログラム記憶部と、
クライアント装置に配布すべき最新版のメインプログラムを記憶する更新プログラム記憶部と、
クライアント装置に最新版のメインプログラムを配布する更新プログラム管理部と、
クライアント装置と通信を行うための外部通信部と、
を有し、
クライアント装置が前記更新用プログラムを実行することにより、最新版のメインプログラムをサーバ装置から取得して、前記記憶手段内のメインプログラムを更新するコンピューターシステムであって、
前記クライアント装置は、前記メインプログラム、前記更新用プログラムおよび前記外部通信用プログラムのダイジェスト値を求めるための、耐タンパ性デバイスで構成されたコード測定部をさらに有し、
前記サーバ装置は、各クライアント装置について、メインプログラム、更新用プログラムおよび外部通信用プログラムの正しいダイジェスト値を記憶する正常状態記憶部をさらに有し、
（１）クライアント装置の起動時に、前記フラグによってメインプログラムの更新処理の実行中ではないと判断される場合は、
クライアント装置は、メインプログラムおよび外部通信用プログラムのダイジェスト値を前記コード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から送信されるメインプログラムおよび外部通信用プログラムのダイジェスト値が正しいか否か判定し、
クライアント装置は、メインプログラムおよび外部通信用プログラムのダイジェスト値が正しい場合はメインプログラムを実行し、
（２）クライアント装置の起動時に、前記フラグによってメインプログラムの更新処理の実行中であると判断される場合は、
クライアント装置は、更新用プログラムおよび外部通信用プログラムのダイジェスト値を前記コード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から送信される更新用プログラムおよび外部通信用プログラムのダイジェスト値が正しいか否か判定し、
クライアント装置は、更新用プログラムおよび外部通信用プログラムのダイジェスト値が正しい場合は、更新用プログラムによってメインプログラムの更新処理を実行する
ことを特徴とするコンピューターシステム。
【請求項５】
メインプログラムのダイジェスト値のみが異常であって更新用プログラムによってメインプログラムの更新を実行するときに、
サーバ装置の更新プログラム管理部は、更新プログラム記憶部に最新版のメインプログラムが存在しない場合は、クライアント装置の前記フラグが改ざんされたと判断する
ことを特徴とする請求項４に記載のコンピューターシステム。
【請求項６】

前記サーバ装置は、クライアント装置から受信した前記メインプログラムおよび外部通信用プログラムのダイジェスト値が正しい場合は、前記コンピューターシステム内で共通の暗号鍵をクライアント装置に送信し、
前記クライアント装置は、メインプログラム実行後にサーバ装置または他のクライアント装置と通信する場合は、前記暗号鍵を用いて秘匿通信または署名付き通信を行う
ことを特徴とする請求項４または５に記載のコンピューターシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、プログラムを安全に実行可能なコンピューターシステムに関する。

【背景技術】

【０００２】

コンピューターシステムの普及に伴い、セキュリティ保証の重要性がますます高まっている。たとえば、近年電子化が進められている車載コンピューターシステムにおいて、プログラムが改ざんされるなどして車載コンピューターシステムを構成する他のマイコン（Electronic Control Unit、以下ＥＣＵ）や他の車両に対して誤った情報が送出されると危険である。したがって、コンピューターシステムにおいて実行するプログラムが、悪意者による改ざんを受けておらず製造者によって提供された正しいプログラムであることを保証する必要性がある。このようにプログラムの正当性を保証する技術として、車載コンピューターシステムを起動する際に、各ＥＣＵの搭載プログラムが正しいことを確認した後に起動を行うことが提案されている（非特許文献１および２）。

【０００３】

また、車載コンピューターシステムにおいて、製品出荷後にＥＣＵ内に格納されているプログラムを外部から取得して更新することで、機能を修正したり追加したりすることが行われている。しかしながら、このようなプログラム更新処理が正常に終了しなかった場合、プログラムが不整合な状態でメモリ内に格納され、次回起動時にプログラムが改ざんされたと判断されてしまい起動できなくなってしまう。

【０００４】

更新処理の中断に対処するために、更新対象の機器に十分な量の二次記憶を用意し、更新前のプログラムと最新のプログラムの両方を保持可能とし、更新処理が中断した場合には更新前のプログラムを起動する技術が提案されている（特許文献１）。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００５－１９６７４５号公報

【非特許文献】

【０００６】

【非特許文献１】吉岡顕　他，「構成証明機能を持つ車内通信プロトコルの提案」，マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム．

【非特許文献２】H. Oguma, et. al., New Attestation-Based Security Architecture for In-Vehicle Communication, GLOBECOM 2008.

【発明の概要】

【発明が解決しようとする課題】

【０００７】

特許文献１の技術は複合機など比較的計算機資源が豊富な機器を対象としている。しかしながら、車載システムを構成する多くのＥＣＵは計算機資源に乏しくこのような手法を採用することは困難である。また、豊富な二次記憶や特殊なハードウェアをＥＣＵへ導入することは、製造コストの観点からも困難である。なお、このような問題点は車載コンピューターシステムに限られるものではなく、計算機資源に乏しいコンピューターシステム一般に当てはまる問題である。

【０００８】
本発明はこのような問題点を考慮してなされたものであり、その目的は、起動時にプログラムの正当性を検証してから動作するコンピューターシステムにおいて、ソフトウェア更新処理に失敗した場合であっても、プログラムを安全に復旧可能とすることを目的とする。また、本発明は、このようなコンピューターシステムを、特殊なハードウェアをできるだけ使用せず低コストに実現可能とすることも目的とする。
【課題を解決するための手段】
【０００９】
〈第１の態様〉
本発明の第１の態様では、クライアント装置が記憶する、更新処理の対象であるメインプログラムと、更新処理の対象ではないその他のプログラムの正当性の検証を起動時に行い、全てのプログラムが正しい場合はメインプログラムを実行し、メインプログラムのみが異常である場合はメインプログラムの更新処理を実行し、それ以外の場合はプログラムが改ざんされていると判断して実行を中止する。ここで、更新処理の対象ではないプログラムには、メインプログラムを更新するための更新用プログラムおよびサーバ装置や他のクライアントと通信するための外部通信用プログラムが含まれる。
【００１０】
より具体的には、本発明の第１の態様に係るコンピューターシステムは、
互いに通信可能なサーバ装置と複数のクライアント装置とから構成され、
前記クライアント装置は、
プロセッサと、
メインプログラム、前記メインプログラムを更新するための更新用プログラム、サーバ装置および他のクライアント装置と通信を行うための外部通信用プログラムを記憶する記憶手段と、
を有し、
前記サーバ装置は、
クライアント装置が記憶しているメインプログラムを記憶する現在プログラム記憶部と、
クライアント装置に配布すべき最新版のメインプログラムを記憶する更新プログラム記憶部と、
クライアント装置に最新版のメインプログラムを配布する更新プログラム管理部と、
クライアント装置と通信を行うための外部通信部と、
を有し、
クライアント装置が前記更新用プログラムを実行することにより、最新版のメインプログラムをサーバ装置から取得して、前記記憶手段内のメインプログラムを更新するコンピューターシステムであって、
前記クライアント装置は、前記メインプログラム、前記更新用プログラムおよび前記外部通信用プログラムのダイジェスト値を求めるための、耐タンパ性デバイスで構成されたコード測定部をさらに有し、
前記サーバ装置は、各クライアント装置について、メインプログラム、更新用プログラムおよび外部通信用プログラムの正しいダイジェスト値を記憶する正常状態記憶部をさらに有し、
クライアント装置は、起動時に、メインプログラム、更新用プログラムおよび外部通信用プログラムのダイジェスト値をコード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から受信した３つのダイジェスト値それぞれが正しいか否か判定し、
クライアント装置は、前記３つのハッシュの全てが正しい場合はメインプログラムを実行し、メインプログラムのダイジェスト値のみが異常の場合は更新用プログラムによってメインプログラムの更新を実行し、それ以外の場合は起動処理を終了する
ことを特徴とする。

【００１１】
本発明の第１の態様によれば、メインプログラムの更新処理が中断した場合であっても、更新用プログラムおよび外部通信用プログラムの正当性が確保されればメインプログラムの更新処理を再開できる。また、メインプログラムのみが改ざんされた場合も、それを検知してプログラム更新処理により正しいメインプログラムを再取得することができる。さらに、メインプログラム以外のプログラムが改ざんされた場合も検知可能であり、異常なプログラムが実行されることを防止できる。
【００１２】
さらに、本発明の第１の態様において、耐タンパ性デバイスを用いて構成する必要があるものはコード測定部だけであり、メインプログラム、更新用プログラムおよび外部通信用プログラムは通常の記憶装置（耐タンパ性を有しないデバイス）に格納できるため、製造コストの大幅な上昇を避けられる。
【００１３】
また、本発明の第１の態様において、メインプログラムのダイジェスト値のみが異常で更新用プログラムによってメインプログラムの更新を実行するときに、サーバ装置の更新プログラム管理部は、更新プログラム記憶部に最新版のメインプログラムが存在する場合は当該メインプログラムをクライアント装置に配布し、更新プログラム記憶部に最新版のメインプログラムが存在しない場合は、現在プログラム記憶部内のメインプログラムをクライアント装置に配布することが好ましい。
【００１４】
これにより、メインプログラム更新処理に失敗してメインプログラムが異常な場合だけでなく、メインプログラムが改ざんされて異常な場合にも、メインプログラムを復旧して正しいプログラムを実行することができる。
【００１５】
また、本発明の第１の態様において、サーバ装置は、クライアント装置から受信した前記３つのダイジェスト値の全てが正しい場合は、前記コンピューターシステム内で共通の暗号鍵をクライアント装置に送信し、前記クライアント装置は、メインプログラム実行後にサーバ装置または他のクライアント装置と通信する場合は前記暗号鍵を用いた通信を行い、他のクライアント装置からの通信に前記暗号鍵が用いられていない場合は当該通信を無視することが好適である。
【００１６】
このような構成によれば、起動時にプログラムの正当性が検証されたクライアント装置のみが他の装置と通信可能であるため、改ざんされた情報を他のクライアント装置から受け取って誤動作が発生するのを防止できる。
【００１７】
〈第２の態様〉
本発明の第２の態様は、クライアント装置においてメインプログラムを更新途中であるか否かを示すフラグを保持し、起動時において、フラグが更新中を示している場合（つまり更新処理が中断した場合）は更新処理に必要なプログラムの正当性を検証し、プログラムが正しければ更新処理を再開し、フラグが更新中を示していない場合はメインプログラムとメインプログラムの実行に必要な他のプログラムの正当性を検証し、プログラムが正しければメインプログラムを実行する。
【００１８】
より具体的には、本発明の第２の態様に係るコンピューターシステムは、
互いに通信可能なサーバ装置と複数のクライアント装置とから構成され、
前記クライアント装置は、
プロセッサと、
メインプログラム、前記メインプログラムを更新するための更新用プログラム、サーバ装置および他のクライアント装置と通信を行うための外部通信用プログラム、および、前記更新用プログラムによる前記メインプログラムの更新処理を実行中であるか否かを示

すフラグを記憶する記憶手段と、
を有し、
前記サーバ装置は、
クライアント装置が記憶しているメインプログラムを記憶する現在プログラム記憶部と、
クライアント装置に配布すべき最新版のメインプログラムを記憶する更新プログラム記憶部と、
クライアント装置に最新版のメインプログラムを配布する更新プログラム管理部と、
クライアント装置と通信を行うための外部通信部と、
を有し、
クライアント装置が前記更新用プログラムを実行することにより、最新版のメインプログラムをサーバ装置から取得して、前記記憶手段内のメインプログラムを更新するコンピューターシステムであって、
前記クライアント装置は、前記メインプログラム、前記更新用プログラムおよび前記外部通信用プログラムのダイジェスト値を求めるための、耐タンパ性デバイスで構成されたコード測定部をさらに有し、
前記サーバ装置は、各クライアント装置について、メインプログラム、更新用プログラムおよび外部通信用プログラムの正しいダイジェスト値を記憶する正常状態記憶部をさらに有し、
（１）クライアント装置の起動時に、前記フラグによってメインプログラムの更新処理の実行中ではないと判断される場合は、
クライアント装置は、メインプログラムおよび外部通信用プログラムのダイジェスト値を前記コード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から送信されるメインプログラムおよび外部通信用プログラムのダイジェスト値が正しいか否か判定し、
クライアント装置は、メインプログラムおよび外部通信用プログラムのダイジェスト値が正しい場合はメインプログラムを実行し、
（２）クライアント装置の起動時に、前記フラグによってメインプログラムの更新処理の実行中であると判断される場合は、
クライアント装置は、更新用プログラムおよび外部通信用プログラムのダイジェスト値を前記コード測定部によって求めてサーバ装置に送信し、
サーバ装置は、クライアント装置から送信される更新用プログラムおよび外部通信用プログラムのダイジェスト値が正しいか否か判定し、
クライアント装置は、更新用プログラムおよび外部通信用プログラムのダイジェスト値が正しい場合は、更新用プログラムによってメインプログラムの更新処理を実行する
ことを特徴とする。

【００１９】

本発明の第２の態様によれば、第１の態様と同様に、メインプログラムの更新処理が中断した場合であっても、その他のプログラムの正当性が検証されればメインプログラムの更新処理を再開できる。また、耐タンパ性デバイスを用いる必要があるのはコード測定部であり、その他のプログラムは通常の記憶装置に格納できるため、製造コストの上昇を避けることができる点も同様である。

【００２０】

本発明の第２の態様では、起動時に検証する必要のあるプログラムは、フラグが更新中を示す場合は更新用プログラムと外部通信用プログラム、フラグが更新中を示していない場合はメインプログラムと外部通信用プログラムと、いずれの場合も２つのプログラムだけである。第１の態様においては、メインプログラムと更新用プログラムと外部通信用プログラムの３つのプログラムの正当性を検証する必要があるため、これら３つのプログラムのダイジェスト値を求めていた。本態様においては、２つのプログラムのダイジェスト値を求めるだけで済むため、システム起動時の検証処理を少なくして、高速なシステム起

動を可能としている。なお、ダイジェスト値の算出は演算量が比較的多い処理であるため、ダイジェスト値の算出回数を減らすことで得られる効果は大きい。

【００２１】

また、本発明の第２の態様において、メインプログラムのダイジェスト値のみが異常であって更新用プログラムによってメインプログラムの更新を実行するときに、サーバ装置の更新プログラム管理部は、更新プログラム記憶部に最新版のメインプログラムが存在しない場合は、クライアント装置の前記フラグが改ざんされたと判断することが好ましい。

【００２２】

このようにすることで、フラグの改ざんを検知可能である。

【００２３】

また、本発明の第２の態様において、サーバ装置は、クライアント装置から受信した前記メインプログラムおよび外部通信用プログラムのダイジェスト値が正しい場合は、前記コンピューターシステム内で共通の暗号鍵をクライアント装置に送信し、前記クライアント装置は、メインプログラム実行後にサーバ装置または他のクライアント装置と通信する場合は、前記暗号鍵を用いて秘匿通信または署名付き通信を行うことが好適である。

【００２４】

このような構成によれば、起動時にプログラムの正当性が検証されたクライアント装置のみが他の装置と通信可能であるため、改ざんされた情報を他のクライアント装置から受け取って誤動作が発生するのを防止できる。

【００２５】

なお、本発明は、上記手段の少なくとも一部を有するコンピューターシステムとして捉えることができる。また、本発明は、上記処理の少なくとも一部を含むプログラム起動方法、またはその方法を実行するプログラムとして捉えることもできる。上記手段および処理の各々は可能な限り互いに組み合わせて本発明を構成することができる。

【発明の効果】

【００２６】

本発明によれば、起動時にプログラムの正当性を検証してから動作するコンピューターシステムにおいて、ソフトウェアの更新処理に失敗した場合であっても、プログラムを復旧することが可能である。また、本発明によれば、このようなコンピューターシステムを比較的低コストで実現することが可能である。

【図面の簡単な説明】

【００２７】

【図１】第１および第２の実施形態におけるシステム概要を示す図である。

【図２】第１の実施形態におけるクライアント装置およびサーバ装置の機能構成を示す図である。

【図３Ａ】第１の実施形態におけるクライアント装置のハードウェア構成を示す図である。

【図３Ｂ】第１の実施形態におけるサーバ装置のアーキテクチャを示す図である。

【図４】第１の実施形態におけるプログラム検査処理およびプログラム更新処理の概要を示すフローチャートである。

【図５Ａ】第１の実施形態におけるシステム停止時のクライアント装置でのメインプログラム更新処理の流れを示すフローチャートである。

【図５Ｂ】第１の実施形態におけるシステム停止時のサーバ装置でのメインプログラム更新処理の流れを示すフローチャートである。

【図６Ａ】第１の実施形態におけるシステム起動時のクライアント装置でのプログラム検査処理の流れを示すフローチャートである。

【図６Ｂ】第１の実施形態におけるシステム起動時のサーバ装置でのプログラム検査処理の流れを示すフローチャートである。

【図７】第２の実施形態におけるクライアント装置およびサーバ装置の機能構成を示す図である。

【図８】第２の実施形態におけるクライアント装置のハードウェア構成を示す図である。
【図９Ａ】第２の実施形態におけるシステム停止時のクライアント装置でのメインプログラム更新処理の流れを示すフローチャートである。
【図９Ｂ】第２の実施形態におけるシステム停止時のサーバ装置でのメインプログラム更新処理の流れを示すフローチャートである。
【図１０Ａ】第２の実施形態におけるシステム起動時のクライアント装置でのプログラム検査処理の流れを示すフローチャートである。
【図１０Ｂ】第２の実施形態におけるシステム起動時のサーバ装置でのプログラム検査処理の流れ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】
【００２８】
以下に図面を参照して、この発明の好適な実施の形態を例示的に詳しく説明する。
【００２９】
＜第１の実施形態＞
〈構成〉
図１は本実施形態に係るコンピューターシステムの概略構成を示す図である。本実施形態に係るコンピューターシステムは、複数のクライアント装置１００と、サーバ装置２００とから構成される。各クライアント装置１００はサーバ装置２００と車載ネットワークを介して通信可能に構成されている。本システムを車載システムに適用した場合、クライアント装置１００はセンサやアクチュエータを制御する個々のＥＣＵ（Electronic Control Unit）に相当するものであり、クライアント装置１００は計算機資源の乏しい装置である。サーバ装置２００はシステム内に数台のみあればよいものであるため、豊富な計算機資源を備えセキュリティが確保された装置として構成することができる。サーバ装置２００は、既存の車載システムに新しい装置として追加されても良いが、カーナビゲーション装置（ナビ制御ＥＣＵ）などの汎用的な処理を行う装置の一機能として実装されても良い。また、一台のサーバ装置が管理するクライアント装置の数が少ない方が起動時の検証処理等が迅速に完了することを考慮すると、サーバ装置を車載ネットワークのゲートウェイＥＣＵの一機能として実装されることも好ましい。サーバ装置２００は、クライアント装置１００に配布するソフトウェアの入手するために、配信サーバ３００と広域ネットワークを介して通信可能である。なお、サーバ装置２００と配信サーバ３００とは常に通信可能である必要はなく、適当なタイミングで通信できればよい。また、ここでは車載システムを例に説明を行うが、本実施形態に係るコンピューターシステムは、その他の任意のコンピューターシステムに対して適用することができる。
【００３０】
図２は、クライアント装置１００およびサーバ装置２００の機能構成を示す図である。図３Ａ，３Ｂはそれぞれ、クライアント装置１００およびサーバ装置２００のハードウェア構成を示す図である。
【００３１】
クライアント装置１００は、外部通信部１０２、暗号関連処理部１０４、コード測定部１０６、ユニークＩＤ記憶部１０８、メインプログラム記憶部１１０、プログラム更新部１１２を備える。外部通信部１０２は、車載システム内の他のクライアント装置１００やサーバ装置２００と通信を行う機能を有する。暗号関連処理部１０４は、データの暗号化および復号処理や、署名の付加や検証処理などの機能を有する。なお、後で詳しく説明するように、本実施形態においては、送受信装置のユニークＩＤを利用して共通鍵を生成する。暗号関連処理部１０４は、この共通鍵を生成するための鍵生成機能（鍵生成関数）も備えている。コード測定部１０６は、各種プログラムのダイジェスト値を求める。コード測定部１０６が求めるダイジェスト値は、ＳＨＡ－１やＳＨＡ－２５６などのハッシュ関数によって求めたダイジェスト値（ハッシュ値）であっても良く、ＭＤ５などその他のアルゴリズムによって求めたダイジェスト値であっても良い。ユニークＩＤ記憶部１０８は、クライアント装置１００に固有のＩＤを記憶する。メインプログラム記憶部１１０は、

クライアント装置がセンサＥＣＵやアクチュエータＥＣＵとして機能するために必要なメインプログラムを記憶する。プログラム更新部１１２は、メインプログラムが更新されている場合には、サーバ装置２００から取得してメインプログラム記憶部１１０を更新する機能を有する。

【００３２】

クライアント装置１００は、図３Ａに示すように、大略、耐タンパ性デバイス１２０とＣＰＵ（Central Processing Unit）１３０と汎用記憶デバイス１４０から構成されている。耐タンパ性デバイスとは、内部情報の不正取得や改ざんに対して耐性のあるデバイスのことである。本実施形態では、耐タンパ性デバイス１２０によって暗号関連処理部１０４、コード測定部１０６、ユニークＩＤ記憶部１０８は記憶部１０８の機能を実現する。また、フラッシュメモリなどの汎用記憶デバイス１４０には、メインプログラム１４１、更新用プログラム１４２、外部通信用プログラム１４３が記憶されており、これらのプログラムをＣＰＵ１３０が実行することによって、ＥＣＵとしての機能や、プログラム更新部１１２、外部通信部１０２の機能が実現される。なお、耐タンパ性デバイス１２０も、その内部にＣＰＵや記憶装置などを有しており、記憶装置内に格納されたプログラムを実行することで前記の各機能部が実現されることは同様である。また、メインプログラムは更新の対象であるため書き換え可能なメモリに記憶する必要があるが、更新用プログラムや外部通信用プログラムを更新する必要がなければ、これらのプログラムは読み出し専用メモリ（ＲＯＭ）に記憶しても構わない。

【００３３】

次に、サーバ装置２００の機能構成を、図２を参照して説明する。サーバ装置２００は、大略、外部通信部２０２、暗号関連処理部２０４、更新プログラム管理部２０６、現在プログラム記憶部２０８、更新プログラム記憶部２１０、測定結果判定部２１２、正常状態記憶部２１４を備える。外部通信部２０２は、車載システム内のクライアント装置１００と通信を行う機能を有する。暗号関連処理部２０４は、データの暗号化および復号処理や、署名の付加や検証処理などの機能を有する。なお、サーバ装置２００の暗号関連処理部２０４もクライアント装置と同様に、送受信装置のユニークＩＤに基づく共通鍵生成機能を備える。更新プログラム管理部２０６は、クライアント装置１００からの更新要求に応じて、メインプログラムをクライアント装置１００に送信する機能を有する。現在プログラム記憶部２０８には、それぞれのクライアント装置がメインプログラム記憶部１１０に記憶しているメインプログラムが記憶される。更新プログラム記憶部２１０には、それぞれのクライアント装置について、最新版（クライアント装置に配布前）のメインプログラムを記憶している。更新プログラム管理部２０６は、広域ネットワークを介して配信サーバ３００から更新版のプログラムを安全な経路で入手する。配信サーバ３００から安全に更新プログラムを入手することは、通信を暗号化するなど既存の手法によって達成可能である。測定結果判定部２１２は、クライアント装置から送信される各種プログラムが正しいか否か判定する機能を有する。本実施形態においては、クライアント装置から各種プログラムのハッシュ値（ダイジェスト値）が送信される。正常状態記憶部２１４には各クライアント装置が現在有しているプログラムの正しいハッシュ値が格納されており、測定結果判定部２１２はクライアント装置から送信されるハッシュ値が正常状態記憶部２１４に格納されているハッシュ値と同じであれば、クライアント装置のプログラムが正常である（改ざんされていない）と判断する。なお、メインプログラムの正しいハッシュ値は、配信サーバ３００から最新版のメインプログラムとともに取得されて、正常状態記憶部２１４に格納される。

【００３４】

サーバ装置２００が有する外部通信部２０２、暗号関連処理部２０４、更新プログラム管理部２０６、現在プログラム記憶部２０８、更新プログラム記憶部２１０、測定結果判定部２１２、正常状態記憶部２１４は、図３Ｂに示すように、セキュアドメイン２３０において実行される。サーバ装置２００が、ゲートウェイ装置のＥＣＵ内に設けられる場合は、ゲートウェイ装置としての機能は一般ドメイン２４０において実行される。セキュア

ドメインは、信頼性が確保されたプログラムのみが実行可能な環境であり、一般ドメイン２４０からのアクセスが禁止される。また、セキュアドメインと一般ドメインとは独立しており、一般ドメインにおいて異常が発生した場合であってもセキュアドメインに悪影響が及ぶことはない。このようなセキュアドメインは、たとえば、ＡＲＭ社のＴｒｕｓｔＺｏｎｅテクノロジー（同社の商標）によって実現することができる。

【００３５】

〈全体処理概要〉

次に、図４を参照して、本車載コンピューターシステムにおけるシステム起動時および終了時の処理を大まかな流れを説明する。

【００３６】

車載システムに電源が供給されてシステムが起動すると（Ｓ１００）、各クライアント装置１００はメインプログラム１４１、更新用プログラム１４２、外部通信用プログラム１４３が正常であるか検査を行う（Ｓ１０２）。後述するようにこの検査は、クライアント装置においてプログラムのハッシュ値を計算してサーバ装置に送信し、サーバ装置においてハッシュ値が正常であるか否か判断することによって行われる。ここで、全てのプログラムが正常である場合は、クライアント装置においてメインプログラムを実行する（Ｓ１０６）。一方、メインプログラム１４１のみが異常であり、更新用プログラム１４２および外部通信用プログラム１４３が正常である場合は、更新用プログラム１４２を実行してメインプログラムの更新処理を実行する（Ｓ１０８）。これにより、前回の更新処理が途中で失敗してメインプログラムが不整合な状態であっても、更新処理を再度行ってメインプログラムを復旧することができる。また、メインプログラムが改ざんされた場合であっても、正常な状態のメインプログラムに戻すことができる。更新処理後には、メインプログラムを実行する（Ｓ１０６）。一方、プログラムの検査結果が上記以外の場合、すなわち、更新用プログラム１４２または外部通信用プログラム１４３のいずれかに異常がある場合には、メインプログラムを実行することなく処理を終了する（Ｓ１１２）。このようにして、システム起動時のプログラム検査処理が行われて、正当性が確認されたプログラムのみが実行されることになる。

【００３７】

以上のようにしてメインプログラムの実行が開始された後にイグニッションがＯＦＦされるとメインプログラムの実行を終了して、更新用プログラムを実行する（Ｓ１１０）．この更新用プログラムにより、メインプログラムの更新処理が実行される。このように本システムにおいては、システム停止時にメインプログラムの更新処理を実行するとともに、システム起動時に各種プログラムの検査処理を実行する。

【００３８】

なお、メインプログラム以外に更新用プログラムや外部通信用プログラムの検査を行う理由は以下の通りである。更新用プログラムは、メインプログラムを書き換える機能を有しているため正しく動作する必要があり、悪意者によって書き換え機能が削除されたり、全く別のプログラムがメインプログラム記憶部に格納されたりするのを防ぐ必要があるためである。外部通信部は、サーバ装置と正しく通信する必要があり、別のサーバと通信したりクライアント装置が送信しようとするデータとは異なるデータを送信したりするように書き換えられる危険があるためである。なお、外部通信用プログラムが正しいか否かが判断できないときに、この外部通信プログラムを利用してサーバ装置にハッシュ値を送信しているのが、外部通信用プログラムの正当性の検査が行われるため安全が確保される。仮に外部通信プログラムが改ざんされてサーバ装置と通信できない場合には、サーバ装置から必要な情報を受信することができず、クライアント装置が起動しない。また、外部通信プログラムが改ざんされて、求めたダイジェスト値と異なるダイジェスト値をサーバ装置へ送信した場合には、サーバ側で電子署名の検証または復号処理を行うことで、通信の改ざんを検知できる。この場合も、クライアント装置はサーバ装置から必要な情報を受信できず起動しない。このように、外部通信用プログラムが改ざんされた場合はクライアント装置が起動せず、改ざんされたプログラムを含むクライアント装置が他の装置に対して

悪影響を与えることはない。

【００３９】

［１．メインプログラム更新処理（システム終了時）］

次に、図５Ａ，５Ｂを参照して、システム停止時のメインプログラムの更新処理（図４のＳ１１０）の詳細を説明する。図５Ａはメインプログラム更新時にクライアント装置１００において実行される処理の流れを示し、図５Ｂはサーバ装置２００において実行される処理の流れを示す。

【００４０】

１－Ａ．クライアント側処理

クライアント装置１００においてイグニッションがＯＦＦされると（Ｓ２００）、実行中のメインプログラムは、プログラム更新部１１２（更新用プログラム１４２）を呼び出して終了する（Ｓ２０２）。プログラム更新部１１２は、サーバ装置２００に対して更新プログラムがあれば送信するように要求する（Ｓ２０４）。このとき、プログラム更新部１１２は、クライアント装置１００のユニークＩＤと、クライアント装置１００が一度に受信可能なデータのサイズをサーバ装置２００に通知する。

【００４１】

プログラムの更新要求がサーバ装置２００に送信されると、サーバ装置２００は、更新プログラムがある場合にはその一部をメインプログラム記憶部１１０（汎用記憶デバイス１４０）の書き込むべきアドレスとともに送信する。一方、更新プログラムがない場合には、サーバ装置２００はＮＵＬＬ（ペイロード長が０の通知）を送信する。したがって、プログラム更新部１１２は、サーバ装置２００から受信した通知のペイロード長が０であるか否かを判断し（Ｓ２０６）、０でない場合（Ｓ２０６）は受信データに指定されているアドレスを、受信データに含まれる更新プログラム（の一部）で書き換える（Ｓ２０８）。更新プログラム（受信した部分）の書き換えが完了したら、その旨をサーバ装置２００に通知して、次の受信を待つ。一方、サーバ装置から受信した通知のペイロード長が０である場合（Ｓ２０６－ＮＯ）は、更新プログラムが存在しないか、または、プログラムの更新が全て完了した場合であるので、システムを終了する（Ｓ２１２）。

【００４２】

１－Ｂ．サーバ側処理

一方、サーバ装置２００においてイグニッションがＯＦＦされると（Ｓ３００）、クライアント装置１００からメインプログラムの更新要求を受信する（Ｓ３０２）。このとき、どのクライアント装置からの要求であるかを示すユニークＩＤと、そのクライアント装置が一度に受信可能なデータサイズを取得する。そして、更新プログラム管理部２０６は、要求元のクライアント装置に対応する更新プログラムが存在するか否かを確認する（Ｓ３０４）。対応する更新プログラムが存在しない場合（Ｓ３０６－ＮＯ）は、更新プログラムが存在しないことを通知するために、更新プログラム管理部２０６がＮＵＬＬを通知する（Ｓ３１８）。一方、要求元のクライアント装置に対応する更新プログラムが存在する場合（Ｓ３０６－ＹＥＳ）は、更新プログラム管理部２０６は更新プログラムをクライアント装置の受信可能サイズに分割して、順次クライアント装置１００に送信する。すなわち、更新プログラム管理部２０６は、更新プログラムの一部を、書き込むべきアドレスとともにクライアント装置１００へ送信する（Ｓ３０８）。送信後は、クライアント装置からの更新プログラム書き換え終了の通知を受信するまで待機し（Ｓ３１０）、書き換え終了の通知を受信したら更新プログラムの未送信部分があるか確認する（Ｓ３１２）。更新プログラムに未送信部分がある場合（Ｓ３１４－ＹＥＳ）は、ステップＳ３０８に戻って更新プログラムの次の分割部分を送信する。一方、更新プログラムの未送信部分がない場合（Ｓ３１４－ＮＯ）は、更新プログラムを全て送信したことを通知するためにＮＵＬＬをクライアント装置に送信した後、更新プログラムの全体を現在プログラム記憶部２０８に移動する（Ｓ３１６）。以上により、１つのクライアント装置からのプログラム更新要求に対する処理が終了する。車載システム内の全てのクライアント装置からの更新要求に対する処理が完了したら、サーバ装置２００は実行を終了する。

【００４３】
［２．プログラム検査処理（システム起動時）］
次に、図６Ａ、６Ｂを参照して、システム起動時のプログラム検査処理（図４のＳ１０２）の詳細を説明する。図６Ａはプログラム検査時にクライアント装置１００において実行される処理の流れを示し、図６Ｂはサーバ装置２００において実行される処理の流れを示す。
【００４４】
２－Ａ．クライアント側処理
クライアント装置１００では、イグニッションがＯＮされると（Ｓ４００）、コード測定部１０６が、メインプログラム１４１、更新用プログラム１４２および外部通信用プログラム１４３のハッシュ値をそれぞれ求める（Ｓ４０２）。コード測定部１０６は、算出したハッシュ値をクライアント装置１００のユニークＩＤとともにサーバ装置２００へ送信し（Ｓ４０４）、プログラムの検査結果がサーバ装置２００から送信されるのを待つ。サーバ装置からの応答が、全てのプログラムが正常（以下、「ＳＷ正常」と表す）を示す場合（Ｓ４０６－ＹＥＳ）は、メインプログラム１４１を実行する（Ｓ４１０）。一方、サーバ装置からの応答が、メインプログラム１４１のみが異常であり更新用プログラム１４２および外部通信用プログラム１４３が正常である（以下、「ＳＷ異常」と表す）を示す場合（Ｓ４０６－ＮＯ）は、更新用プログラム１４２を実行してメインプログラムの更新処理を実行する（Ｓ４０８）。ステップＳ４０８の処理の詳細は、図３のフローチャートにおけるステップＳ２０４～Ｓ２１２の処理と同じである。なお、更新用プログラム１４２または外部通信用プログラム１４３が異常である場合は、本実施形態においてはサーバ装置２００から応答がなく、したがってクライアント装置１００においてはそれ以上の処理が実行されず、改ざんされたプログラムは実行されない。
【００４５】
２－Ｂ．サーバ側処理
一方、サーバ装置２００では、イグニッションがＯＮされると（Ｓ５００）、測定結果判定部２１２が、正常状態記憶部２１４を利用してクライアント装置１００から受信したプログラムのハッシュ値が正しいか否か検査する（Ｓ５０２）。なお、前述したように正常状態記憶部２１４には、クライアント装置１００ごとにメインプログラム１４１、更新用プログラム１４２および外部通信用プログラム１４３の正しいハッシュ値が格納されている。３つ全てのプログラムのダイジェストが正しい場合（Ｓ５０４－ＹＥＳ）は、測定結果判定部２１２はクライアント装置１００に対して「ＳＷ正常」を通知する（Ｓ５０６）。これによって、クライアント装置１００ではメインプログラムの実行が開始される。
【００４６】
いずれかのプログラムのハッシュ値が正しくない場合（Ｓ５０４－ＮＯ）は、メインプログラムのみが異常であるか否か判断する（Ｓ５０８）。メインプログラム１４１のみが異常である場合（Ｓ５０８－ＹＥＳ）は、測定結果判定部２１２はクライアント装置１００に対して「ＳＷ異常」を通知する（Ｓ５１０）。これにより、クライアント装置１００ではメインプログラムの更新処理が実行される。サーバ装置２００においても、更新処理を実行する（Ｓ５１２）。ここでのサーバ装置２００における更新処理は、実質的に図５Ｂのフローチャートと同様であるが、更新プログラムが無い場合には、現在プログラム記憶部２０８に格納されているメインプログラムをクライアント装置１００に送信する点が異なる。
【００４７】
また、プログラム検査の結果、更新用プログラム１４２または外部通信用プログラム１４３のいずれかが異常である場合（Ｓ５０４－ＮＯ）は、クライアント装置１００に通知を行わずに処理を終了する。これにより、クライアント装置１００ではそれ以上の処理が進行せず、改ざんされたプログラムが実行されることを防止できる。
【００４８】
〈暗号処理〉

システム起動時におけるクライアント装置１００とサーバ装置２００との間の通信は、秘匿・署名通信によって、盗聴や改ざんを防ぐことが好ましい。暗号化通信を行うにあたって、共通鍵方式および公開鍵方式のいずれを採用しても良いが、計算量を考慮して本実施形態では共通鍵方式による秘匿・署名通信を採用する。共通鍵方式を採用する場合も、システム内で１つの共通鍵を採用する方式と、装置ペアごとに異なる共通鍵を採用する方式が考えられるが、システム内で共通の鍵を採用した場合は鍵漏洩時になりすましによって誤動作を引き起こすことが可能であり危険である。そこで、本実施形態では、通信相手ごとに異なる共通鍵を用いるために、ＫＰＳ（Key Predistribution System）を採用する。

【００４９】

ＫＰＳでは、以下の鍵生成関数を用いて共通鍵を作成する。

【数１】

$$F(x,y)=F(y,x)=\sum_{i=0}^{T}\sum_{j=0}^{T}a_{ij}x^{i}y^{j} \pmod{q}$$

ここで行列$\{a_{ij}\}$は対称行列、すなわち、$a_{ij}=a_{ji}$であり、ｘ、ｙは各装置のＩＤ、Ｔはセキュリティパラメーター、ｑは素数である。

【００５０】

クライアント装置１００およびサーバ装置２００の暗号関連処理部には、自装置のＩＤをＡとして以下の鍵生成関数K_A（ｙ）が格納される。

【数２】

$$K_A(y)=F(A,y)=\sum_{j=0}^{T}\left\{\sum_{i=0}^{T}a_{ij}A^{i}\right\}y^{j} \pmod{q}$$

他の装置と通信を行う場合には、通信相手のＩＤ（Ｂとする）を取得して、K_A（Ｂ）を共通鍵として用いる。K_A（Ｂ）＝K_B（Ａ）であるので、互いのＩＤを交換することで通信相手も同一の共通鍵を生成できる。

【００５１】

なお、ＫＰＳは情報量的安全性に基づいた鍵管理方式であり、セキュリティパラメーターＴ個以下の鍵生成関数が漏洩した場合でも、他の鍵を推測できないことが証明されている。

【００５２】

本実施形態におけるシステム起動時のクライアント装置１００とサーバ装置２００との間の処理は、このような鍵生成アルゴリズムによって生成された共通鍵によって秘匿化される。また、メインプログラム起動後のユニキャスト通信（サーバとクライアントの間およびクライアント同士の間）の通信も、この鍵生成アルゴリズムによって生成された共通鍵によって秘匿化される。

【００５３】

システム起動時のプログラム検査によって、クライアント装置１００のプログラムが改ざんされていないことが確認された場合には、サーバ装置２００からクライアント装置１００に対して、構成証明トークンを送信する。この構成証明トークンは、システムが起動するたびにサーバ装置２００によって新しく生成される乱数値であり、システム稼働中は同一の値が使用される。プログラムの検証を通過した装置では、それ以降の他の装置との通信にこの構成証明トークンを利用することで、自身が正規のプログラムであることを提示する。たとえば、ユニキャスト通信においては、メッセージに構成証明トークンを含めて、ＫＰＳ鍵生成アルゴリズムによって生成される通信相手との共通鍵を用いて秘匿・署名通信を行う。ユニキャスト通信を受信した装置では、正しい構成証明トークンが含まれているメッセージのみを処理し、その他のメッセージを破棄することで構成証明が行われ

た装置とだけ通信を行う。また、ブロードキャスト通信の場合は、構成証明トークンを共通鍵として秘匿・署名通信を行う。ブロードキャスト通信を受信した装置では、構成証明トークンによって復号・署名検証が行えるメッセージだけを処理することで、構成証明が行われた装置とだけ通信を行う。このように起動時に各種プログラムの正当性が検証されないと、他の装置との通信が一切行えなくなる。

【００５４】

（本実施形態の作用・効果）

本実施形態においては、クライアント装置のメインプログラム更新処理において、メインプログラム記憶部を二重化することなくプログラムの書き換えを実施している。したがって、プログラム更新処理の途中で、電源断などによって処理が中断すると、メインプログラムの状態が不整合となる。したがって、システム起動時におけるプログラム検査によって、メインプログラムが異常である（改ざんされた）と判断されることになる。

【００５５】

しかしながら、本実施形態においては、システム起動時に、メインプログラムだけでなく、その他のプログラムである更新用プログラムと外部通信用プログラムの正当性も検査している。このようにすることで、メインプログラムのみが異常である場合には、正当性が保証された更新用プログラムと外部通信用プログラムによって、メインプログラムをサーバ装置から取得し直すことができる。なお、サーバ装置はクライアント装置が現在記憶しているべきメインプログラムも保持しているので、更新処理が中断することによってメインプログラムが不整合となった場合だけでなく、悪意者による改ざんによってメインプログラム（のみ）が改ざんされた場合も、メインプログラムを再取得して正常に実行することができる。

【００５６】

また、本実施形態においては耐タンパ性デバイスに格納する機能を少なくすることで、耐タンパ性デバイスに要するコストを抑えている。車載システムのように多数のＥＣＵ（クライアント装置）から構成されるシステムにおいて、それぞれの装置に耐タンパ性デバイスが必要となるためコストの上昇が発生するが、耐タンパ性デバイスで構築する機能を限定することでコストの上昇を防いでいる。更新用プログラムや外部通信用のプログラムは、通常の記憶装置に格納しているが、ハッシュ値を利用した正当性の検証を行っているため、セキュリティは確保される。

【００５７】

＜第２の実施形態＞

第１の実施形態では、システム起動時にクライアント装置の、メインプログラム、更新用プログラムおよび外部通信用プログラムの３つのプログラムのハッシュ値を算出してサーバ装置に送信している。ハッシュ値の算出は比較的長い処理時間を要する。そこで、本実施形態では、システム起動時にハッシュ値を算出するプログラムの数を減らすことによって高速なシステム起動を実現する。

【００５８】

図７は、本実施形態におけるクライアント装置１００およびサーバ装置２００の機能構成を示す図である。第１の実施形態と比較して、クライアント装置１００にブートフラグ記憶部１１４が加えられている点が異なる。このブートフラグは、メインプログラムの更新処理開始時に「更新中」に書き換えられ、更新処理が完了すると「更新済み」に書き換えられるフラグである。後述するように、このブートフラグを参照することで、更新処理が完了しているのか途中で失敗したのかを判断し、システム起動時の処理を切り替える。なお、サーバ装置２００の機能構成は第１の実施形態と同様である。

【００５９】

図８は、クライアント装置１００のハードウェア構成を示す図である。ブートフラグは汎用記憶デバイス１４０に格納される。ブートフラグは、耐タンパ性デバイス内部に格納しても良いが、更新対象の情報であるため汎用記憶デバイスのプログラムからアクセスできるようなインタフェースが用意され外部アクセスによる状態変化を許し状態保護が困難

なので、汎用記憶デバイスに記憶している。ブートフラグを汎用記憶デバイスに格納することにより、耐タンパ性デバイスの容量増大を抑えコスト上昇を抑制することもできる。

【００６０】

本実施形態においても、システム起動時にプログラムの検査を行い、システム終了時にメインプログラムの更新を行うという全体的な流れは第１の実施形態と同様である。

【００６１】

［１．メインプログラム更新処理（システム終了時）］

図９Ａ，９Ｂを参照して、システム停止時のメインプログラムの更新処理を説明する。図９Ａはメインプログラム更新時におけるクライアント装置１００において実行される処理の流れを示し、図９Ｂはサーバ装置２００において実行される処理の流れを示す。

【００６２】

１－Ａ．クライアント側処理

本実施形態におけるメインプログラム更新時のクライアント側処理は、第１の実施形態における処理（図５Ａ）と基本的に同様である。異なる点の一つは、イグニッションＯＦＦ時にメインプログラムがコード測定部１０６を呼び出して終了し（Ｓ６０２）、コード測定部１０６が更新用プログラム１４２のハッシュ値を算出してサーバ装置２００へ送信する（Ｓ６０４）点である。そして、サーバからプログラムが正常であるという応答がある場合（Ｓ６０６－ＹＥＳ）に、第１の実施形態と同様の更新処理を実行する。このように更新処理に先立って更新用プログラムの検証処理を実施するのは、後述するように本実施形態においてはシステム起動時に、更新用プログラムの正当性検証を省略しているためである。なお、更新プログラムが異常である場合には、サーバ装置からの応答がなく、クライアント装置ではそれ以上の処理を続行せずに処理を終了する。

【００６３】

第１の実施形態と異なる点のもう一つは、サーバ装置から更新プログラムを受信したとき（Ｓ２０６－ＹＥＳ）にブートフラグを「更新中」に変更し（Ｓ６０８）、更新プログラムを全て受信したとき（Ｓ２０６－ＮＯ）にブートフラグを「更新済み」に変更する（Ｓ６１０）処理が加えられている点である。このように、ブートフラグによって、更新中であるか否かが判別可能である。

【００６４】

１－Ｂ．サーバ側処理

本実施形態におけるメインプログラム更新時のサーバ側処理は、第１の実施形態における処理（図５Ｂ）と基本的に同様である。異なる点は、イグニッションＯＦＦ時にクライアント装置１００から更新用プログラムのハッシュ値を取得し、測定結果判定部２１２が正常状態記憶部２１４を参照して更新用プログラムが正しいか否か検査する処理（Ｓ７０２）が加えられている点である。更新用プログラムのハッシュ値が正常である場合（Ｓ７０４－ＹＥＳ）は、第１の実施形態と同様の処理（Ｓ３０２以降）を実行する。一方、更新用プログラムのハッシュ値が異常である場合（Ｓ７０４－ＮＯ）は、クライアント装置に異常が発生したことを記録し、このクライアント装置についてのプログラム更新処理はそれ以上実行せずに終了する。

【００６５】

［２．プログラム検査処理（システム起動時）］

次に、図１０Ａ，１０Ｂを参照して、システム起動時のプログラム検査処理を説明する。図１０Ａはプログラム検査時におけるクライアント装置１００において実行される処理の流れを示し、図１０Ｂはサーバ装置２００において実行される処理の流れを示す。

【００６６】

２－Ａ．クライアント側処理

クライアント装置１００では、イグニッションがＯＮされると（Ｓ８００）、コード測定部１０６がブートフラグを参照して、更新中（すなわち、更新処理が途中で失敗したか）否かを確認する（Ｓ８０２）。ブートフラグが「更新中」を示している場合（Ｓ８０４－ＹＥＳ）は、メインプログラムの更新処理が途中で失敗しメインプログラムが不整合な

状態であることが分かる。そこで、メインプログラムの更新処理を再度行うために、コード測定部１０６が更新用プログラム１４２と外部通信用プログラム１４３のハッシュ値を求め、ユニークＩＤとともにサーバ装置２００へ送信する（Ｓ８０６）。サーバ装置２００から、更新用プログラム１４２と外部通信用プログラム１４３の両方が正常である（「ＳＷ正常」）旨の通知を受信した場合（Ｓ８０８－ＹＥＳ）は、更新処理を行う（Ｓ８１０）。このステップＳ８１０における更新処理は、図９Ａのフローチャートのステップ２０４以降の処理に相当する。そして、更新処理が完了したら、メインプログラムを実行する（Ｓ８１８）。一方、更新用プログラム１４２または外部通信用プログラム１４３のいずれかが異常である（「ＳＷ異常」）旨の通知を受信した場合（Ｓ８０８－ＮＯ）は、更新処理を正しく行えない可能性があるため、それ以上何も行わずに電源をＯＦＦして処理を終了する。

【００６７】

また、ブートフラグが「更新済み」を示している場合（Ｓ８０４－ＮＯ）は、コード測定部１０６がメインプログラム１４１と外部通信用プログラム１４３のハッシュ値を求め、ユニークＩＤとともにサーバ装置２００へ送信する（Ｓ８１４）。ここで、前回のメインプログラム更新処理は正常に終了しているため、この段階で更新用プログラム１４２は実行しないため、検査を省略することができる。サーバ装置から、メインプログラム１４１と外部通信用プログラム１４３の両方が正常である（「ＳＷ正常」）旨の通知を受信した場合は、メインプログラムを実行する（Ｓ８１８）。一方、メインプログラム１４１または外部通信用プログラム１４３のいずれかが異常である（「ＳＷ異常」）旨の通知を受信した場合（Ｓ８１６－ＮＯ）は、それ以上何も行わずに電源をＯＦＦして処理を終了する。

【００６８】

２－Ｂ．サーバ側処理

サーバ装置２００では、イグニッションがＯＮされると（Ｓ９００）、クライアント装置１００からプログラムのハッシュ値を受信する。そして、測定結果判定部２１２が、正常状態記憶部２１４を利用して受信したプログラムのハッシュ値が正しいか否か検査する（Ｓ９０２）。クライアント装置１００から送信されるハッシュ値は、メインプログラムと外部通信用プログラムの２つ、または、更新用プログラムと外部通信用プログラムの２つのプログラムのハッシュ値である。受信したハッシュ値の両方が正常であるか判定し（Ｓ９０４）、いずれかに異常がある場合（Ｓ９０４－ＮＯ）には、クライアント装置１００に異常が発生したと記録して（Ｓ９０６）、このクライアント装置についての検査処理は終了する。

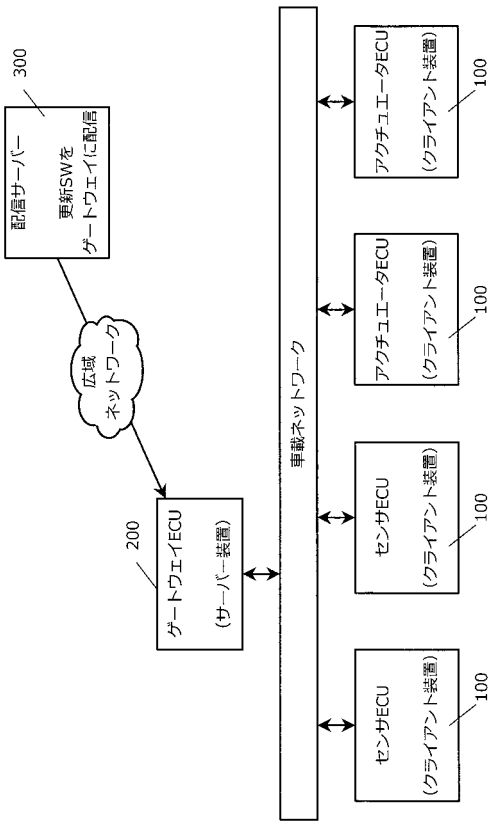
【００６９】

一方、クライアント装置から受信した２つのハッシュ値の両方が正しい場合は、測定結果判定部２１２が「ＳＷ正常」をクライアント装置へ通知する（Ｓ９０８）。ここで、クライアント装置１００から送信されたハッシュ値の１つがメインプログラムのものである場合（Ｓ９１０－ＹＥＳ）には、クライアント装置においてメインプログラムが実行されるので、サーバ装置側での処理は終了する。クライアント装置１００から送信されたハッシュ値にメインプログラムのものが含まれない場合（Ｓ９１０－ＮＯ）は、クライアント装置１００でメインプログラムの更新処理が実行されるので、このクライアント装置について更新プログラムが存在するか確認する（Ｓ９１２）。更新プログラムが存在する場合（Ｓ９１２－ＹＥＳ）は、更新処理を実行する（Ｓ９１４）。ステップＳ９１４の更新処理は、図９Ｂにおけるステップ３０２以降の処理に相当する。一方、このクライアント装置に対応する更新プログラムが存在しない場合（Ｓ９１２）は、クライアント装置のブートフラグは「更新中」であることを示しているにもかかわらず、更新プログラムが存在しないので、ブートフラグに異常があることが分かる。そこで、サーバ装置２００は、クライアント装置のブートフラグに異常があると記録して、検査処理を終了する。この場合、サーバ装置側での更新処理が実行されないので、クライアント装置の更新処理（Ｓ８１０）も実行されず、したがってクライアント装置のメインプログラムは実行されない。

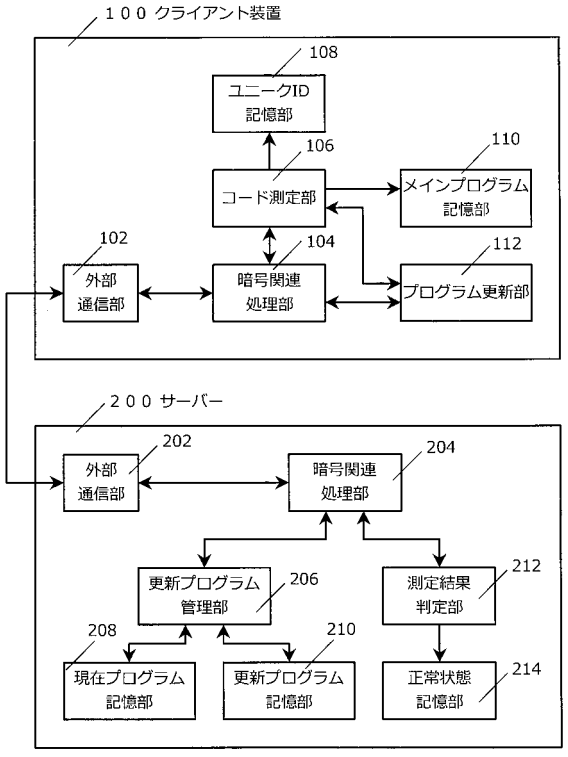
【００７０】
（実施形態の作用・効果）
本実施形態によっても、クライアント装置のメインプログラム更新処理が途中で失敗した場合であっても、更新処理を再開して正常なメインプログラムを実行できる。また、システム起動時に、メインプログラム等の検査を行ってからメインプログラムを実行しているので、メインプログラム等に改ざんがあればそれを検知して、改ざんされたプログラムが実行されないようにすることができる。
【００７１】
本実施形態においては、ブートフラグによって更新処理の途中であるか否かを管理しているため、システム起動時に算出するハッシュ値がメインプログラムと外部通信用プログラム、または、更新用プログラムと外部通信用プログラムの２つのみとすることができる。ハッシュ値の算出は計算量の多い処理であるので、求めるハッシュ値を３つから２つにすることで、プログラム検査に要する時間を短縮することが可能である。
【００７２】
ここで、ブートフラグは耐タンパ性デバイスではなく汎用記憶装置に格納されているため、改ざんされる危険がある。ただし、ブートフラグが改ざんされた場合であっても、改ざんされたプログラムが実行されることはない。以下、そのことを説明する。
【００７３】
（ａ）実際は「更新済み」であるが、ブートフラグは「更新中」を示している場合
この場合、クライアント装置は更新用プログラムと外部通信用プログラムのハッシュ値をサーバに送信し（Ｓ８１４）、サーバ側では更新処理を実行しようとするが、更新プログラムが存在しないため、ブートフラグに改ざんがあることが分かる（Ｓ９１２，Ｓ９１６）。また、仮にブートフラグの改ざんが、更新プログラムの配布のタイミングと一致した場合であっても、クライアント装置が新しいメインプログラムを取得することになるので問題は生じない。
【００７４】
（ｂ）実際は「更新中」であるが、ブートフラグは「更新済み」を示している場合
この場合、クライアント装置はメインプログラムと外部通信用プログラムのハッシュ値をサーバに送信する（Ｓ８０６）。ここで、更新処理の失敗によりクライアント装置のメインプログラムは不整合な状態となっているため、メインプログラムのハッシュ値が異常であることがサーバ装置において判別可能である。したがって、異常なプログラムが実行されることはない。
【００７５】
ただし、ブートフラグに改ざんがなく（すなわち、更新処理が正常に終了しており）、その後にメインプログラムに改ざんがあった場合も、同様の判断がなされる。したがって、ブートフラグが改ざんされたのか、ブートフラグは改ざんされずにメインプログラムが改ざんされたのかを区別することができない。
【００７６】
したがって、本実施形態においては、更新処理が中断した場合であって、ブートフラグに改ざんがない場合のみ更新処理の再開を行い、フラグまたはプログラムに改ざんがあった場合には復旧処理は行わない。本実施形態によってもプログラム等に改ざんがあればそれを検知して不正なプログラムが実行されるのを防ぐことができる。
【符号の説明】
【００７７】
１００　クライアント装置
１０２　外部通信部、　１０４　暗号関連処理部、　１０６　コード測定部、１０８　ユニークＩＤ記憶部、　１１０　メインプログラム記憶部、　１１２　プログラム更新部、　１１４　ブートフラグ記憶部
２００　サーバ装置
２０２　外部通信部、　２０４　暗号関連処理部、　２０６　更新プログラム管理

部、　２０８　現在プログラム記憶部、　２１０　更新プログラム記憶部、　２１２　測定結果判定部、　２１４　正常状態記憶部

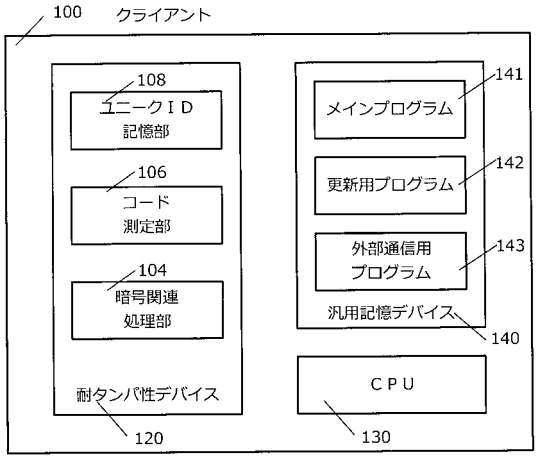
【図１】



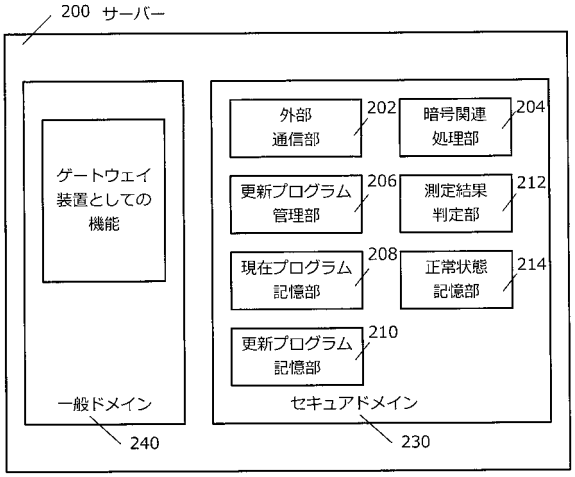
【図２】



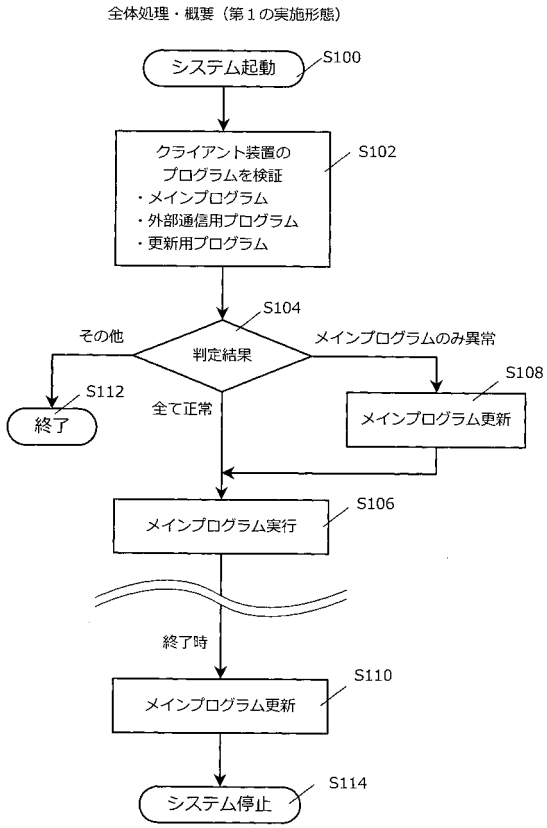
【図３Ａ】



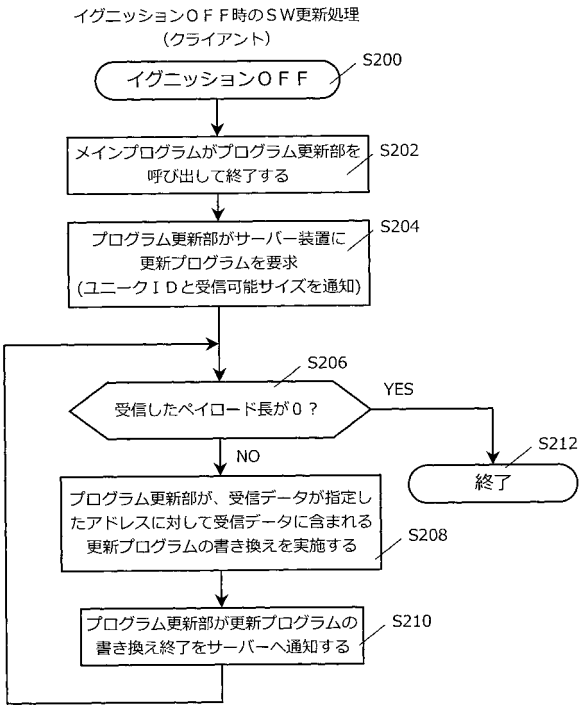
【図３Ｂ】



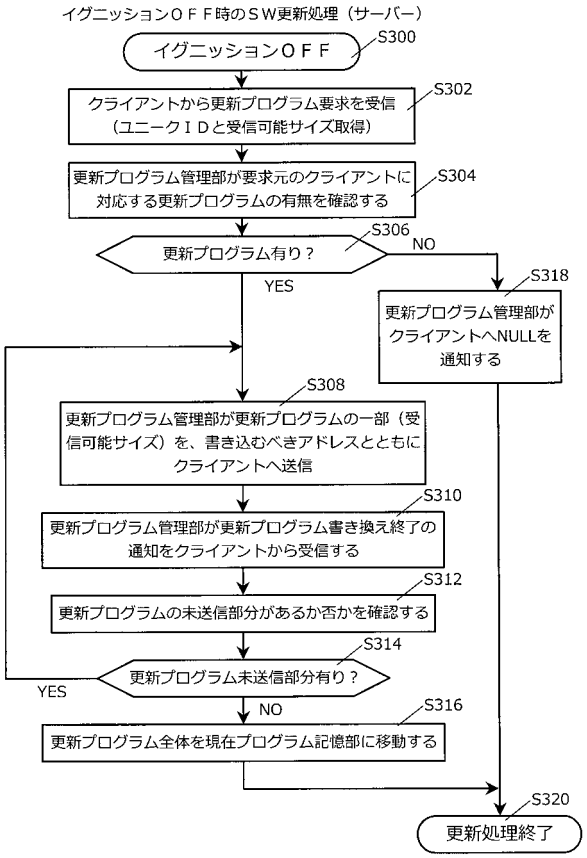
【図４】



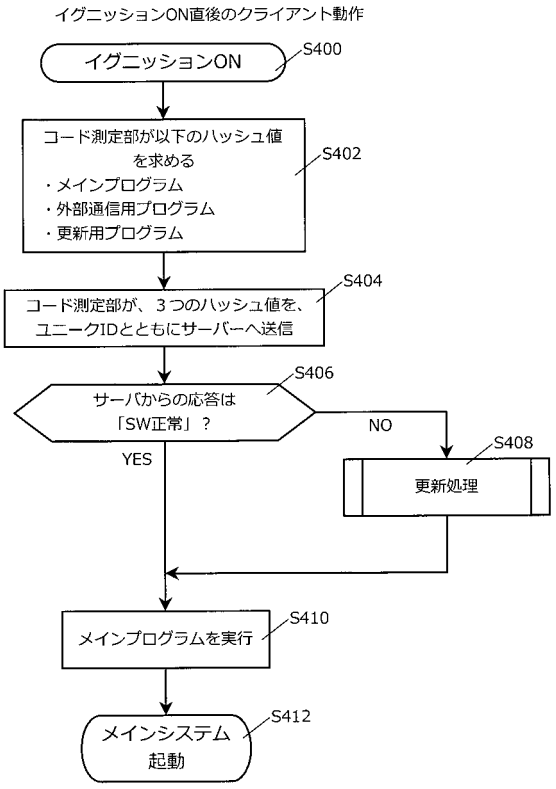
【図５Ａ】



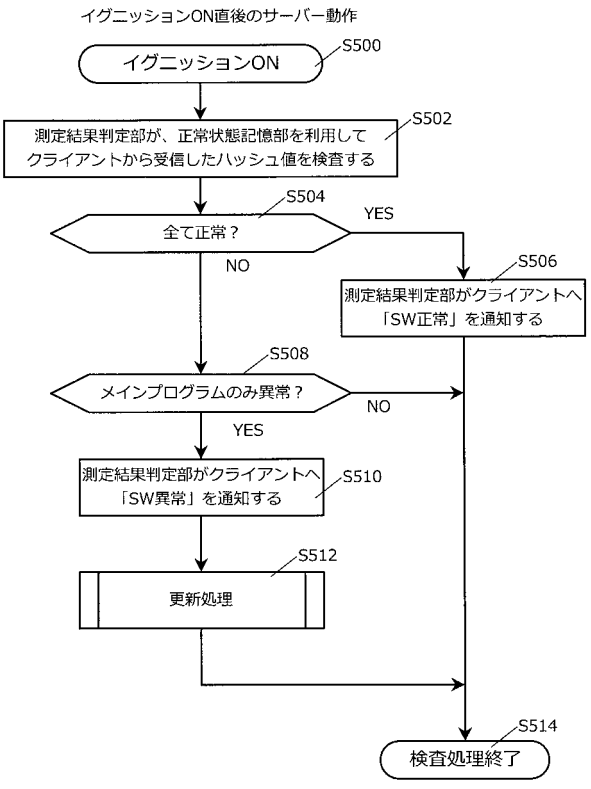
【図５Ｂ】



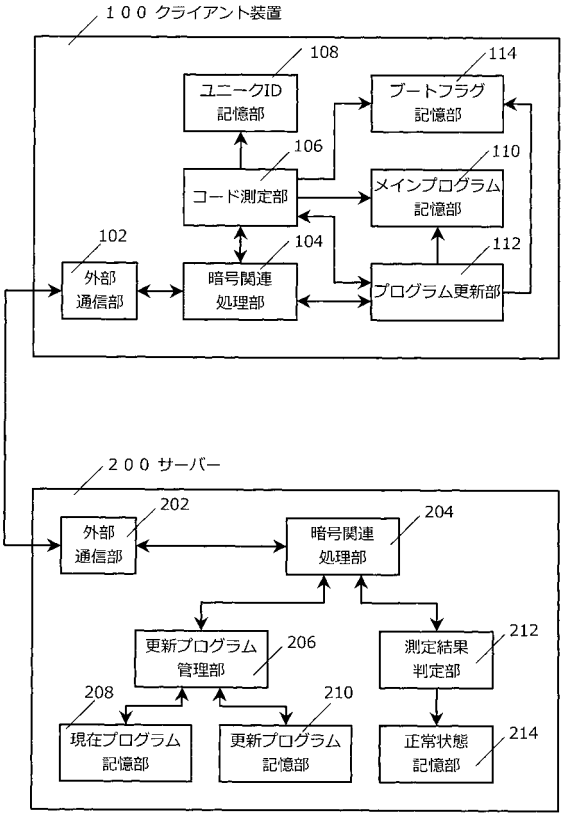
【図６Ａ】



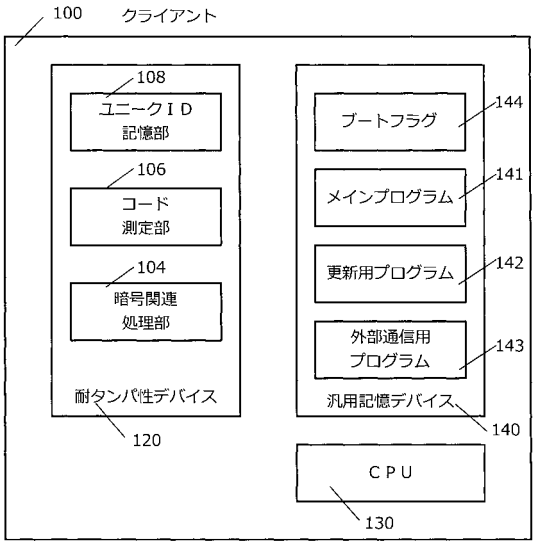
【図６Ｂ】



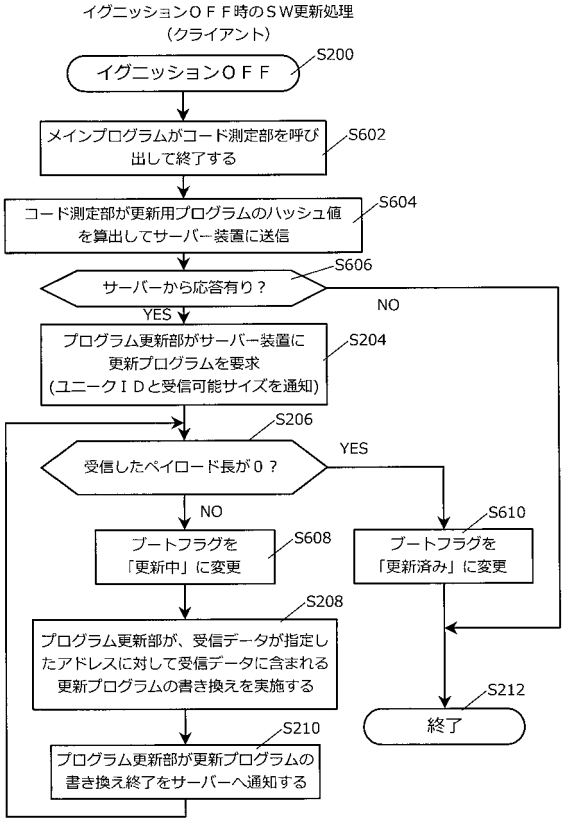
【図７】



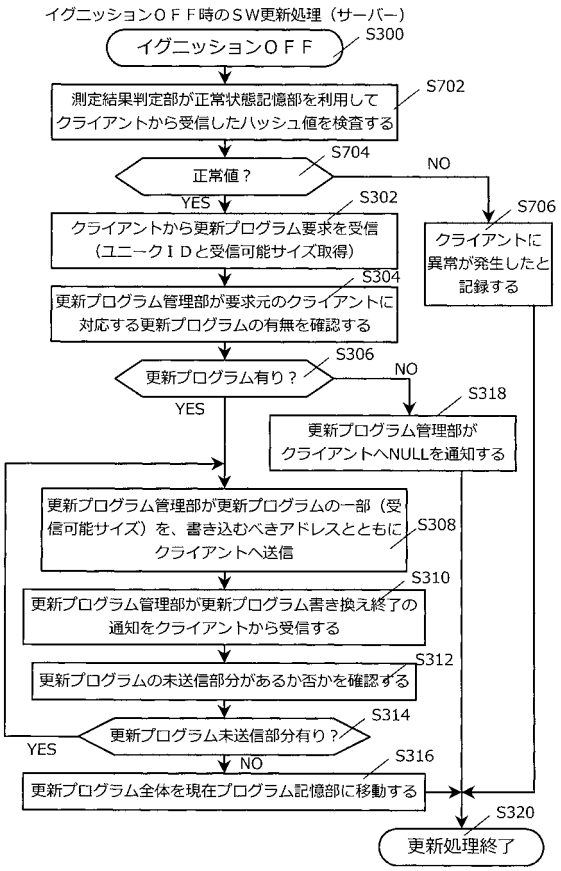
【図８】



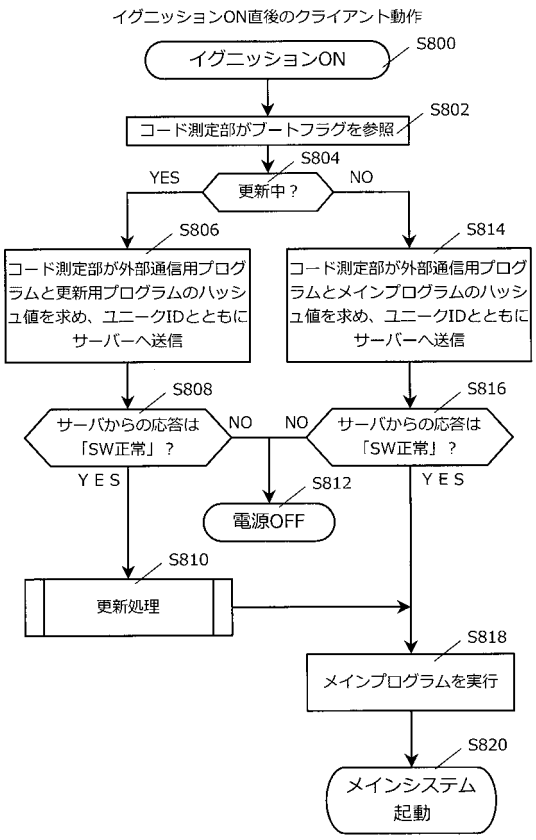
【図９Ａ】



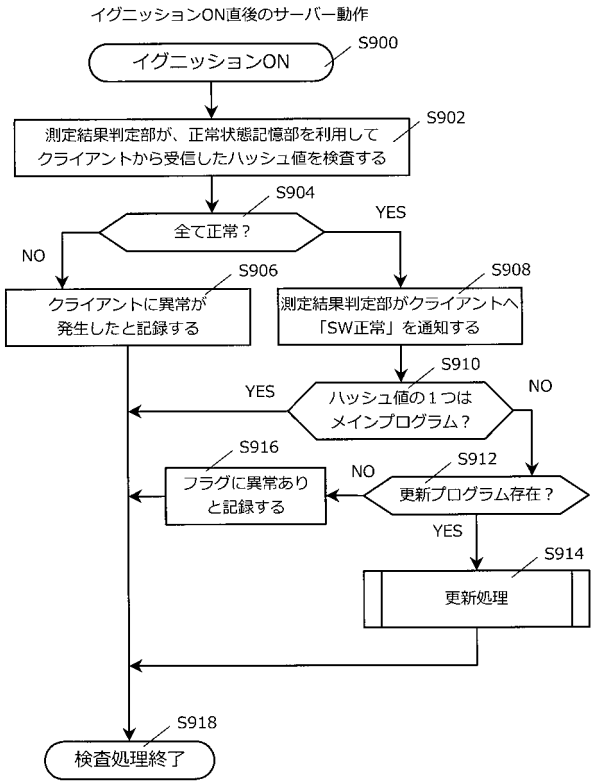
【図９Ｂ】



【図１０Ａ】



【図１０Ｂ】


イグニッションON直後のサーバー動作
イグニッションON
S900
測定結果判定部が、正常状態記憶部を利用して
クライアントから受信したハッシュ値を検査する
S902
全て正常？
S904
YES
NO
クライアントに異常が
発生したと記録する
S906
測定結果判定部がクライアントへ
「SW正常」を通知する
S908
ハッシュ値の１つは
メインプログラム？
S910
YES
NO
フラグに異常あり
と記録する
S916
NO
更新プログラム存在？
S912
YES
更新処理
S914
検査処理終了
S918

フロントページの続き

(74)代理人 100123319
弁理士 関根 武彦
(74)代理人 100125357
弁理士 中村 剛
(72)発明者 小熊 寿
東京都港区赤坂６丁目６番２０号 株式会社トヨタＩＴ開発センター内

Ｆターム(参考) 5B276 FD00
5B376 AB06 AC07 AE62 CA13 CA33 CA39 CA47 CA56 CA58 CA76
FA11 GA08