(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年4 月9 日 (09.04.2009)

PCT

(10) 国際公開番号
WO 2009/044533 A1

(51) 国際特許分類:
G06F 21/22 (2006.01) *G06F 9/445* (2006.01)

(21) 国際出願番号: PCT/JP2008/002728

(22) 国際出願日: 2008 年9 月30 日 (30.09.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2007-261977 2007 年10 月5 日 (05.10.2007) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 高山久 (TAKAYAMA, Hisashi). 松島秀樹 (MATSUSHIMA, Hideki). 伊藤孝幸 (ITO, Takayuki). 芳賀智之 (HAGA, Tomoyuki). ニコルソンケネス アレクサンダー (NICOLSON, Kenneth Alexander).

(74) 代理人: 中島司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

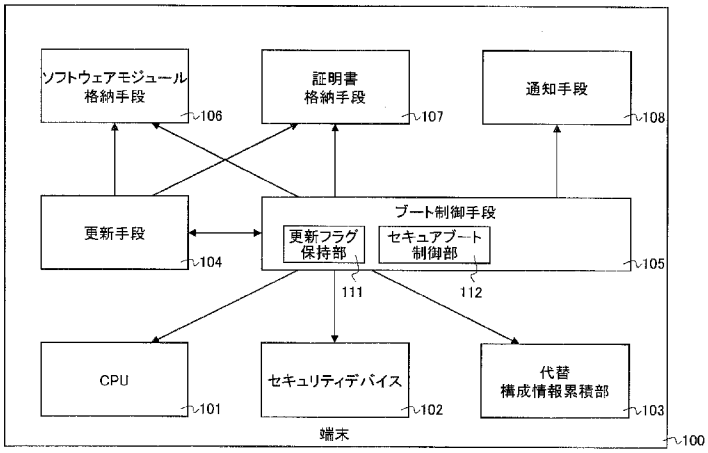
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM,

[続葉有]

(54) **Title:** SECURE BOOT TERMINAL, SECURE BOOT METHOD, SECURE BOOT PROGRAM, RECORDING MEDIUM, AND INTEGRATED CIRCUIT

(54) 発明の名称: セキュアブート端末、セキュアブート方法、セキュアブートプログラム、記録媒体及び集積回路

[図1]



100 TERMINAL
106 SOFTWARE MODULE STORAGE MEANS
104 UPDATING MEANS
107 CERTIFICATE STORAGE MEANS
105 BOOT CONTROL MEANS
111 UPDATE FLAG HOLDING SECTION
112 SECURE BOOT CONTROL SECTION
102 SECURITY DEVICE
108 NOTIFICATION MEANS
103 ALTERNATE CONFIGURATION INFORMATION ACCUMULATING SECTION

(57) Abstract: A terminal for performing a secure boot processing at the time of boot up can be reliably booted even if power-down or the like occurs in the middle of the update of a software module. The terminal comprises a CPU, a software module storage means, a certificate storage means, an updating means for updating the software module and a certificate, a security device provided with a configuration information storage means for storing the configuration information of the software module, an alternate configuration information storage means for storing the configuration information of a software module in the configuration before the update, and aboot control means for verifying and executing the software module by using the certificate. The terminal verifies the certificate of the software module with reference to the configuration information stored by the configuration information storage means and the configuration information stored by the alternate configuration information storage means.

[続葉有]

WO 2009/044533 A1

KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

(57) 要約: 起動時にセキュアブート処理を行う端末において、ソフトウェアモジュールの更新の途中で電源断等が起こった場合でも、確実に起動することを可能にする。ＣＰＵとソフトウェアモジュール格納手段と証明書格納手段と、ソフトウェアモジュール及び証明書を更新する更新手段とソフトウェアモジュールの構成情報を格納する構成情報格納手段を備えるセキュリティデバイスと更新前の構成でのソフトウェアモジュールの構成情報を格納する代替構成情報格納手段と証明書を用いてソフトウェアモジュールを検証して実行するブート制御手段とを備える端末であり、構成情報格納手段が格納する構成情報と代替構成情報格納手段が格納する構成情報とを参照してソフトウェアモジュールの証明書の検証を行う。

明　細　書

セキュアブート端末、セキュアブート方法、セキュアブートプログラム、記録媒体及び集積回路

技術分野

[0001] 本発明は、パーソナルコンピュータや携帯電話などの情報通信機器、インターネットアクセス機能を備えたテレビ受信装置などの情報家電機器等の端末と、その端末に内蔵されるセキュリティモジュールに関するものである。特に、端末のソフトウェアが複数のソフトウェアモジュールから構成され、それらのソフトウェアモジュールが更新可能な場合において、不正な動作をするモジュールにすり替えたり、不正にソフトウェアを古いバージョンに戻したりするといった不正行為を防止し、安定して確実に正しいソフトウェア構成で起動することを可能にするものである。

背景技術

[0002] 近年、ネットワークを介して提供されるサービスは、音楽や映像といった著作物の提供や、企業が保有する機密情報の閲覧、オンラインバンキングなど多岐に渡り、かつ、その中で扱われる情報の価値も高価なものになってきている。多岐に渡るサービスに対応するため、パーソナルコンピュータ、携帯端末、携帯電話、デジタル家電などの端末には、複数のソフトウェアモジュールがインストールされている。例えば、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）やＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）等の通信プロトコルで外部との通信を可能とする通信モジュール、さらにはアプリケーションなどがそれである。

[0003] これらは、正規のソフトウェアモジュールが定められた順番で起動される必要があり、端末にはソフトウェアモジュールの改ざん等の不正行為を防止する仕組みが組み込まれている。例えば、各ソフトウェアモジュールに対し

て提供者が証明書を発行し、各ソフトウェアモジュールの起動時に、その証明書を用いてソフトウェアモジュールの完全性を検証するといった仕組もその一つである。この仕組は、ソフトウェアモジュールをモジュール単位で更新する場合にも有効であり、ソフトウェアモジュールの提供者が新しいソフトウェアモジュールと共に、その新しいソフトウェアモジュールの証明書を提供することにより、新しいソフトウェアモジュールの完全性を検証することが可能となる。

[0004] 上記の証明書を用いて不正行為を防止する仕組みと同様の技術は、例えば特許文献１において公開されている。

[0005] また、セキュアなコンピュータプラットフォームを開発、普及させることを目的として、Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ（ＴＣＧ）が設立されている。ＴＣＧでは、Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ（ＴＰＭ）と呼ばれるセキュリティコアモジュールを利用し、安全な端末環境を実現している（非特許文献１～５参照）。

特許文献1：ＵＳ２００５／００２１９６８

非特許文献1：ＴＰＭ Ｍａｉｎ，Ｐａｒｔ１ Ｄｅｓｉｇｎ Ｐｒｉｎｃｉｐｌｅｓ，Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｖｅｒｓｉｏｎ １．２ Ｌｅｖｅｌ２ Ｒｉｖｉｓｉｏｎ１０３（９ Ｊｕｌｙ ２００７）

非特許文献2：ＴＰＭ Ｍａｉｎ，Ｐａｒｔ２ ＴＰＭ Ｓｔｒｕｃｔｕｒｅｓ，Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｖｅｒｉｏｎ１．２ Ｌｅｖｅｌ２ Ｒｉｖｉｓｉｏｎ１０３（９ Ｊｕｌｙ ２００７）

非特許文献3：ＴＰＭ Ｍａｉｎ Ｐａｒｔ３ Ｃｏｍｍａｎｄｓ，Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｖｅｒｉｏｎ １．２ Ｌｅｖｅｌ２ Ｒｉｖｉｓｉｏｎ１０３（９ Ｊｕｌｙ ２００７）

非特許文献4：ＴＣＧ Ｍｏｂｉｌｅ Ｔｒｕｓｔｅｄ Ｍｏｄｕｌｅ Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｖｅｒｓｉｏｎ １．０ Ｒｅｖｉｓｉｏｎ １（１２ Ｊｕｎｅ ２００７）

非特許文献5：ＴＣＧ Ｍｏｂｉｌｅ Ｒｅｆｅｒｅｎｃｅ Ａｒｃｈｉｔｅ

ｃｔｕｒｅ Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｖｅｒｓｉｏｎ１．０ Ｒｅｖｉｓｉｏｎ１（１２ Ｊｕｎｅ ２００７）

発明の開示

発明が解決しようとする課題

[0006] しかし、図１７に示すように、従来提案されている技術では、端末のソフトウェアが、複数のソフトウェアモジュールから構成される場合に課題がある。

図１７において、本来は、それぞれのモジュールにおいて検証と起動とを行ない、ＢＩＯＳの検証、ＢＩＯＳの起動、ＯＳの検証、ＯＳの起動、通信モジュールの検証、通信モジュールの起動といった図１７に示す番号の順番で検証と起動を行うことでブート処理が行なわれる。

[0007] しかし、ＯＳが何らかの問題がある古いＯＳと古い証明書にすり替えられてしまった場合、ＯＳの証明書は古いというだけで証明書に施されている署名等は正しいものであるため、問題がある古いモジュールであることが検出されず、その後の通信モジュールも起動されて、正常にブート処理を完了してしまう。

[0008] また、ソフトウェアモジュールの更新では、ソフトウェアモジュールのコードイメージと、それに対応する証明書の両方を更新する必要があるため、証明書の更新を完了し、コードイメージの更新を完了する前に電源断等が起こった場合に課題がある。更新された証明書と更新されなかったコードイメージとは整合性が取れていないため検証がエラーとなり、端末はブート処理を正しく完了できす、起動できない状態となってしまう。

[0009] 本発明は、こうした従来の問題点を解決するものであり、端末のソフトウェアが、複数のソフトウェアモジュールから構成される場合における古いモジュールにすりかえるといった不正行為を防止し、各モジュールの更新処理を個別に行うことが可能であり、さらに、更新処理の途中で電源断等が起こっても、安定して確実にブート処理が行なえる端末と、その端末に内蔵されるセキュリティモジュールを提供することを目的としている。

課題を解決するための手段

[0010] 上記課題を解決するために、本発明の一実施態様であるセキュアブート端末は、複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末であって、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納している第１格納手段と、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証手段と、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新手段と、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納手段と、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御手段とを備える。

発明の効果

[0011] 本発明の一実施態様であるセキュアブート端末は、上述の構成を備えることにより、デジタル証明書やソフトウェアモジュールの更新の際に電源断が

起こるなどによって、ソフトウェアモジュールのコードイメージやデジタル証明書間に不整合が生じてしまった場合でも、古いソフトウェアモジュールを実行して累積値を計算することなく前記代替累積値を用いて整合性を確保しブート処理を完了させることが出来る。

図面の簡単な説明

[0012] [図1]本発明の実施の形態１に係る端末の構成を示すブロック図

[図2]図２（ａ）は、本発明の実施の形態１に係る端末のセキュリティデバイスの構成を示すブロック図、図２（ｂ）は、本発明の実施の形態１に係る端末の代替構成情報累積部の構成を示すブロック図

[図3]本発明の実施の形態１におけるソフトウェアモジュールの証明書のデータ構造を示す図

[図4]本発明の実施の形態１または実施の形態２におけるセキュアブート処理のフロー図

[図5]本発明の実施の形態１または実施の形態２における通常セキュアブート処理のフロー図

[図6]本発明の実施の形態１または実施の形態２における更新時セキュアブート処理のフロー図

[図7]本発明の実施の形態２に係る端末の構成を示すブロック図

[図8]本発明の実施の形態３におけるソフトウェアモジュールの証明書のデータ構造を示す図

[図9]本発明の実施の形態４におけるソフトウェアモジュールの証明書のデータ構造を示す図

[図10]本発明の実施の形態４における更新時セキュアブート処理のフロー図

[図11]本発明の実施の形態５に係る端末の構成を示すブロック図

[図12]本発明の実施の形態１、２、３、４、５における更新処理のフロー図

[図13]本発明の実施の形態５におけるサイレントブート処理のフロー図

[図14]本発明の実施の形態６における更新処理のフロー図

[図15]図１５（ａ）は、端末の更新前のプログラムモジュールの証明書の構

成の一例を示す図、図１５（ｂ）は、端末のソフトウェアモジュールの更新を完了した場合のプログラムモジュールと証明書の構成の一例を示す図、図１５（ｃ）は、端末のソフトウェアモジュールの更新の途中の状態にけるプログラムモジュールと証明書の構成の一例を示す図

[図16]本発明の実施の形態１、２、３、４、５、６におけるブート制御手段の内部に保持されるデータの一例を示す模式図

[図17]従来技術に基づくブート処理の一例を説明する図

符号の説明

[0013] １００　端末

１０１　ＣＰＵ

１０２　セキュリティデバイス

１０３　代替構成情報累積部

１０４　更新手段

１０５　ブート制御手段

１０６　ソフトウェアモジュール格納手段

１０７　証明書格納手段

１０８　通知手段

発明を実施するための最良の形態

[0014] 本発明の一実施態様であるセキュアブート端末は、複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末であって、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納している第１格納手段と、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較し

て、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証手段と、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新手段と、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納手段と、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御手段とを備える。

[0015] 前記更新手段は、更に、全ソフトウェアモジュールが起動した後に、前記検証手段による検証に失敗したソフトウェアモジュールについて、当該ソフトウェアモジュールに対応するデジタル証明書を更新する。

[0016] この構成によれば、デジタル証明書やソフトウェアモジュールの更新の際に電源断が起こるなどによって、ソフトウェアモジュールのコードイメージや証明書間に不整合が生じてしまった場合でも、ブート処理を完了させその後に、デジタル証明書、ソフトウェアモジュールの更新処理を再開することが出来る。

[0017] また、前記セキュアブート端末は、更に、前記他のソフトウェアモジュールそれぞれについて更新があったか否かを判定する更新判定手段と、更新があったソフトウェアモジュールについては、当該ソフトウェアモジュールに係る更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新がなかったソフトウェアモジュールについては、当該ソフトウェアモジュールに係るデジタル証明書に含まれる目標要約値を累積演算して前記代替累積値を

算出し、前記第２格納手段に記録する代替累積手段とを備えることとしてもよい。

[0018] この構成によれば、各ソフトウェアモジュールが改ざん、不完全な更新等がない場合における実累積値と一致する代替累積値を演算でき、この代替累積値を用いブート処理を中断させず完了することができる。

[0019] また、前記代替累積手段は、更に、前記更新があったソフトウェアモジュールについては、前記ソフトウェアモジュールから算出される要約値が、前記ソフトウェアモジュールに係るデジタル証明書に含まれる目標要約値と一致するか否かを確認し、一致する場合に、前記更新前のデジタル証明書に含まれる目標要約値を累積演算することとしてもよい。

[0020] この構成によれば、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれに改ざんがなく、かつ、更新の完了を確認した上で当該ソフトウェアモジュールを起動することができ、より安全性を高めることができる。

[0021] また、前記代替累積手段は、前記代替累積値を暗号化して前記第２格納手段に格納することとしてもよい。

[0022] この構成によれば、代替累積値が暴露されるのを防ぐことができる。

[0023] また、前記セキュアブート端末は、更に、前記検証手段による有効性の検証が失敗したソフトウェアモジュールが前記ブート制御手段によって起動された場合、当該ソフトウェアモジュールに対応するデジタル証明書の更新が必要である旨を通知する通知手段を備えることとしてもよい。

[0024] この構成によれば、ユーザに対して証明書の更新が必要であることを明示的に通知し、更新処理の実行をユーザに促すことで、更新処理を完了させることが出来る確度を上げることができる。

[0025] また、前記デジタル証明書は、対応するソフトウェアモジュールについて、前記検証手段による検証が失敗した場合に制限すべき機能を示す制限情報を含み、前記ブート制御手段は、前記検証手段による検証が失敗したソフト

ウェアモジュールを起動する場合、前記制限情報により示される機能を制限した状態で前記ソフトウェアモジュールを起動することとしてもよい。

[0026] この構成によれば、更新処理が正常終了していない状態でブート処理が行われた場合、ブート処理の後に実行できる処理を制限するので、更新処理が未完了なソフトウェアモジュールによって不当な機能が実行させる危険性を回避することができる。

[0027] 例えば、制限情報に「検証手段による検証が失敗した場合に、更新処理の再開以外の処理を制限する」という内容を規定した場合、更新処理が正常終了していない状態でブート処理が行われると、ブート処理の後、更新処理の再開以外の処理が制限されるため、更新処理が優先的に実行され、より高い確度で更新処理を完了させるとともに、更新処理以外の処理が行われるのを防ぐことができる。

[0028] また、前記セキュアブート端末は、更に、前記複数のソフトウェアモジュールのそれぞれについて、前記ソフトウェアモジュールを示す情報と、前記ソフトウェアモジュールに係る現在のデジタル証明書を示す情報と、前記ソフトウェアモジュールに係る更新前のデジタル証明書を示す情報とを格納する領域を持つ複数の構造体、及び、前記複数の構造体のうち１つの構造体を使用中の現構造体として指し示す現構造体ポインタを記憶する構造体格納手段を備え、前記更新手段は、前記１つのソフトウェアモジュールの更新版及び前記１つのソフトウェアモジュールに係るデジタル証明書の更新版を取得する取得部と、前記１つのソフトウェアモジュールに対応する構造体のうち、現構造体ポインタによって示されていない構造体である更新用構造体について、（ａ）前記更新用構造体の前記ソフトウェアモジュールを示す情報として、前記１つのソフトウェアモジュールの更新版を示す情報を格納し、（ｂ）前記更新用構造体の前記現在のデジタル証明書を示す情報として、前記１つのソフトウェアモジュールに係るデジタル証明書の更新版を示す情報を格納し、（ｃ）前記更新用構造体中の前記更新前のデジタル証明書を示す情報として、前記現構造体ポインタの示す構造体の前記現在のデジタル証明書

を示す情報を格納する構造体更新部と、前記現構造体ポインタを、前記更新用構造体を示すように更新するポインタ変更部とを備えることとしてもよい。

[0029] この構成によれば、ソフトウェアモジュール、又はデジタル証明書の格納場所を構造体で一括管理し、更新を要するソフトウェアモジュール、又はデジタル証明書について更新が完了してから、現構造体ポインタをソフトウェアモジュールの更新版、又はデジタル証明書の更新版の格納場所を管理する構造体に切り替える。実行するソフトウェアモジュール、使用するデジタル証明書を一括変更するので、これらを個別に変更する場合に生じるような変更処理間のタイムラグが無くなり、安全確実に更新後のソフトウェアモジュール、又はデジタル証明書を使用することができる。

[0030] また、前記セキュアブート端末は、更に、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュールについてデジタル証明書の更新版を取得する取得手段と、前記１つのソフトウェアモジュールより起動の順番が前の他のソフトウェアモジュールそれぞれに対応する目標要約値を累積演算して事前累積値を生成する事前累積値生成手段と、前記事前累積値と、前記デジタル証明書の更新版に含まれる目標累積値とを比較して、前記１つのソフトウェアモジュールよりも起動の順番が前のソフトウェアモジュールの有効性を検証する事前検証手段とを備え、前記更新手段は、更に、前記事前検証手段による検証に成功した場合に、前記デジタル証明書の更新版で、前記１つのソフトウェアモジュールに係るデジタル証明書を更新することとしてもよい。

[0031] この構成によれば、更新処理を開始する前に、入手したソフトウェアモジュールのコードイメージと証明書と更新対象ではない証明書との整合性を検証するので、誤って整合性がない構成に更新されてしまうことを防止し、確実にソフトウェアモジュールのコードイメージと証明書との間に不整合がないソフトウェア構成へと更新することが出来る。

[0032] 本発明の一実施態様であるセキュアブート方法は、複数のソフトウェアモ

ジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブート方法であって、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新ステップと、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップとを含む。

[0033] 本発明の一実施態様であるセキュアブートプログラムは、複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブートプログラムであって、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される

他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新ステップと、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップとを含む。

[0034] 本発明の一実施態様である記録媒体は、複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブートプログラムを記録する記録媒体であって、前記セキュアブートプログラムは、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他の

ソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新ステップと、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップとを含む。

[0035] 本発明の一実施態様である集積回路は、複数のソフトウェアモジュールを予め定められた順番で起動する集積回路であって、前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納している第１格納手段と、起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証手段と、前記複数のソフトウェアモジュールのうち１つのソフトウェア

モジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新手段と、前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納手段と、（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御手段とを備える。

[0036] この構成によれば、デジタル証明書やソフトウェアモジュールの更新の際に電源断が起こるなどによって、ソフトウェアモジュールのコードイメージやデジタル証明書間に不整合が生じてしまった場合でも、古いソフトウェアモジュールを実行して累積値を計算することなく前記代替累積値を用いて整合性を確保しブート処理を完了させることが出来る。

以下本発明の実施の形態について、図面を参照しながら説明する。

[0037] （第１の実施形態）

本発明の第１の実施形態における端末１００の構成について説明する。

[0038] 端末１００は、図１に示すように、ＣＰＵ１０１と、耐タンパ性を備えるセキュリティデバイス１０２と、ＣＰＵ１０１が実行するソフトウェアモジュールのコードイメージを格納するソフトウェアモジュール格納部１０６と、ソフトウェアモジュールの証明書を格納する証明書格納手段１０７と、ソフトウェアモジュール格納部１０６に格納されるソフトウェアモジュールと証明書格納手段１０７に格納される証明書とを更新する更新手段と１０４と、ソフトウェアモジュールの更新前のソフトウェア構成における構成情報を示す代替構成情報累積部１０３と、端末１００のブート処理を制御するブート制御手段１０５と、端末１００のユーザにブート処理の状況を通知する通

知手段１０８と、から構成される。

[0039] ブート制御手段１０５は、証明書ごとの更新状況を示す更新フラグを保持する更新フラグ保持部１１１と、セキュアブート処理における実際の処理シーケンスを制御するセキュアブート制御部１１２とを備えている。

[0040] 代替構成情報累積部１０３と更新手段１０４とブート制御手段１０５は、具体的には、以下において詳しく説明する動作を行う専用ハードウェアまたはＣＰＵ１０１が実行するソフトウェアによって実現され、ソフトウェアによって実現される場合には、端末１００上のメモリ（不図示）にソフトウェア・オブジェクトデータとして生成される。この場合、特に更新フラグ保持部１１１は、不揮発性のメモリ上に実現される。

[0041] ソフトウェアモジュール格納部１０６と証明書格納手段１０７は、具体的には不揮発性メモリやハードディスクその他の記憶装置によって実現される。

[0042] 通知手段１０８は、具体的にはディスプレイやスピーカ、ＬＥＤ等のインジケータ等によって実現される。

[0043] さらに、セキュリティデバイス１０２は、図２（ａ）に示すように、ＣＰＵ１０１が実際に実行するソフトウェアモジュールの構成を示す構成情報を保持する構成情報累積部２０１と、ソフトウェアモジュールの証明書の有効性を検証する証明書検証部２０２と、構成情報累積部２０１が保持する構成情報を証明書の中の照合値と照合する照合部２０３と、ソフトウェアモジュールの有効なバージョンの下限を示すカウンタ値を保持するカウンタ部２０４と、データの暗復号及び署名生成や署名検証を行う暗復号部２０５と、を備える。また、構成情報累積部２０１は、ソフトウェアモジュールのハッシュ値の累積演算を行なう累積部２１１と、累積部２１１が算出した累積値（以下、累積演算の結果をこのように呼ぶ）を保持する構成情報保持部２１２と、を備えている。

[0044] 暗復号部２０５は、データの暗復号処理や署名生成や署名検証を行うための複数の鍵データを保持しており、代替構成情報累積部１０３は、暗復号部

２０５が保持する鍵データによって暗号化され、不正な改ざんがされないようになっている。

[0045] 累積部２１１は、構成情報保持部２１２が保持する値のバイト列とソフトウェアモジュールのハッシュ演算の結果のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算を行い、その結果を構成情報保持部２１２に格納する。

[0046] また、代替構成情報累積部１０３は、構成情報累積部２０１と同様の構成を備え、図２（ｂ）に示すように、更新前のソフトウェア構成におけるソフトウェアモジュールのハッシュ値の累積演算を行なう累積部２２１と、累積部２２１が算出した累積値を保持する代替構成情報保持部２２２と、を備えている。

[0047] 累積部２２１は、代替構成情報保持部２２２が保持する値のバイト列とソフトウェアモジュールのハッシュ演算の結果のバイト列とを連結し、さらに連結したバイト列（この場合、例えば、代替構成情報保持部２２２が保持する値が２０バイト、ソフトウェアモジュールのハッシュ演算の結果が２０バイトの場合、連結したバイト列は４０バイトのバイト列となる）に対してハッシュ演算を行い、その結果を代替構成情報保持部２２２に格納する。

[0048] 図３は、証明書のデータ構造を示しており、証明書は、その証明書が対応付けられたソフトウェアモジュールの識別情報３０１と、ソフトウェアモジュールのバージョン３０２と、ソフトウェアモジュールのダイジェストとしてモジュールのコードイメージをハッシュした場合の値を示す参照計測値３０３と、ソフトウェアモジュールが実行される前の端末１００の状態においてセキュリティデバイス１０２の構成情報累積部２０１に保持されるべき累積値を示す参照累積値３０４と、ソフトウェアモジュールのバージョンを示す参照カウンタ値３０５と、証明書を検証する鍵を示す検証鍵ＩＤ３０６と、検証鍵ＩＤ３０６が示す鍵に対応する秘密鍵による電子署名３０７と、から構成される。

[0049] 参照計測値３０３は、正当なソフトウェアモジュールのコードイメージの

ハッシュ値であり、実際のソフトウェアモジュールのコードイメージのハッシュ演算の結果と照合することで、証明書とソフトウェアモジュールとの対応関係を検証することが可能となる。また、参照累積値３０４は、セキュリティデバイス１０２の構成情報累積部２０１に格納される構成情報と照合することで、ソフトウェアモジュールを実行する前の状態として正しい状態（その前に実行されているソフトウェアモジュールが有効なソフトウェアモジュールであり、正しい順番で実行されている）であることを検証するために用いられる。

[0050] 次に、端末１００の動作について説明する。

[0051] まず、図１２を用いて、ソフトウェアモジュール格納手段１０６に格納されるソフトウェアモジュールのコードイメージと証明書格納手段１０７に格納される証明書とを更新する端末１００の更新処理における動作について説明する。

[0052] 最新のソフトウェアモジュールのコードイメージと証明書は、更新処理を行うソフトウェアモジュールのコードイメージと証明書の一覧を示す更新リストファイルと共に、ネットワーク通信手段（不図示）を介してダウンロードまたは蓄積媒体（不図示）を介して更新手段１０４の内部の記憶領域に一時的に保持されるものとする。また、具体的には、１つの更新されるソフトウェアモジュールに関して、そのソフトウェアモジュールのコードイメージと証明書、さらには、参照累積値３０４が更新されるソフトウェアモジュールに依存している証明書と更新リストファイルとが更新手段１０４の内部の記憶領域に保持される。

[0053] 更新リストファイルは、ソフトウェアモジュールの提供者によって、ソフトウェアモジュールのコードイメージおよび証明書と共に提供されるファイルである。

[0054] 更新リストファイルには、更新処理を行う順番でソフトウェアモジュールの証明書の識別情報とコードイメージの識別情報とが順番に記載されている。この順番は、セキュアブート処理の際に先に実行されるソフトウェアモジ

ュールの順番に従っており、先に実行されるソフトウェアモジュールほど、そのソフトウェアモジュールの証明書とコードイメージの更新処理が先に行われるように記載されている。

[0055] なお、更新されるソフトウェアモジュールが複数ある場合には、更新リストファイルと、それぞれのソフトウェアモジュールに関して、そのソフトウェアモジュールのコードイメージと証明書、さらには、参照累積値３０４が更新されるソフトウェアモジュールに依存している証明書と、が更新手段１０４の内部の記憶領域に保持される。

[0056] また、証明書の参照累積値３０４が更新されるソフトウェアモジュールに依存していない場合には、更新リストファイルと、それぞれのソフトウェアモジュールのコードイメージと証明書とが更新手段１０４の内部の記憶領域に保持される。

[0057] 最新のソフトウェアモジュールのコードイメージと証明書のダウンロードは、以下のようにして行われる。まず、更新手段１０４がソフトウェアモジュールの提供者のサイトに定期的にアクセスし、最新のソフトウェアモジュールのコードイメージや証明書が登録されているかどうかを確認する。登録されていた場合には、自動的にダウンロードが行われる。なお、端末のユーザが自らソフトウェアモジュールの提供者のサイトにアクセスしてダウンロードを行うようにしても良い。

[0058] 図１２は、更新されるべき最新のソフトウェアモジュールのコードイメージと証明書とが更新手段１０４の内部に保持された状態における端末１００が行なう更新処理のフローを示している。更新処理は、最新のソフトウェアモジュールのコードイメージと証明書とが更新手段１０４の内部に格納された時に、更新手段１０４が自動的に開始するようにしても良いし、ユーザの更新処理の開始操作に基づいて更新処理を開始するようにしても良い。

[0059] また、図１６は、ブート制御手段１０５の内部に保持されるデータの一例を示している。本実施の形態では、各ソフトウェアモジュールに関して、更新フラグと、コードイメージと証明書と旧証明書（更新処理をする前の古い

証明書）のそれぞれの実体へのポインタを管理するモジュール構造体Ａとモジュール構造体Ｂと、モジュール構造体へのポインタが保持される。図１６は、ＢＩＯＳとＯＳと通信モジュールの３つのソフトウェアモジュールに関して、ブート制御手段１０５の内部に保持されるデータを示している。

[0060] モジュール構造体へのポインタには、モジュール構造体Ａへのポインタまたはモジュール構造体Ｂへのポインタが設定される。

[0061] 本実施の形態では、モジュール構造体を使って、各ソフトウェアモジュール（ＢＩＯＳ、ＯＳ、通信モジュール）について、最新の証明書と旧証明書を管理している。本実施の形態ではモジュール構造体は２つあるが、一方は更新用に用いる構造体である。また、もう一方は現在のソフトウェア構成におけるソフトウェアモジュールの実体や証明書へのポインタを含む構造体であり、ソフトウェアモジュールの起動に用いる。本実施の形態では、ソフトウェアモジュールの更新があった場合は、更新用の構造体（すなわち、現在使用していない方の構造体）について、新しいソフトウェアモジュールのコードイメージや証明書の実体へのポインタを格納する。その上で、現在使用している方の構造体から、更新用の構造体へ各モジュール構造体へのポインタを切り替えることで、モジュール構造体の更新を完了する。すなわち、使用中のモジュール構造体と更新用のモジュール構造体と入れ替わるので、更新用のモジュール構造体の方が、新しく現在使用中のモジュール構造体となる。

[0062] また、各モジュール構造体の対応するソフトウェアモジュールよりも先に起動するモジュールについてのみ更新があった場合は、コードイメージの実体は変更されないが、証明書を更新する必要があることがある。これは、各ソフトウェアモジュールの証明書は自身が対応するソフトウェアモジュールよりも先に起動するモジュールの影響を受けることがあるためである。そのため、この場合も更新用のモジュール構造体について、更新前と同じコードイメージと、更新後の証明書と、更新前に最新だった証明書（更新後の旧証明書）とのそれぞれの実体を指すようポインタを設定する。その後、更新用

のモジュール構造体と現在使用中のモジュール構造体とを入れ替えることで、モジュール構造体の更新を完了する。これらの動作については、以下の動作説明で詳細を述べる。

[0063] 図１２において、まず、更新手段１０４が更新するソフトウェアモジュールに対応する更新フラグをセットする（ステップＳ１２０１）。

[0064] 次に、更新手段１０４は、ソフトウェアモジュールの証明書の更新を行う（ステップＳ１２０２）。この時、証明書格納手段１０７に格納される更新前の証明書は証明書格納手段１０７からは消去されず、ブート制御手段１０５において旧証明書として管理されるようになる。

[0065] また、古い証明書への差し替えを防止するため、更新手段１０４がセキュリティデバイス１０２に命令を送信する。命令を受けたセキュリティデバイス１０２は、証明書を更新する際に、証明書の参照カウンタ値３０５にセキュリティデバイス１０２のカウンタ部２０４に保持されているカウンタ値に１を加算した値を設定し、セキュリティデバイス１０２の暗復号部２０５に保持されている暗号鍵によって署名を生成して、電子署名３０７のフィールドに設定する。

[0066] また、この時、ブート制御手段１０５では、更新手段１０４からの要求に基づいて、モジュール構造体へのポインタが示しているモジュール構造体とは逆のモジュール構造体（ここで「逆のモジュール構造体」とはモジュール構造体へのポインタがモジュール構造体Ａを示している場合はモジュール構造体Ｂ、モジュール構造体へのポインタがモジュール構造体Ｂを示している場合はモジュール構造体Ａという意味）の証明書へのポインタに証明書格納手段１０７上の更新した証明書へのポインタを設定する。また、同じ逆のモジュール構造体の旧証明書へのポインタに、現在、モジュール構造体へのポインタが示しているモジュール構造体の証明書へのポインタと同じポインタを設定する。

[0067] 次に、更新手段１０４は、ソフトウェアモジュール格納手段１０６に格納されているソフトウェアモジュールのコードイメージを更新する（ステップ

Ｓ１２０３）。この時、ブート制御手段１０５では、更新手段１０４からの要求に基づいて、モジュール構造体へのポインタが示しているモジュール構造体とは逆のモジュール構造体のコードイメージへのポインタにソフトウェアモジュール格納手段１０６上の更新したコードイメージへのポインタを設定する。さらに、モジュール構造体へのポインタに逆のモジュール構造体へのポインタを設定して、更新した証明書とコードイメージとがセキュアブート処理において使用されるように切り替える。

[0068] 次に、更新手段１０４は、更新リストファイルに記載されている順番で、次に更新をすべきソフトウェアモジュールが存在するか否かを判定し（ステップＳ１２０４）、存在しない場合には、ステップＳ１２０５へ進み、他に更新をすべきソフトウェアモジュールが存在する場合には、ステップＳ１２０１に戻り、各ソフトウェアモジュールに関してステップＳ１２０１からステップＳ１２０４の処理を繰り返す。

[0069] ステップＳ１２０５では、更新手段１０４は、ソフトウェアモジュールのコードイメージを更新する必要はないが、証明書の内容が更新されたソフトウェアモジュールに依存しているために更新が必要な証明書が存在する場合に、それらの証明書を更新して、更新処理を終了する。この時、ブート制御手段１０５では、更新手段１０４からの要求に基づいて、モジュール構造体へのポインタが示しているモジュール構造体とは逆のモジュール構造体の証明書へのポインタに証明書格納手段１０７上の更新した証明書へのポインタを設定する。また、同じ逆のモジュール構造体のコードイメージへのポインタに、現在、モジュール構造体へのポインタが示しているモジュール構造体のコードイメージへのポインタと同じポインタを設定する。さらに、同じ逆のモジュール構造体の旧証明書へのポインタに、現在、モジュール構造体へのポインタが示しているモジュール構造体の証明書へのポインタと同じポインタを設定する。さらに、モジュール構造体へのポインタに逆のモジュール構造体へのポインタを設定して、更新した証明書がセキュアブート処理において使用されるように切り替える。

[0070] ステップＳ１２０５での証明書の更新の処理は、更新手段１０４は、ステップＳ１２０２での処理と同様の処理を行う。

[0071] 次に、図４、５、６を用いて、端末１００のセキュアブート処理における動作について説明する。

[0072] 図４は、端末１００が行なうセキュアブート処理のフローの概要を示している。

[0073] まず、ステップＳ４０１においてセキュアブート制御部１１２が更新フラグ保持部１１１の更新フラグを参照し、何れかの更新フラグが有効になっている場合には、更新時セキュアブート処理（ステップＳ４０３）へ進み、それ以外の場合は、通常セキュアブート処理（ステップＳ４０２）へ進む。

[0074] 通常セキュアブート処理（ステップＳ４０２）へ進んだ場合、セキュアブート制御部１１２は図５に示すフローに基づいてセキュアブート処理を行なう。

[0075] また、更新時セキュアブート処理（ステップＳ４０３）へ進んだ場合、セキュアブート制御部１１２は図６に示すフローに基づいてセキュアブート処理を行なう。

[0076] まず、通常セキュアブート処理（ステップＳ４０２）における端末１００の動作について説明する。

[0077] 通常セキュアブート処理では、まず、セキュアブート制御部１１２がソフトウェアモジュールと証明書との照合を行いソフトウェアモジュールに対応する証明書が存在することを検証する（ステップＳ５０１）。具体的には、ソフトウェアモジュールのコードイメージのハッシュ演算（例えば、ＳＨＡ－１などのハッシュ演算）を行い、その結果と証明書の参照計測値３０３とを照合する。照合の結果、参照計測値３０３と一致した場合には、セキュリティデバイス１０２に証明書の検証を要求してステップＳ５０２へ進む。

[0078] また、参照計測値３０３と一致しなかった場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフ

トウェアモジュールのコードイメージと証明書との整合性が取れていないことがユーザに通知される（不図示）。

[0079] ステップＳ５０２では、セキュリティデバイス１０２の証明書検証部２０２が、証明書のバージョンの検証を行い、証明書が古い無効化された証明書でないこと検証する（ステップＳ５０２）。具体的には、セキュリティデバイスのカウンタ部２０４が保持するカウンタ値と証明書の参照カウンタ値３０５とを比較する。カウンタ部２０４には、ソフトウェアモジュールの有効なバージョンの下限を示すカウンタ値が保持されており、カウンタ値の比較の結果、参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値以上であった場合には、ステップＳ５０３へ進む。

[0080] また、それ以外の場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフトウェアモジュールのコードイメージと証明書が古いものであることがユーザに通知される（不図示）。

[0081] ステップＳ５０３では、セキュリティデバイス１０２の証明書検証部２０２が、さらに、証明書の署名の検証を行い、有効な電子署名が施された証明書であることを検証する（ステップＳ５０３）。署名検証の結果、電子署名が有効であった場合には、ステップＳ５０４へ進む。

[0082] また、電子署名が無効であった場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、証明書の署名検証においてエラーが検出されたことがユーザに通知される（不図示）。

[0083] ステップＳ５０１、Ｓ５０２、Ｓ５０３の検証により、ソフトウェアモジュールと証明書とは対応関係にあり、かつ、その証明書の有効性が検証されることにより、ソフトウェアモジュール自体の有効性が検証される。

[0084] ステップＳ５０４では、セキュリティデバイス１０２の照合部２０３が、証明書の参照累積値と構成情報保持部２１２が保持する構成情報とを照合し

、ソフトウェアモジュールを実行する前の状態として正しい状態（その前に実行されているソフトウェアモジュールが有効なソフトウェアモジュールであり、正しい順番で実行されている）であることが検証される。証明書の参照累積値と構成情報保持部２１２が保持する構成情報とが一致した場合には、ステップＳ５０５へ進む。

[0085] また、それ以外の場合には、エラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフトウェアモジュールのコードイメージ及び証明書との間の整合性が取れていないことがユーザに通知される（不図示）。

[0086] ステップＳ５０５では、セキュリティデバイス１０２の構成情報累積部２０１の累積部２１１が、構成情報保持部２１２が保持する値のバイト列と証明書の参照累積値のフィールドに設定されている参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算（例えば、ＳＨＡ－１のハッシュ演算）を行い、その結果を構成情報保持部２１２に格納する（ステップＳ５０５）。

[0087] 次に、ステップＳ５０６において、セキュアブート制御部１１２がソフトウェアモジュールを実行し、ステップＳ５０７へ進む。

[0088] ステップＳ５０７では、セキュアブート処理を完了したか否かを判定する。

[0089] セキュアブート処理において実行されるべき全てのソフトウェアモジュールの実行を完了した場合には、通常セキュアブート処理（ステップＳ４０２）を完了し、

セキュアブート処理を完了していないと判定した場合には、ステップＳ５０１に戻り、次に実行するソフトウェアモジュールと証明書に関してステップＳ５０１からステップＳ５０７までの処理を繰り返す。

[0090] 次に、更新時セキュアブート処理（ステップＳ４０３）における端末１００の動作について説明する。セキュアブート制御部１１２は図６に示すフロ

ーに基づいてセキュアブート処理を行なう。

[0091] 更新時セキュアブート処理では、まず、セキュアブート制御部１１２がソフトウェアモジュールと証明書との照合を行いソフトウェアモジュールに対応する証明書が存在することを検証する（ステップＳ６０１）。具体的には、ソフトウェアモジュールのコードイメージのハッシュ演算（例えば、ＳＨＡ－１などのハッシュ演算）を行い、その結果と証明書の参照計測値３０３とを照合する。照合の結果、参照計測値３０３と一致した場合には、セキュリティデバイス１０２に証明書の検証を要求してステップＳ６０２へ進む。

[0092] また、参照計測値３０３と一致しなかった場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフトウェアモジュールのコードイメージと証明書との整合性が取れていないことがユーザに通知される（不図示）。

[0093] ステップＳ６０２では、セキュリティデバイス１０２の証明書検証部２０２が、証明書のバージョンの検証を行い、証明書が古い無効化された証明書でないこと検証する（ステップＳ６０２）。具体的には、セキュリティデバイスのカウンタ部２０４が保持するカウンタ値と証明書の参照カウンタ値３０５とを比較する。カウンタ部２０４には、ソフトウェアモジュールの有効なバージョンの下限を示すカウンタ値が保持されており、カウンタ値の比較の結果、参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値以上であった場合には、ステップＳ６０３へ進む。

[0094] また、それ以外の場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフトウェアモジュールのコードイメージと証明書が古いものであることがユーザに通知される（不図示）。

[0095] ステップＳ６０３では、セキュリティデバイス１０２の証明書検証部２０２が、さらに、証明書の署名の検証を行い、有効な電子署名が施された証明

書であることを検証する（ステップＳ６０３）。署名検証の結果、電子署名が有効であった場合には、ステップＳ６０４へ進む。

[0096] また、電子署名が無効であった場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、証明書の署名検証においてエラーが検出されたことがユーザに通知される（不図示）。

[0097] ステップＳ６０１、Ｓ６０２、Ｓ６０３の検証により、ソフトウェアモジュールとそれに対応する証明書との対応関係が正しいことが検証され、かつ、その証明書の有効性が検証されることにより、ソフトウェアモジュール自体の有効性が検証される。

[0098] ステップＳ６０４では、セキュリティデバイス１０２の照合部２０３が、証明書の参照累積値と構成情報保持部２１２が保持する構成情報とを照合し、ソフトウェアモジュールを実行する前の状態として正しい状態（その前に実行されているソフトウェアモジュールが有効なソフトウェアモジュールであり、正しい順番で実行されている）であることが検証される。

[0099] 次のステップＳ６０５では、ステップＳ６０４における証明書の参照累積値と構成情報保持部２１２が保持する構成情報との照合に成功したか否かを判定する。

[0100] 照合に成功した場合、つまり、証明書の参照累積値と構成情報保持部２１２が保持する構成情報とが一致し、ソフトウェアモジュールを実行する前の状態として正しい状態であることが検証された場合には、ステップＳ６０８へ進む。

[0101] また、照合に成功しなかった場合、つまり、証明書の参照累積値と構成情報保持部２１２が保持する構成情報とが一致しなかった場合には、ステップＳ６０７へ進み、証明書の参照累積値と代替構成情報保持部２２２が保持する構成情報との照合を行い、更新処理の途中の状態であることを要因とする証明書の不整合によるエラーであるか否かを検証する。

[0102] ステップＳ６０７では、セキュアブート制御部１１２が、証明書の参照累

積値と代替構成情報保持部２２２が保持する構成情報とを照合し、ソフトウェアモジュールの更新処理を行う前のソフトウェア構成において、ソフトウェアモジュールを実行する前の状態として正しい状態（但し、厳密には、ソフトウェアプログラムのコードイメージと証明書との整合性が取れていない状態）であることが検証される。証明書の参照累積値と代替構成情報保持部２２２が保持する構成情報とが一致した場合には、ステップＳ６０８へ進む。

[0103] また、それ以外の場合には、エラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ソフトウェアモジュールのコードイメージ及び証明書との間の整合性が取れていないことがユーザに通知される（不図示）。

[0104] ステップＳ６０８では、セキュリティデバイス１０２の構成情報累積部２０１の累積部２１１が、構成情報保持部２１２が保持する値のバイト列と証明書の参照累積値のフィールドに設定されている参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算（例えば、ＳＨＡ－１のハッシュ演算）を行い、その結果を構成情報保持部２１２に格納する（ステップＳ６０８）。

[0105] 次に、ステップＳ６０９において、更新フラグが有効になっているソフトウェアモジュールであるか否かを判定し、更新フラグが有効になっているソフトウェアモジュールである場合、つまり、更新処理中または更新処理を完了したソフトウェアモジュールである場合には、ステップＳ６１０へ進み、それ以外の更新されていないソフトウェアモジュールである場合には、ステップＳ６１３へ進む。

[0106] ステップＳ６１３では、代替構成情報累積部１０３の累積部２２１が、代替構成情報保持部２２２が保持する値のバイト列と証明書の参照累積値のフィールドに設定されている参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算を行い、その結果を代替構成情報保持部２

２２に格納する（ステップＳ６１３）。

[0107] ステップＳ６１０では、セキュアブート制御部１１２が、更新前の旧証明書のバージョンの検証を行い、旧証明書が更新処理を行う前のバージョンの証明書であること検証する（ステップＳ６１０）。具体的には、セキュリティデバイスのカウンタ部２０４が保持するカウンタ値と証明書の参照カウンタ値３０５とを照合する。カウンタ部２０４には、ソフトウェアモジュールの有効なバージョンの下限を示すカウンタ値が保持されており、カウンタ値の照合の結果、参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値以上であった場合には、ステップＳ６１１へ進む。

[0108] また、それ以外の場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、証明書のバージョン検証においてエラーが検出されたことがユーザに通知される（不図示）

ステップＳ６１１では、セキュアブート制御部１１２が、さらに、更新前の旧証明書の署名の検証を行い、有効な電子署名が施された証明書であることを検証する（ステップＳ６１１）。署名検証の結果、電子署名が有効であった場合には、ステップＳ６１２へ進む。

[0109] また、電子署名が無効であった場合にはエラーとなりセキュアブート処理を完了せずに終了する。この際、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、証明書の署名検証においてエラーが検出されたことがユーザに通知される（不図示）。

[0110] ステップＳ６１０、Ｓ６１１の検証により、旧証明書が更新処理を行う前のバージョンの有効な証明書であることが検証される。

[0111] 次に、ステップＳ６１２では、代替構成情報累積部１０３の累積部２２１が、代替構成情報保持部２２２が保持する値のバイト列と旧証明書の参照累積値のフィールドに設定されている参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算を行い、その結果を代替構成情報保持部２２２に格納する（ステップＳ６１２）。これにより、代替構成情報

保持部２２２には、更新処理を行う前のソフトウェア構成での構成情報が保持されることになる。

[0112] 次に、ステップＳ６１４において、セキュアブート制御部１１２がソフトウェアモジュールを実行し、ステップＳ６１５へ進む。このとき実行されるソフトウェアモジュールのコードイメージには、ステップＳ６０１からステップ６０３で検証した証明書に対応する最新のコードイメージが用いられる。

[0113] ステップＳ６１５では、セキュアブート制御部１１２がセキュアブート処理を完了したか否かを判定する。

[0114] セキュアブート処理において実行されるべき全てのソフトウェアモジュールの実行を完了した場合には、更新時セキュアブート処理（ステップＳ４０３）を完了し、ステップＳ４０４へ進む。

[0115] セキュアブート処理を完了していないと判定した場合には、ステップＳ６０１に戻り、次に実行するソフトウェアモジュールと証明書に関してステップＳ６０１からステップＳ６１５までの処理を繰り返す。

[0116] ステップＳ４０４では、セキュアブート制御部１１２が、証明書の参照累積値の照合に代替構成情報累積部を用いたか否か、つまり、ステップＳ６０７の処理をしたか否かを判定する。

[0117] ステップＳ６０７の処理をした場合には、更新処理においてソフトウェアモジュール及び証明書との間に不整合があり、更新処理が完了していないということであり、ステップＳ４０５へ進む。

[0118] ステップＳ４０５では、セキュアブート制御部１１２が通知手段１０８にユーザへの通知を要求し、通知手段１０８によって、ユーザに更新処理が完了していないことを通知され、セキュアブート処理を終了する。この後、自動的に更新処理を再開する。

[0119] ステップＳ６０７の処理をしなかった場合には、ソフトウェアモジュール及び証明書との間に不整合がなく更新されていることを意味し、ステップＳ４０６へ進み、セキュアブート制御部は更新フラグをリセットし、更新前の

旧証明書を消去する。

[0120] 次に、ステップＳ４０７では、セキュアブート制御部１１２が全ての証明書が更新されたか否かを判定する。具体的には、セキュアブート処理において実行される全てのソフトウェアモジュールに関して、証明書格納手段１０７に格納されている、それらの証明書の参照カウンタ値３０５が、セキュリティデバイス１０２のカウンタ部２０４に保持されているカウンタ値よりも大きな値を示すようになったか否かを判定する。

[0121] 全ての証明書が更新された場合には、古い証明書への差し替えを防止するために、セキュアブート制御部１１２は、セキュリティデバイス１０２にカウンタのインクリメントを要求し、セキュリティデバイス１０２がカウンタ部２０４に保持されているカウンタ値を１インクリメントして、セキュアブート処理を終了する（ステップＳ４０８）。それ以外の場合には、そのまま、セキュアブート処理を終了する。

[0122] 以上のようなセキュアブート処理を行うことにより、端末１００のソフトウェアが、複数のソフトウェアモジュールから構成される場合において、ソフトウェアモジュールを古いソフトウェアモジュールにすりかえるといった不正行為を防止し、各ソフトウェアモジュールの更新処理を個別に行うことが可能となる。また、証明書の更新の際に電源断が起こり、ソフトウェアモジュールのコードイメージや証明書間に不整合が生じてしまった場合でも、古いソフトウェアモジュールを実行することなく、セキュアブート処理を完了させ、証明書の更新処理を再開することが出来る。

[0123] 具体的な例として、端末１００の更新前のソフトウェアが図１５（ａ）に示すようにＢＩＯＳとＯＳと通信モジュールから構成され、ＯＳが更新されて、本来、図１５（ｂ）に示すような構成に更新される場合を考える。この場合、ＯＳのコードイメージとＯＳ証明書が更新されるだけでなく、その参照累積値がＯＳのコードイメージに依存している通信モジュール証明書も更新される（この場合、通信モジュールのコードイメージは更新されない）。

[0124] この更新処理において、例えば、ＯＳのコードイメージとＯＳ証明書の更

新処理が完了して、通信モジュール証明書の更新を完了する前に電源断等のトラブルが起こった場合、図１５（ｃ）に示すような構成になる。この状態での通信モジュール証明書の参照累積値は、図１５（ａ）の更新前のソフトウェア構成を想定した値となっており、更新されたＯＳのコードイメージ（Ｎｅｗ＿ＯＳ）及びＯＳ証明書´と通信モジュール証明書との間には不整合が生じる。

[0125] しかし、端末１００の場合には、図４、５、６に示したセキュアブート処理を行うことにより、セキュアブート処理を完了させ、通信モジュール証明書の更新処理を再開することが出来る。

[0126] なお、以上では、更新フラグ保持部１１１をブート制御手段１０５の内部に設けたが、セキュリティデバイス１０２の内部に設けるようにしても良い。セキュリティデバイス１０２は、耐タンパ性を備えているため、更新フラグの改ざんを防止することができ、端末１００の安全性が向上する。

[0127] また、なお、ソフトウェアモジュールの証明書をセキュリティデバイスの暗復号部が保持する鍵によって暗号化して証明書格納手段に格納するようにしても良い。

[0128] また、なお、ソフトウェアモジュールのコードイメージのハッシュ演算のアルゴリズムとしてＳＨＡ２５６を用いるようにしてもよい。

[0129] また、なお、セキュアブート処理を開始する前に、ブート制御手段が改ざんされていないことをセキュリティデバイス１０２が検証するようにしてもよい。

[0130] また、なお、最新のソフトウェアモジュールのコードイメージと証明書と更新リストファイルは、端末を専用ツールに接続し、専用ツールを介して更新手段の内部の記憶領域に保持されるようにしてもよい。

[0131] また、なお、証明書に施される電子署名のアルゴリズムとして、ＲＳＡ暗号または楕円曲線暗号またはＨＭＡＣを使用するようにしてもよい。

[0132] また、なお、以上では、証明書の参照カウンタ値に１を加算し、セキュリティデバイスのカウンタ部が示すカウンタ値を１インクリメントするとした

が、証明書の参照カウンタ値１以外の数値Ａを加算し、セキュリティデバイスのカウンタ部が示すカウンタ値を数値Ａだけインクリメントするようにしてもよい。

（実施の形態２）

図７を用いて本発明の実施の形態２について説明する。

[0133] 本発明の実施の形態２における端末７００は、代替構成情報累積部１０３を必要に応じて生成し、端末７００のリソースが効率的に使用されるように構成したものである。代替構成情報累積部１０３は、実際には、ＣＰＵ１０１が実行するソフトウェアによって実現され、端末７００上のメモリ（不図示）にソフトウェア・オブジェクトデータとして生成される。

[0134] 図７は、本発明の実施の形態２における端末７００のブロック構成を示している。第２の実施形態の場合には、ブート制御手段７０５にの中に、さらに、代替構成情報累積部１０３を必要に応じて生成する代替構成情報生成部７１３を備えている。代替構成情報累積部１０３は、通常時には存在せず、更新時セキュアブート処理（ステップＳ４０３）を行う際に、代替構成情報生成部７１３によって必要に応じて生成される。

[0135] それ以外の構成要素は、第１の実施形態における端末１００の場合と同じである。

[0136] 本実施の形態の場合、更新時セキュアブート処理（ステップＳ４０３）を開始する際に、代替構成情報生成部７１３が、セキュリティデバイス１０２の構成情報保持部２１２に保持されている値を読み出し、代替構成情報保持部２２２に設定することで、代替構成情報累積部１０３を生成する。それ以外の動作に関しては、第１の実施形態における端末１００の場合と同じである。

[0137] 本実施の形態の場合、代替構成情報累積部１０３を必要になった時にだけ、代替構成情報生成部７１３によって、ソフトウェア・オブジェクトデータとして生成し、それ以外の時は、端末７００のメモリを占有することが無く、通常セキュアブート処理の際にはより多くのメモリを利用して処理を高速

化することが出来るなど、端末７００のリソースを効率的に使用することが出来る。

[0138] なお、生成される代替構成情報累積部１０３の代替構成情報保持部２２２は、耐タンパ化されたメモリ上に生成するようにしてもよい。

（実施の形態３）

本発明の実施の形態３では、更新時セキュアブート処理を行って起動した場合の端末１００の動作モードを、更新時セキュアブート処理の際に行った照合処理に結果に応じて一部の機能を制限するなどの制御できるように構成したものについて説明する。

[0139] 図８は、本発明の実施の形態３におけるソフトウェアモジュールの証明書８００のデータ構造を示しており、機能制御の内容を規定する機能制御定義８０７というフィールドが追加されている以外は、実施の形態１の場合の証明書と同じである。

[0140] 機能制御定義８０７には、機能制御の条件と機能制御の内容が、例えば、ＸＭＬ等の形式で記述される。

[0141] 機能制御の条件としては、「更新時セキュアブート処理を行って起動した場合に常に適用」や「証明書の参照累積値の照合において代替構成情報累積部と照合を行った場合に適用」などの条件が規定される。

[0142] また、機能制御の内容としては、「更新処理の再開以外の処理が制限される緊急モード」や「外部との通信が制限される通信不可モード」、「セキュリティデバイス１０２を利用する暗号処理などのセキュリティサービスを利用不可とする制限モード」、「特定の外部通信（緊急電話など）のみ使用可能とする通報モード」などが規定される。

[0143] 端末１００の構成は、実施の形態１の場合と基本的には同じであり、更新時セキュアブート処理のステップＳ６１４において、ソフトウェアモジュールのコードイメージを実行する際に、ブート制御手段が各証明書８００の機能制御定義８０７が規定する内容に基づいて各ソフトウェアモジュールの内部パラメータを設定して機能制御を行う。それ以外の動作は、実施の形態１

の場合と同じである。

[0144] 本実施の形態の場合、例えば、機能制御の条件として「証明書の参照累積値の照合において代替構成情報累積部と照合を行った場合に適用」という条件を、機能制御の内容として「更新処理の再開以外の処理が制限される緊急モード」という制御内容を、それぞれ定義することにより、更新処理が完了していない状態でセキュアブート処理が行われた場合、ブート処理の後、更新処理の再開以外の処理が制限されるため、更新処理が優先的に実行され、より高い確度で更新処理を完了させることが出来る。また、機能制御として、「通信不可モード」や「制限モード」といったモードを定義することで、更新処理が完了していない状態でセキュアブート処理が行われた場合に、端末の機能を制限するような動作モードを設ける。これにより安全性の低下した状態の端末のソフトウェアの更新を促し、システム全体としてのリスクを低減させることが出来る。

（実施の形態４）

実施の形態１では、更新処理の際、旧証明書を消去せずに保持しておく必要があったが、

本発明の実施の形態４では、それを不要とするように構成したものについて説明する。

[0145] 図９は、本発明の実施の形態４におけるソフトウェアモジュールの証明書９００のデータ構造を示している。図９に示すデータ構造は、更新前のソフトウェアモジュールのコードイメージのハッシュ値を示す旧参照計測値９０７というフィールドが追加されている以外は、実施の形態１の場合の証明書と同じである。

[0146] 旧参照計測値９０７には、ソフトウェアモジュールを更新する前に、ソフトウェアモジュール格納手段１０６に格納されていたソフトウェアモジュールのコードイメージのハッシュ演算の結果が設定される。これは、証明書を更新する前に、証明書格納手段１０７に格納されていた証明書の参照計測値３０３に設定されている値と同じである。

[0147] 端末１００の構成は、実施の形態１の場合と基本的には同じであり、また、次に示す３つの相違点以外は、動作に関しても実施の形態１の場合と同じである。

[0148] 動作における１つ目の相違点は、実施の形態４の場合、更新処理のステップＳ１２０２において旧証明書を保持せずに消去する点である。

[0149] ２つ目の相違点は、実施の形態４の場合、図１０に示すように、更新時セキュアブート処理のステップＳ６０９において、更新フラグが有効になっているソフトウェアモジュールである場合（つまり、更新処理中または更新処理を完了したソフトウェアモジュールである場合）には、ステップＳ１０１２へ進み、代替構成情報累積部１０３の累積部２２１が、代替構成情報保持部２２２が保持する値のバイト列と証明書の旧参照累積値９０７のフィールドに設定されている旧参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算を行い、その結果を代替構成情報保持部２２２に格納する（ステップＳ１０１２）点である。

[0150] ３つ目の相違点は、実施の形態４の場合、セキュアブート処理のステップＳ４０６の処理において、更新フラグのリセットのみを行う点である。

[0151] 本実施の形態の場合、旧証明書を保持しておくために必要であったメモリが不要となり、携帯電話等のリソースに制限がある端末においても適用することが容易になる。

（実施の形態５）

図１１、１３を用いて本発明の実施の形態５について説明する。

[0152] 本発明の実施の形態５における端末１１００は、更新処理を開始する前に、入手した最新のソフトウェアモジュールのコードイメージと証明書、さらには、更新対象ではない証明書との整合性を検証することで、誤って整合性がない構成に更新されてしまうことを防止し、ソフトウェアモジュールのコードイメージ及び証明書との間に不整合がないソフトウェア構成に更新されるように構成したものである。

[0153] 図１１は、本発明の実施の形態５における端末１１００のブロック構成を

示している。第５の実施形態の場合には、更新手段１１０４の中に、さらに、最新のソフトウェアモジュールのコードイメージと証明書と更新対象ではない証明書との整合性を検証するサイレントブート部１１２１を備えている。それ以外の構成要素は、第１の実施形態における端末１００の場合と同じである。

[0154] 本実施の形態の場合、更新処理を開始する前に、サイレントブート部１１２１が図１３に示す処理フローに基づいてサイレントブート処理を行い、サイレントブート処理においてエラーが検出されなかった場合に、更新処理を開始する。それ以外の動作に関しては、第１の実施形態における端末１００の場合と同じである。

[0155] サイレントブート処理は、具体的には、最新のソフトウェアモジュールのコードイメージと証明書とをダウンロードした直後等のタイミングでおこなわれるとする。ただし、端末処理負荷が低いタイミングで行うなどとしてもよく、このタイミングに限定するものではない。

[0156] サイレントブート処理では、まず、サイレントブート部１１２１がソフトウェアモジュールと証明書との照合を行いソフトウェアモジュールに対応する証明書が存在することを検証する（ステップＳ１３０１）。具体的には、ソフトウェアモジュールのコードイメージのハッシュ演算（例えば、ＳＨＡ－１などのハッシュ演算）を行い、その結果と証明書の参照計測値３０３とを照合する。照合の結果、参照計測値３０３と一致した場合には、セキュリティデバイス１０２に証明書の検証を要求してステップＳ１３０２へ進み、一致しなかった場合にはエラーとなりサイレントブート処理を完了せずに終了する。

[0157] ステップＳ１３０２では、セキュリティデバイス１０２の証明書検証部２０２が、証明書のバージョンの検証を行い、証明書が古い無効化された証明書でないこと検証する（ステップＳ１３０２）。具体的には、セキュリティデバイスのカウンタ部２０４が保持するカウンタ値と証明書の参照カウンタ値３０５とを比較する。カウンタ部２０４には、ソフトウェアモジュールの

有効なバージョンの下限を示すカウンタ値が保持されており、カウンタ値の比較の結果、参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値以上であった場合には、ステップＳ１３０３へ進み、それ以外の場合にはエラーとなりサイレントブート処理を完了せずに終了する。

[0158] ステップＳ１３０３では、セキュリティデバイス１０２の証明書検証部２０２が、さらに、証明書の署名の検証を行い、有効な電子署名が施された証明書であることを検証する（ステップＳ１３０３）。署名検証の結果、電子署名が有効であった場合には、ステップＳ１３０４へ進み、無効であった場合にはエラーとなりサイレントブート処理を完了せずに終了する。

[0159] ステップＳ１３０１、Ｓ１３０２、Ｓ１３０３の検証により、ソフトウェアモジュールと証明書とは対応関係にあり、かつ、その証明書の有効であることが検証されることにより、ソフトウェアモジュール自体の有効であることが検証される。

[0160] ステップＳ１３０４では、サイレントブート部１１２１が、証明書の参照累積値と代替構成情報保持部２２２が保持する構成情報とを照合し、ソフトウェアモジュールを実行する前の状態として正しい状態（その前に実行されているソフトウェアモジュールが有効なソフトウェアモジュールであり、正しい順番で実行されている）であることが検証される。証明書の参照累積値と代替構成情報保持部２２２が保持する構成情報とが一致した場合には、ステップＳ１３０５へ進み、それ以外の場合には、エラーとなりサイレントブート部１１２１を完了せずに終了する。

[0161] ステップＳ１３０５では、サイレントブート部１１２１が、代替構成情報保持部２２２が保持する値のバイト列と証明書の参照累積値のフィールドに設定されている参照累積値のバイト列とを連結し、さらに連結したバイト列に対してハッシュ演算（例えば、ＳＨＡ－１のハッシュ演算）を行い、その結果を代替構成情報保持部２２２に格納する（ステップＳ１３０５）。

[0162] サイレントブート処理では、実際にソフトウェアモジュールのコードイメージを実行することはせず、次に、ステップＳ１３０６において、サイレン

トブート処理を完了したか否かを判定する。

[0163] サイレントブート処理において実行されるべき全てのソフトウェアモジュールの実行を完了した場合には、サイレントブート処理を完了し、セキュアブート処理を完了していないと判定した場合には、ステップＳ１３０１に戻り、次に実行されるべきソフトウェアモジュールと証明書に関してステップＳ１３０１からステップＳ５０７までの処理を繰り返す。

[0164] サイレントブート処理においてエラーが検出されなかった場合に、更新手段１１０４が更新処理を開始する。

[0165] 本実施の形態の場合、更新処理を開始する前に、入手したソフトウェアモジュールのコードイメージと証明書と更新対象ではない証明書との整合性を検証する。これにより、誤って整合性がない構成に更新されてしまうことを防止し、確実にソフトウェアモジュールのコードイメージ及び証明書との間に不整合がないソフトウェア構成に更新することが出来る。

（実施の形態６）

本発明の実施の形態６では、古いソフトウェアモジュールが実行されることを、より確実に防止し、端末１００のソフトウェア構成が常に最新のソフトウェア構成となるように構成したものについて説明する。

[0166] 図１４は、本発明の実施の形態６におけるセキュアブート処理のフローを示しており、この図１４のセキュアブート処理を行うことにより、古いソフトウェアモジュールが実行されることを防止することが出来る。

[0167] 端末１００の構成は、実施の形態１の場合と基本的には同じであり、ステップＳ４０６の後の処理以外は、動作に関しても実施の形態１の場合と同じである。

[0168] 本発明の実施の形態６におけるセキュアブート処理では、ステップＳ４０１からステップＳ４０６に関しては実施の形態１と同じ動作を行う。

[0169] ステップＳ４０６の後、つまり、更新時セキュアブート処理においてソフトウェアモジュール及び証明書との間に不整合がなく、ステップＳ４０６において、更新フラグをリセットし、更新前の旧証明書を消去した後、処理は

ステップＳ１４０７へ進む。ステップＳ１４０７では、証明書格納手段１０７に格納されている証明書の内、セキュリティデバイス１０２のカウンタ部２０４が示す値と参照カウンタ値が同じ証明書（つまり、更新されていない証明書）に関して、証明書格納手段に格納されている既存の証明書を用いて更新する。この時、セキュアブート制御部１１２は、更新手段１０４に証明書の更新処理を要求する。また、更新手段１０４がセキュアブート制御部１１２からの要求に基づきセキュリティデバイス１０２に命令を送信する。セキュリティデバイス１０２は、証明書の参照カウンタ値３０５にセキュリティデバイス１０２のカウンタ部２０４に保持されているカウンタ値に１を加算した値を設定し、セキュリティデバイス１０２の暗復号部２０５に保持されている暗号鍵によって署名を生成して、電子署名３０７のフィールドに設定する。なお、証明書の更新は、証明書格納手段に格納されている証明書を用いて行われるので、実質的には、この処理によって、証明書の参照カウンタ値３０５と電子署名３０７のフィールドのみが更新され、その他のフィールドの値は変わらない。

[0170] 次に、ステップＳ１４０８において、更新手段１０４がセキュリティデバイス１０２のカウンタ部に保持されているカウンタ値のインクリメントを要求し、セキュリティデバイス１０２がカウンタ部に保持されているカウンタ値を１インクリメントして更新処理を終了する。

[0171] ステップＳ１４０７、ステップＳ１４０８の処理により、すべての証明書の参照カウンタ値３０５とセキュリティデバイス１０２のカウンタ部に保持されているカウンタ値とが常に同じ値に設定されることになる。

[0172] 本実施の形態の図４、５、６の処理フローに基づくセキュアブート処理では、すべてのソフトウェアモジュールに関して、コードイメージを実行する前に、証明書のバージョンの検証が行われる。また、証明書のバージョンの検証では、証明書の参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値以上であることが検証され、証明書の参照カウンタ値３０５が、カウンタ部２０４が保持するカウンタ値よりも小さい場合には、そのソフト

ウェアモジュールのコードイメージは実行されない。

[0173] したがって、本実施の形態では、古いソフトウェアモジュールが実行されることが確実に防止され、端末１００のソフトウェア構成が常に最新のソフトウェア構成となる。

（実施の形態７）

本発明の実施の形態７では、上述してきた実施の形態１から実施の形態６をＴｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ（ＴＣＧ）で規定している仕様に基づいて実現してもよい。

[0174] この場合、セキュリティデバイス１０２は、ＴＣＧで規定しているＴＰＭモジュールまたはＭＴＭモジュールであり（以降のＴＰＭとは、ＴＰＭあるいはＭＴＭを意味するものとする）、構成情報保持部２０１は、ＴＰＭが備えるＰＣＲであり、カウンタ部は、ＴＰＭが備えるＭｏｎｏｔｏｎｉｃ　Ｃｏｕｎｔｅｒであり、累積部２１１は、証明書検証部２０２、照合部２０３は、ＴＰＭコマンド処理を含んだＴＣＧ機能を実現する部であり、証明書３００、８００、９００は、Ｅｘｔｅｒｎａｌ　ＲＩＭ＿Ｃｅｒｔ、もしくはＩｎｔｅｒｎａｌ　ＲＩＭ＿Ｃｅｒｔであり、代替構成情報保持部１０３は、ＴＰＭ内のＰＣＲの機能を仮想的に実現するためのもの（ここでは代替ＰＣＲと呼ぶ）であり、累積部２２１は、代替ＰＣＲを利用してＴＣＧのＥｘｔｅｎｄ処理をする部である。これによって、ＴＣＧ仕様に基づいて安全にソフトウェアの更新が可能となる。

（その他変形例）

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0175] （１）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭまたはハードディスクユニットには、コンピュータプログラムが記憶されている。前記マ

イクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。なお、各装置は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどの全てを含むコンピュータシステムには限らず、これらの一部から構成されているコンピュータシステムであってもよい。

[0176] （２）上記の各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

[0177] また、上記の各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部又は全てを含むように１チップ化されてもよい。

[0178] また、ここでは、システムＬＳＩとしたが、集積度の違いにより、ＩＣ、ＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

[0179] さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

[0180] （３）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

[0181] （４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0182] また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

[0183] また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

[0184] また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

[0185] また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータ

システムにより実施するとしてもよい。

[0186] （５）セキュリティデバイスは、耐タンパソフトウェアまたはソフトウェアと及びハードウェアにより実施されるよしてもよい。

[0187] （６）ＣＰＵは特別な動作モード（セキュアモードなど）を備え、ＣＰＵによって実行されるソフトウェアはその特別な動作モード（セキュアモードなど）で動作することで安全に実行されるとしてもよい。

[0188] （７）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0189] 本発明は、パーソナルコンピュータや携帯電話、オーディオプレーヤ、テレビ受像機、ビデオレコーダなど、プログラムデータの更新を行う情報通信機器や家電機器に広く利用することができる。

[0190] 本発明の端末に搭載されるセキュリティモジュールをそれらの機器に搭載し、本発明の端末と同様の構成にすることによって、機器のソフトウェアが複数のソフトウェアモジュールから構成される場合において、古いソフトウェアモジュールにすりかえるといった不正行為を防止し、各ソフトウェアモジュールの更新処理を個別に行うことが可能となる。

[0191] また、証明書の更新の際に電源断が起こり、ソフトウェアモジュールのコードイメージや証明書間に不整合が生じてしまった場合でも、ブート処理時に構成情報累積部と代替仮想構成情報累積部の両方を参照して検証をすることで、古いソフトウェアモジュールを実行することなく、セキュアブート処理を完了させ、証明書の更新処理を再開することが出来る。

請求の範囲

[1] 複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末であって、

前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納している第１格納手段と、

起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証手段と、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新手段と、

前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納手段と、

（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御手段と

を備えることを特徴とするセキュアブート端末。

[2] 前記更新手段は、更に、

全ソフトウェアモジュールが起動した後に、前記検証手段による検証に失敗したソフトウェアモジュールについて、当該ソフトウェアモジュールに対応するデジタル証明書を更新する

ことを特徴とする請求項１記載のセキュアブート端末。

[3] 前記セキュアブート端末は、更に、

前記他のソフトウェアモジュールそれぞれについて更新があったか否かを判定する更新判定手段と、

更新があったソフトウェアモジュールについては、当該ソフトウェアモジュールに係る更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新がなかったソフトウェアモジュールについては、当該ソフトウェアモジュールに係るデジタル証明書に含まれる目標要約値を累積演算して前記代替累積値を算出し、前記第２格納手段に記録する代替累積手段と

を備えることを特徴とする請求項２記載のセキュアブート端末。

[4] 前記代替累積手段は、更に、

前記更新があったソフトウェアモジュールについては、前記ソフトウェアモジュールから算出される要約値が、前記ソフトウェアモジュールに係るデジタル証明書に含まれる目標要約値と一致するか否かを確認し、一致する場合に、前記更新前のデジタル証明書に含まれる目標要約値を累積演算する

ことを特徴とする請求項３記載のセキュアブート端末。

[5] 前記代替累積手段は、前記代替累積値を暗号化して前記第２格納手段に格納する

ことを特徴とする請求項３記載のセキュアブート端末。

[6] 前記セキュアブート端末は、更に、

前記検証手段による有効性の検証が失敗したソフトウェアモジュールが前記ブート制御手段によって起動された場合、当該ソフトウェアモジュールに対応するデジタル証明書の更新が必要である旨を通知する通知手段

を備えることを特徴とする請求項１記載のセキュアブート端末。

[7] 前記デジタル証明書は、対応するソフトウェアモジュールについて、前記検証手段による検証が失敗した場合に制限すべき機能を示す制限情報を含み、

前記ブート制御手段は、前記検証手段による検証が失敗したソフトウェアモジュールを起動する場合、前記制限情報により示される機能を制限した状態で前記ソフトウェアモジュールを起動する

ことを特徴とする請求項１記載のセキュアブート端末。

[8] 前記セキュアブート端末は、更に、

前記複数のソフトウェアモジュールのそれぞれについて、

前記ソフトウェアモジュールを示す情報と、前記ソフトウェアモジュールに係る現在のデジタル証明書を示す情報と、前記ソフトウェアモジュールに係る更新前のデジタル証明書を示す情報とを格納する領域を持つ複数の構造体、及び、前記複数の構造体のうち１つの構造体を使用中の現構造体として指し示す現構造体ポインタを記憶する構造体格納手段を備え、

前記更新手段は、

前記１つのソフトウェアモジュールの更新版及び前記１つのソフトウェアモジュールに係るデジタル証明書の更新版を取得する取得部と、

前記１つのソフトウェアモジュールに対応する構造体のうち、現構造体ポインタによって示されていない構造体である更新用構造体について、

（ａ）前記更新用構造体の前記ソフトウェアモジュールを示す情報として、前記１つのソフトウェアモジュールの更新版を示す情報を格納し、（ｂ）前記更新用構造体の前記現在のデジタル証明書を示す情報として、前記１つのソフトウェアモジュールに係るデジタル証明書の更新版を示す情報を格納し、（ｃ）前記更新用構造体の前記更新前のデジタル証明書を示す情報として、前記現構造体ポインタの示す構造体の前記現在のデジタル証明書を示す情報を格納する構造体更新部と、

前記現構造体ポインタを、前記更新用構造体を示すよう更新するポインタ変更部と

を備えることを特徴とする請求項１記載のセキュアブート端末。

[9] 前記セキュアブート端末は、更に、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュールについてデジタル証明書の更新版を取得する取得手段と、

前記１つのソフトウェアモジュールより起動の順番が前の他のソフトウェアモジュールそれぞれに対応する目標要約値を累積演算して事前累積値を生成する事前累積値生成手段と、

前記事前累積値と、前記デジタル証明書の更新版に含まれる目標累積値とを比較して、前記１つのソフトウェアモジュールよりも起動の順番が前のソフトウェアモジュールの有効性を検証する事前検証手段とを備え、

前記更新手段は、更に、前記事前検証手段による検証に成功した場合に、前記デジタル証明書の更新版で、前記１つのソフトウェアモジュールに係るデジタル証明書を更新する

ことを特徴とする請求項１記載のセキュアブート端末。

[10] 複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブート方法であって、

前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、

起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール

、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新ステップと、

前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、

（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップと

を含むことを特徴とするセキュアブート方法。

[11] 複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブートプログラムであって、

前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、

起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する

更新ステップと、

前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、

（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップと

を含むことを特徴とするセキュアブートプログラム。

[12] 複数のソフトウェアモジュールを予め定められた順番で起動するセキュアブート端末に用いられるセキュアブートプログラムを記録する記録媒体であって、

前記セキュアブートプログラムは、

前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納する第１格納ステップと、

起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証ステップと、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール

、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新ステップと、

前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納ステップと、

（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御ステップと

を含む

ことを特徴とする記録媒体。

[13] 複数のソフトウェアモジュールを予め定められた順番で起動する集積回路であって、

前記複数のソフトウェアモジュールそれぞれについて、当該ソフトウェアモジュールから要約値として算出されるべき目標要約値と、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの目標要約値を累積演算した場合に得られるべき目標累積値とを含むデジタル証明書を格納している第１格納手段と、

起動の順番に達したソフトウェアモジュールについて、当該ソフトウェアモジュールより先に起動される他のソフトウェアモジュールそれぞれの要約値を累積演算した実累積値と、当該ソフトウェアモジュールに対応するデジタル証明書に含まれる目標累積値とを比較して、当該ソフトウェアモジュールより先に起動されるソフトウェアモジュールの有効性を検証する検証手段と、

前記複数のソフトウェアモジュールのうち１つのソフトウェアモジュール

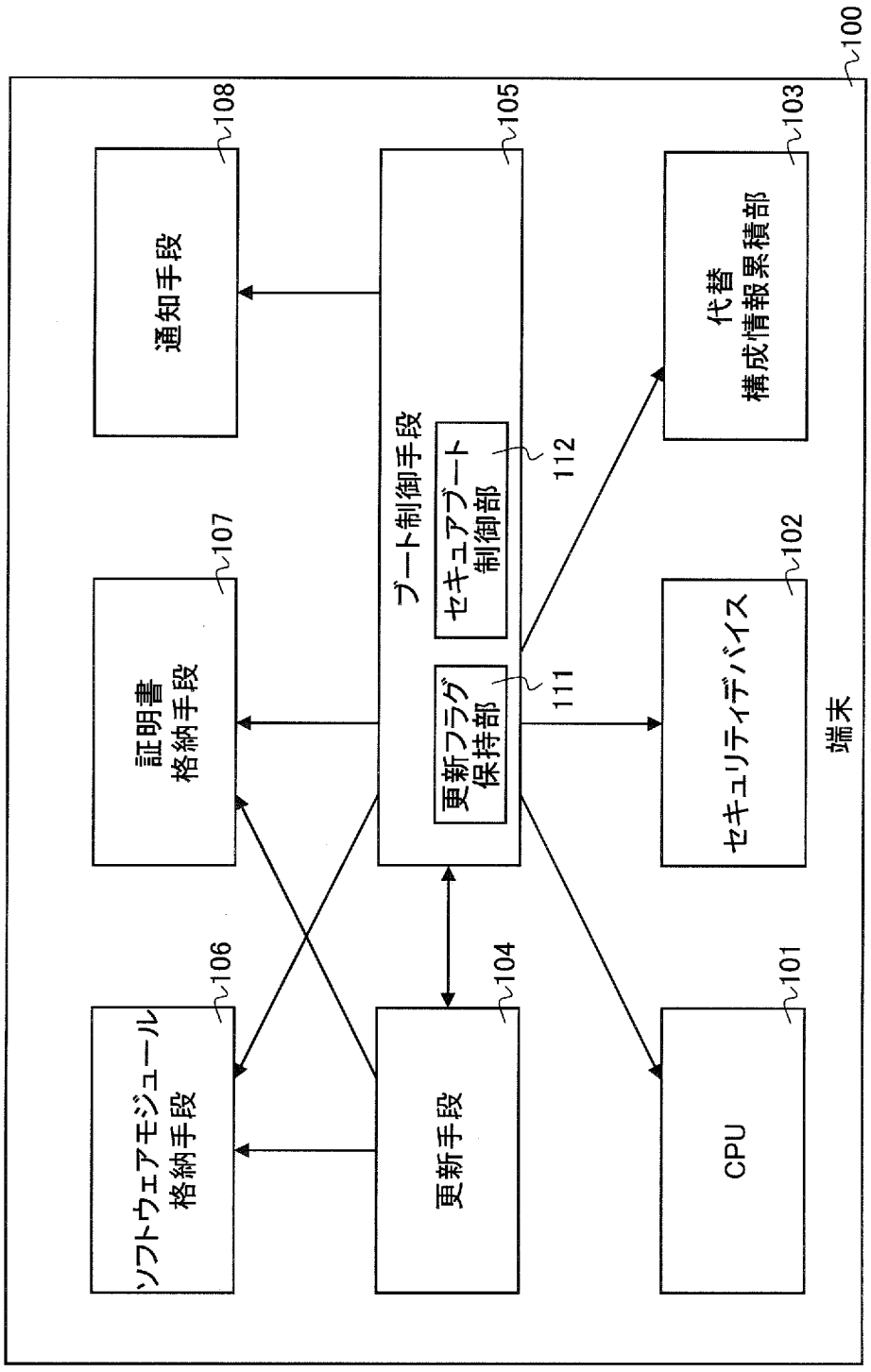
、及び前記１つのソフトウェアモジュールに係るデジタル証明書を更新する更新手段と、

前記他のソフトウェアモジュールそれぞれについて、デジタル証明書が更新されている場合は更新前のデジタル証明書に含まれる目標要約値を累積演算し、更新されていない場合は当該デジタル証明書に含まれる目標要約値を累積演算した代替累積値を格納する第２格納手段と、

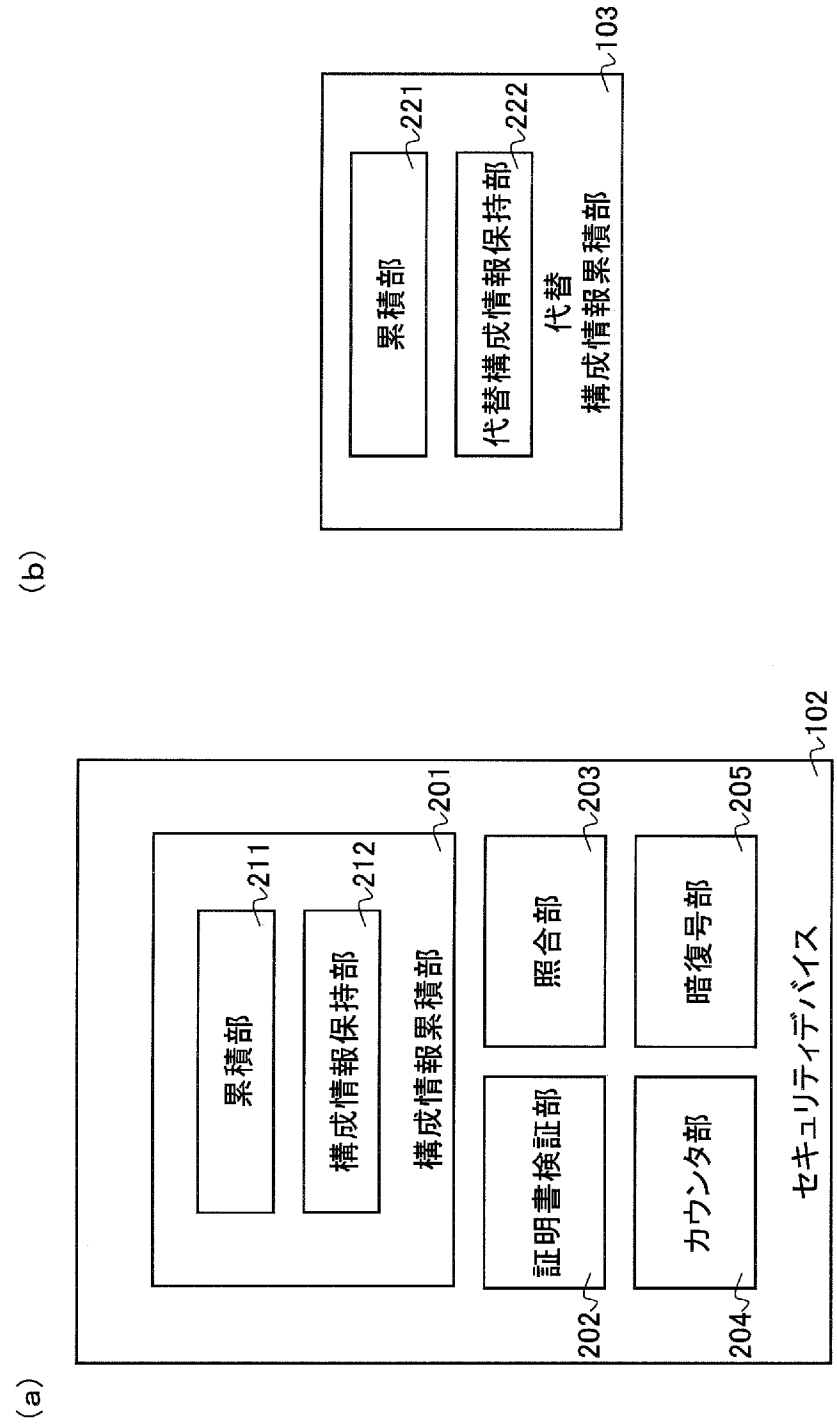
（ａ）前記検証手段による有効性の検証が成功した場合、前記起動の順番に達したソフトウェアモジュールを起動し、（ｂ）前記検証手段による有効性の検証が失敗した場合、前記代替累積値と前記起動の順番に達したソフトウェアモジュールに係るデジタル証明書に含まれる目標累積値とを比較し、前記目標累積値と前記代替累積値が一致すれば、前記起動の順番に達したソフトウェアモジュールを起動するブート制御手段と

を備えることを特徴とする集積回路。

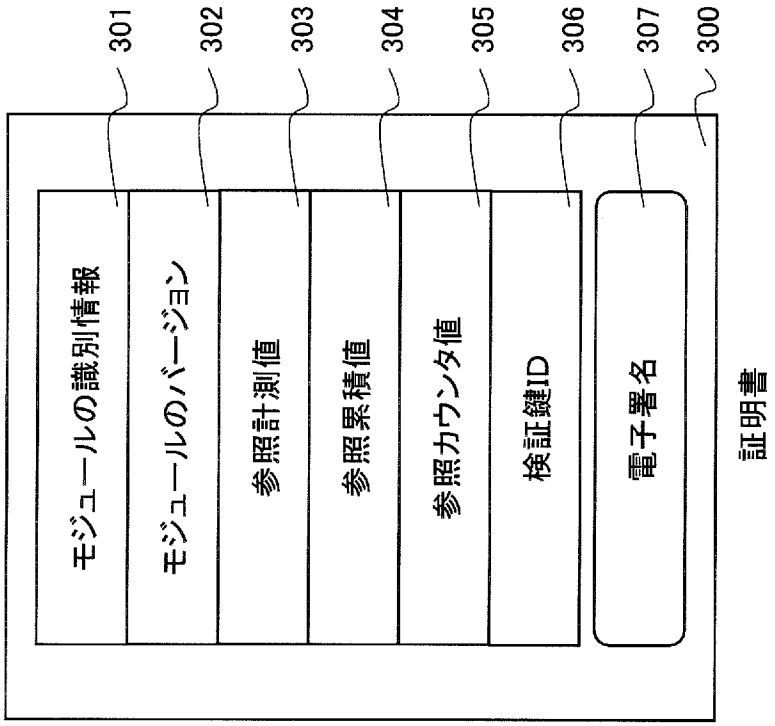
[図1]


100
端末
101
CPU
102
セキュリティデバイス
103
代替
構成情報累積部
104
更新手段
105
ブート制御手段
111
更新フラグ
保持部
112
セキュアブート
制御部
106
ソフトウェアモジュール
格納手段
107
証明書
格納手段
108
通知手段

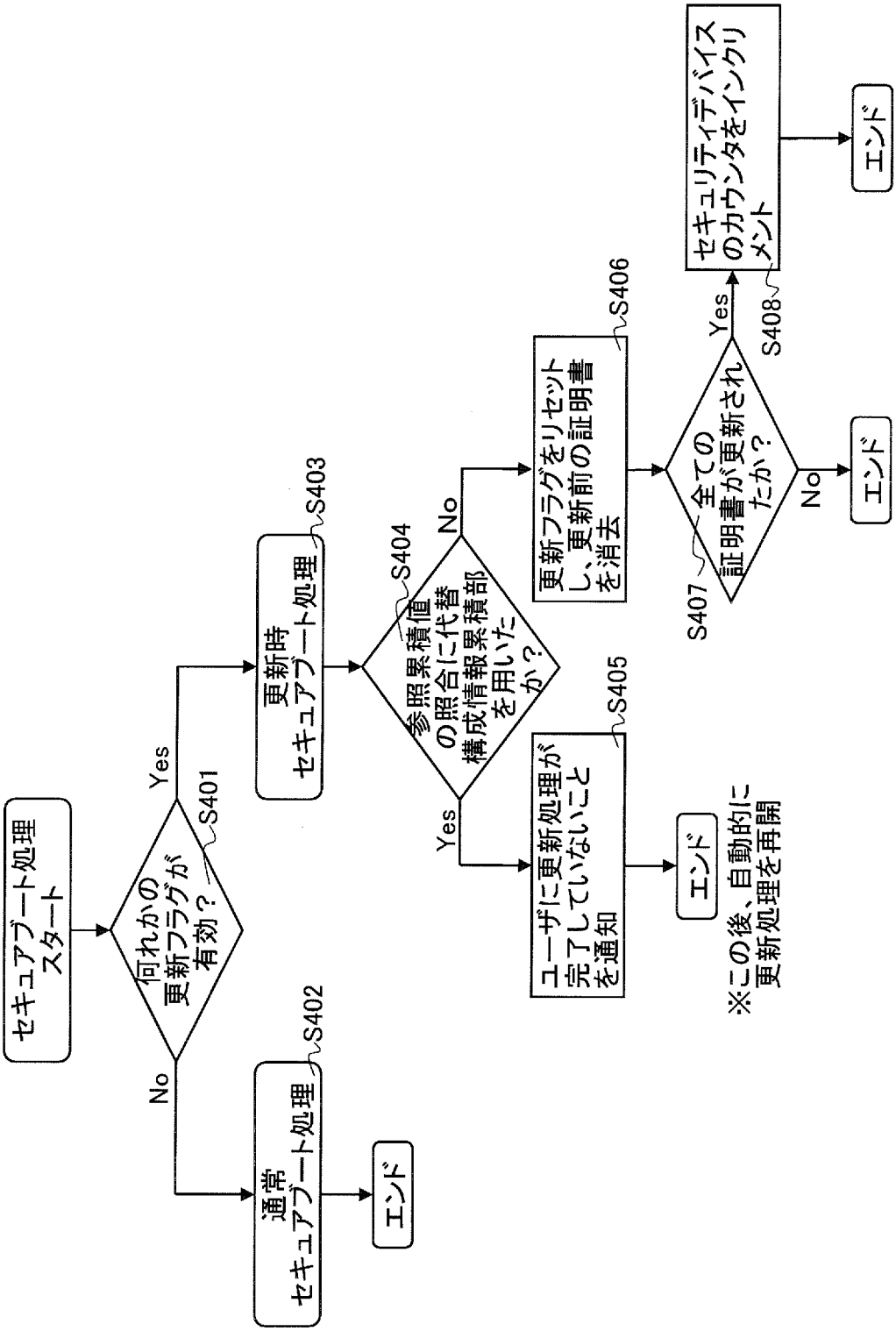
[図2]


(a)
102
セキュリティデバイス
201
構成情報累積部
211
累積部
212
構成情報保持部
202
証明書検証部
203
照合部
204
カウンタ部
205
暗復号部
(b)
103
代替
構成情報累積部
221
累積部
222
代替構成情報保持部

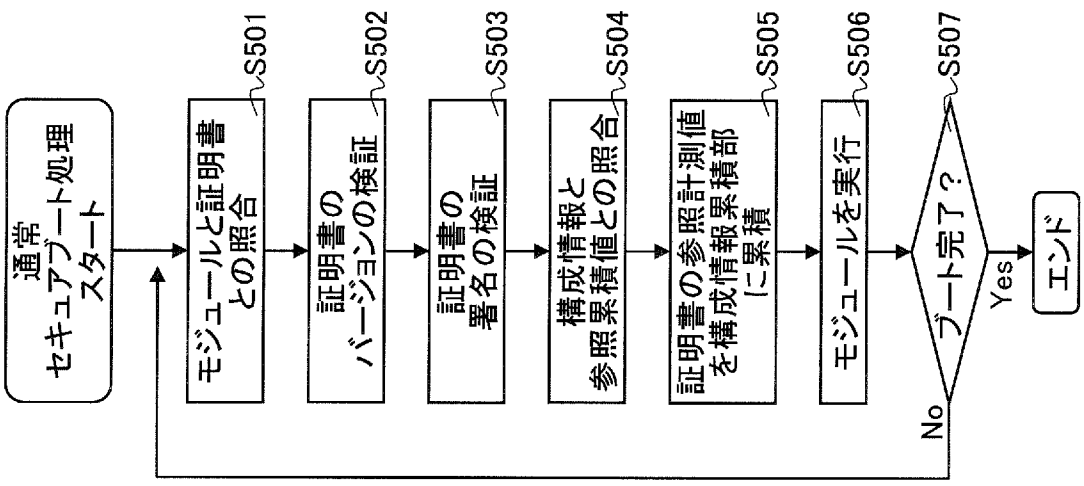
[図3]


301
302
303
304
305
306
307
300
モジュールの識別情報
モジュールのバージョン
参照計測値
参照累積値
参照カウンタ値
検証鍵ID
電子署名
証明書

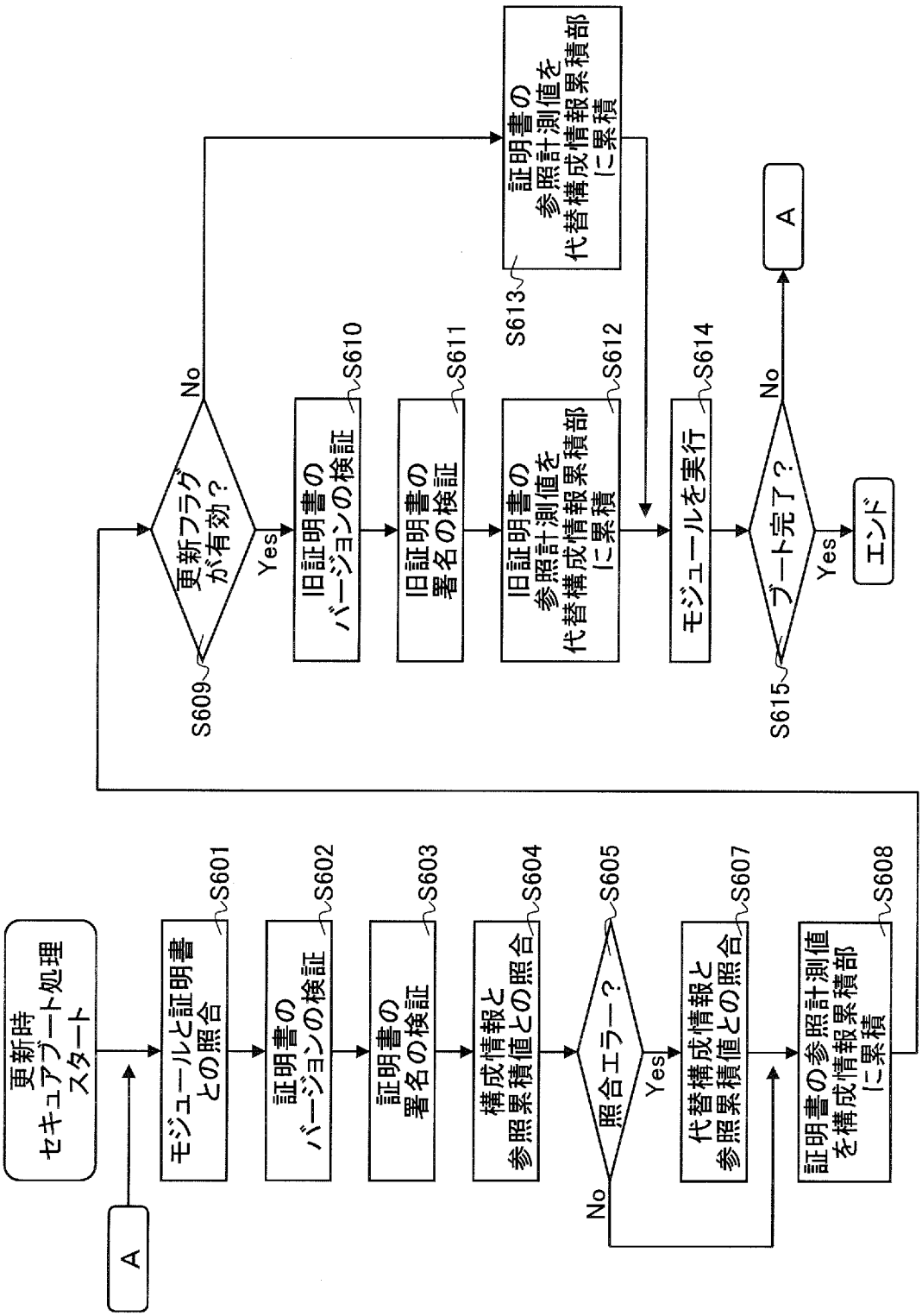
[図4]


セキュアブート処理
スタート
何れかの
更新フラグが
有効？
S401
Yes
No
通常
セキュアブート処理
S402
エンド
更新時
セキュアブート処理
S403
参照累積値
の照合に代替
構成情報累積部
を用いた
か？
S404
No
Yes
ユーザに更新処理が
完了していないこと
を通知
S405
エンド
※この後、自動的に
更新処理を再開
更新フラグをリセット
し、更新前の証明書
を消去
S406
全ての
証明書が更新され
たか？
S407
Yes
No
セキュリティデバイス
のカウンタをインクリ
メント
S408
エンド
エンド

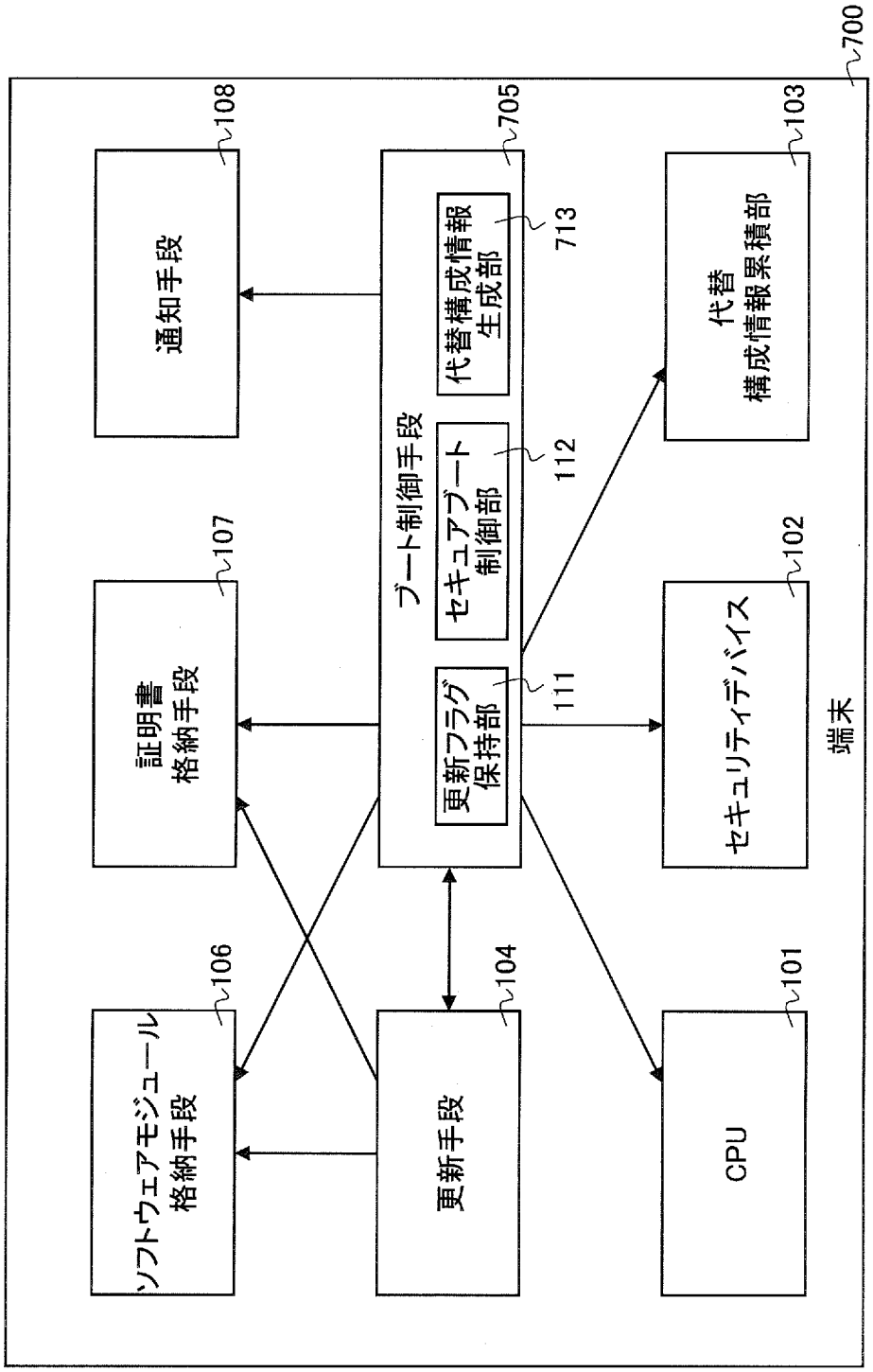
[図5]


通常
セキュアブート処理
スタート
S501
モジュールと証明書
との照合
S502
証明書の
バージョンの検証
S503
証明書の
署名の検証
S504
構成情報と
参照累積値との照合
S505
証明書の参照計測値
を構成情報累積部
に累積
S506
モジュールを実行
S507
ブート完了？
No
Yes
エンド

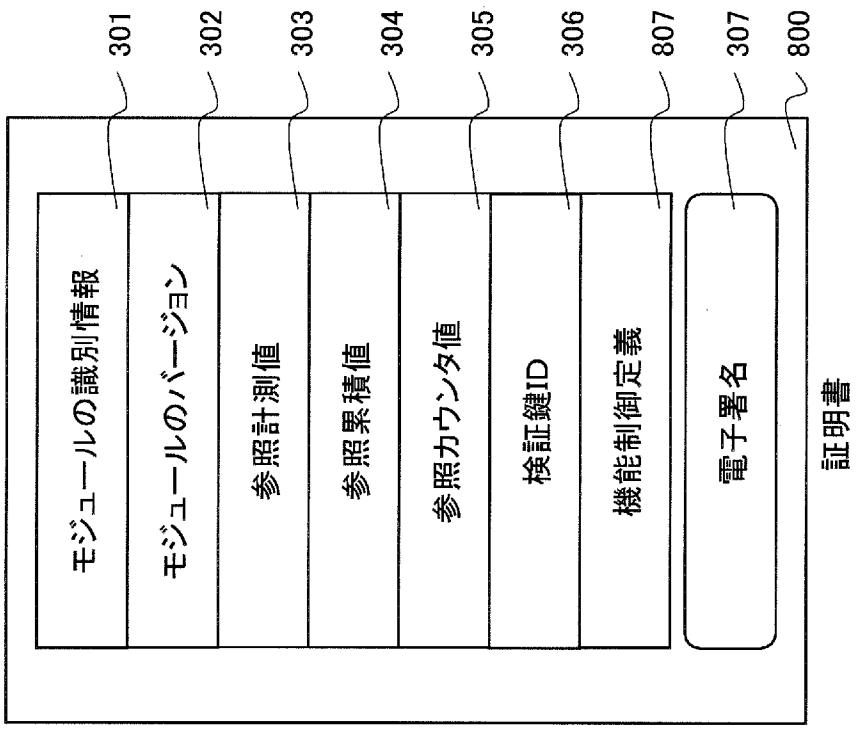
[図6]


更新時
セキュアブート処理
スタート
A
モジュールと証明書
との照合
S601
証明書の
バージョンの検証
S602
証明書の
署名の検証
S603
構成情報と
参照累積値との照合
S604
照合エラー？
S605
No
Yes
代替構成情報と
参照累積値との照合
S607
証明書の参照計測値
を構成情報累積部
に累積
S608
更新フラグ
が有効？
S609
No
Yes
旧証明書の
バージョンの検証
S610
旧証明書の
署名の検証
S611
旧証明書の
参照計測値を
代替構成情報累積部
に累積
S612
証明書の
参照計測値を
代替構成情報累積部
に累積
S613
モジュールを実行
S614
ブート完了？
S615
No
Yes
A
エンド

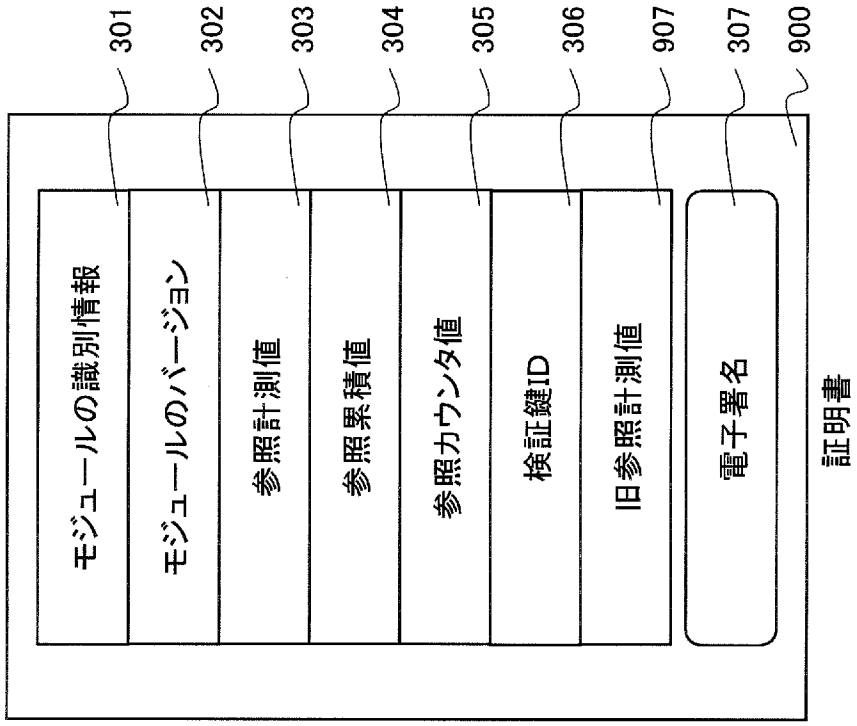
[図7]


700
端末
通知手段
108
ブート制御手段
705
代替構成情報生成部
713
セキュアブート制御部
112
更新フラグ保持部
111
代替構成情報累積部
103
証明書格納手段
107
セキュリティデバイス
102
ソフトウェアモジュール格納手段
106
更新手段
104
CPU
101

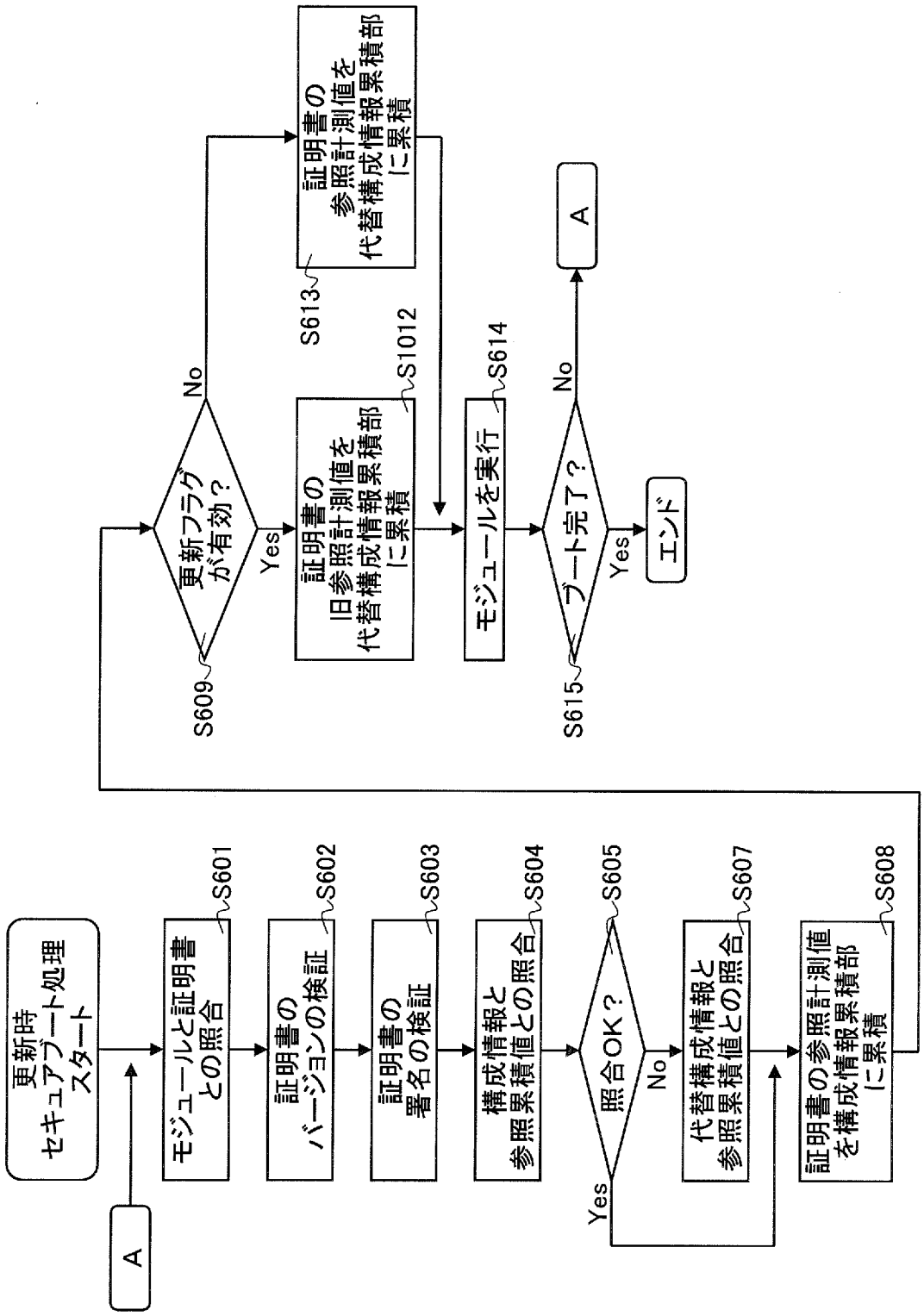
[図8]


301
302
303
304
305
306
807
307
800
モジュールの識別情報
モジュールのバージョン
参照計測値
参照累積値
参照カウンタ値
検証鍵ID
機能制御定義
電子署名
証明書

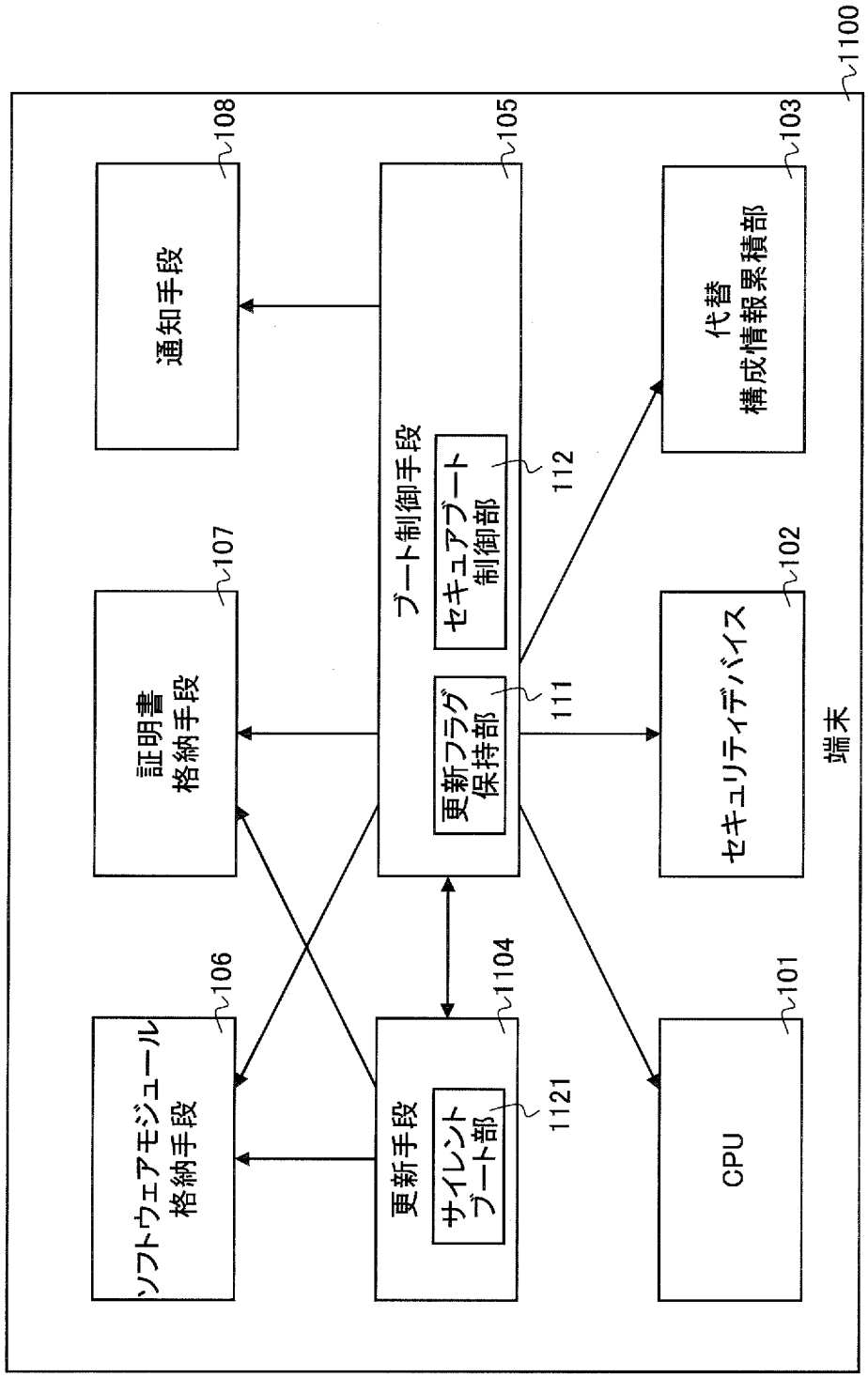
[図9]


301
302
303
304
305
306
907
307
900
モジュールの識別情報
モジュールのバージョン
参照計測値
参照累積値
参照カウンタ値
検証鍵ID
旧参照計測値
電子署名
証明書

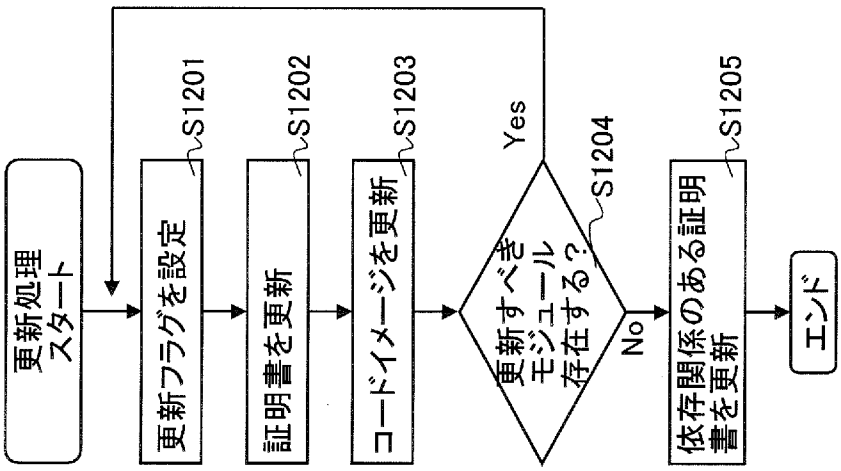
[図10]


更新時
セキュアブート処理
スタート
A
モジュールと証明書
との照合
S601
証明書の
バージョンの検証
S602
証明書の
署名の検証
S603
構成情報と
参照累積値との照合
S604
照合OK？
S605
Yes
No
代替構成情報と
参照累積値との照合
S607
証明書の参照計測値
を構成情報累積部
に累積
S608
更新フラグ
が有効？
S609
No
Yes
証明書の
旧参照計測値を
代替構成情報累積部
に累積
S1012
証明書の
参照計測値を
代替構成情報累積部
に累積
S613
モジュールを実行
S614
ブート完了？
S615
No
Yes
A
エンド

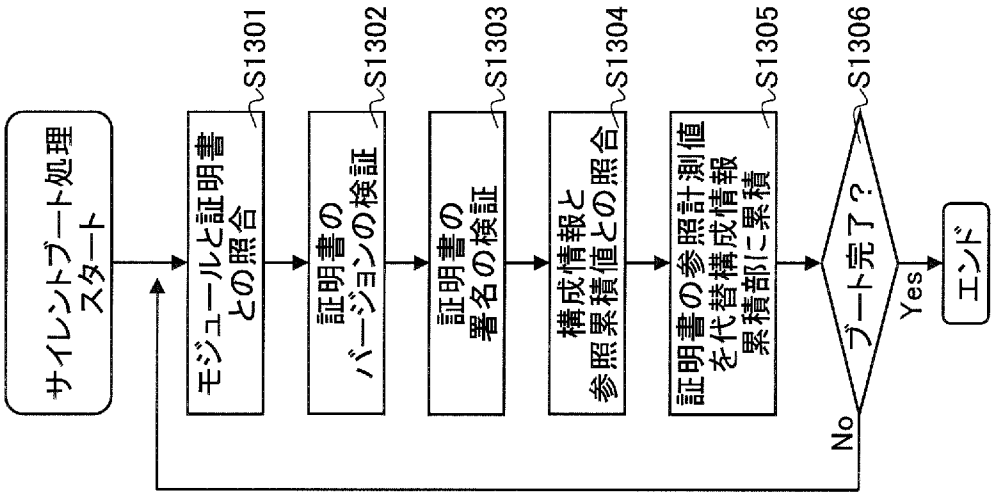
[図11]


1100
端末
通知手段
108
ブート制御手段
105
セキュアブート制御部
112
更新フラグ保持部
111
代替構成情報累積部
103
証明書格納手段
107
セキュリティデバイス
102
ソフトウェアモジュール格納手段
106
更新手段
1104
サイレントブート部
1121
CPU
101

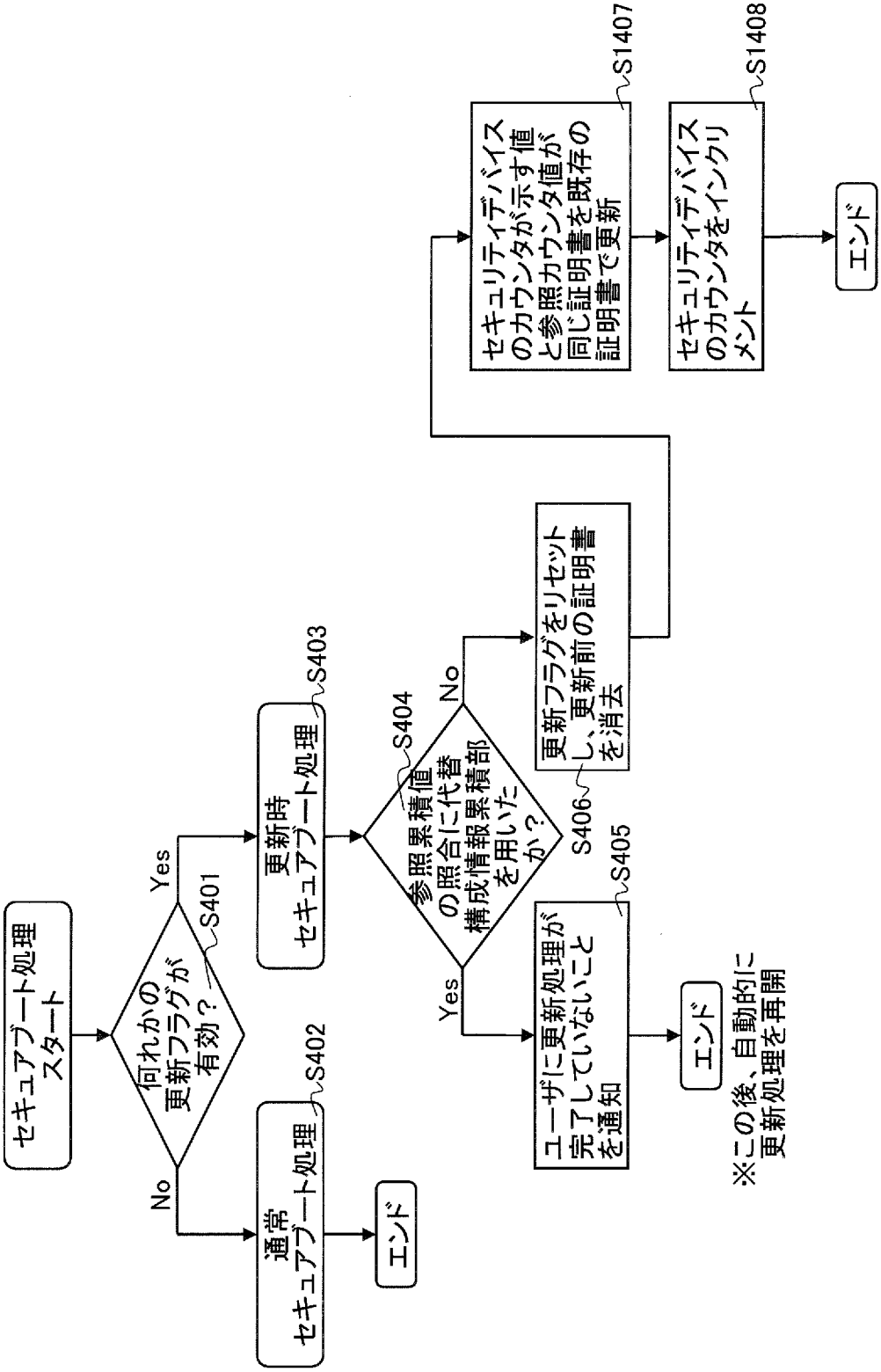
[図12]


更新処理
スタート
更新フラグを設定
S1201
証明書を更新
S1202
コードイメージを更新
S1203
更新すべき
モジュール
存在する？
S1204
Yes
No
依存関係のある証明
書を更新
S1205
エンド

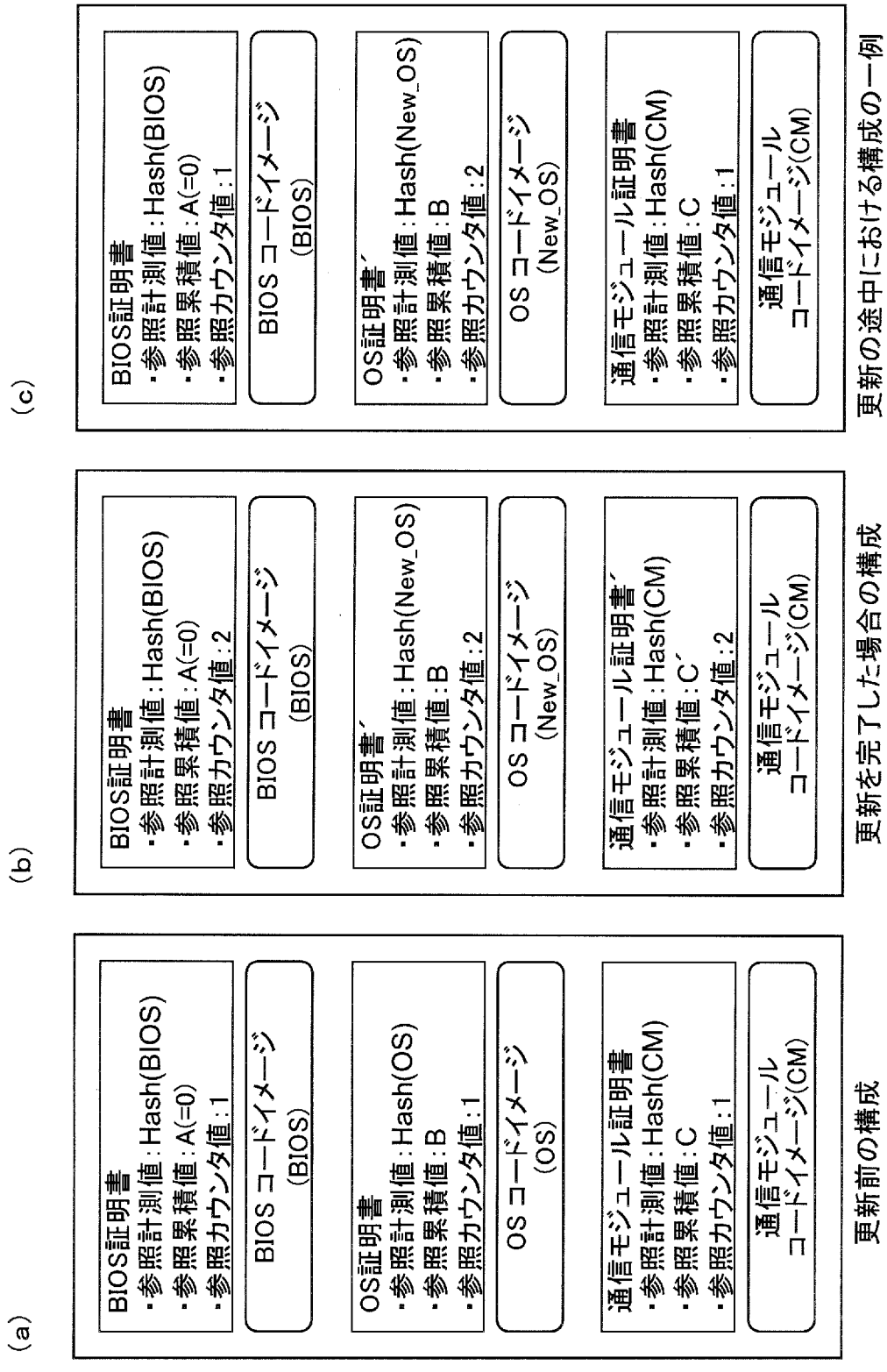
[図13]


サイレントブート処理
スタート
モジュールと証明書
との照合
S1301
証明書の
バージョンの検証
S1302
証明書の
署名の検証
S1303
構成情報と
参照累積値との照合
S1304
証明書の参照計測値
を代替構成情報
累積部に累積
S1305
ブート完了？
S1306
No
Yes
エンド

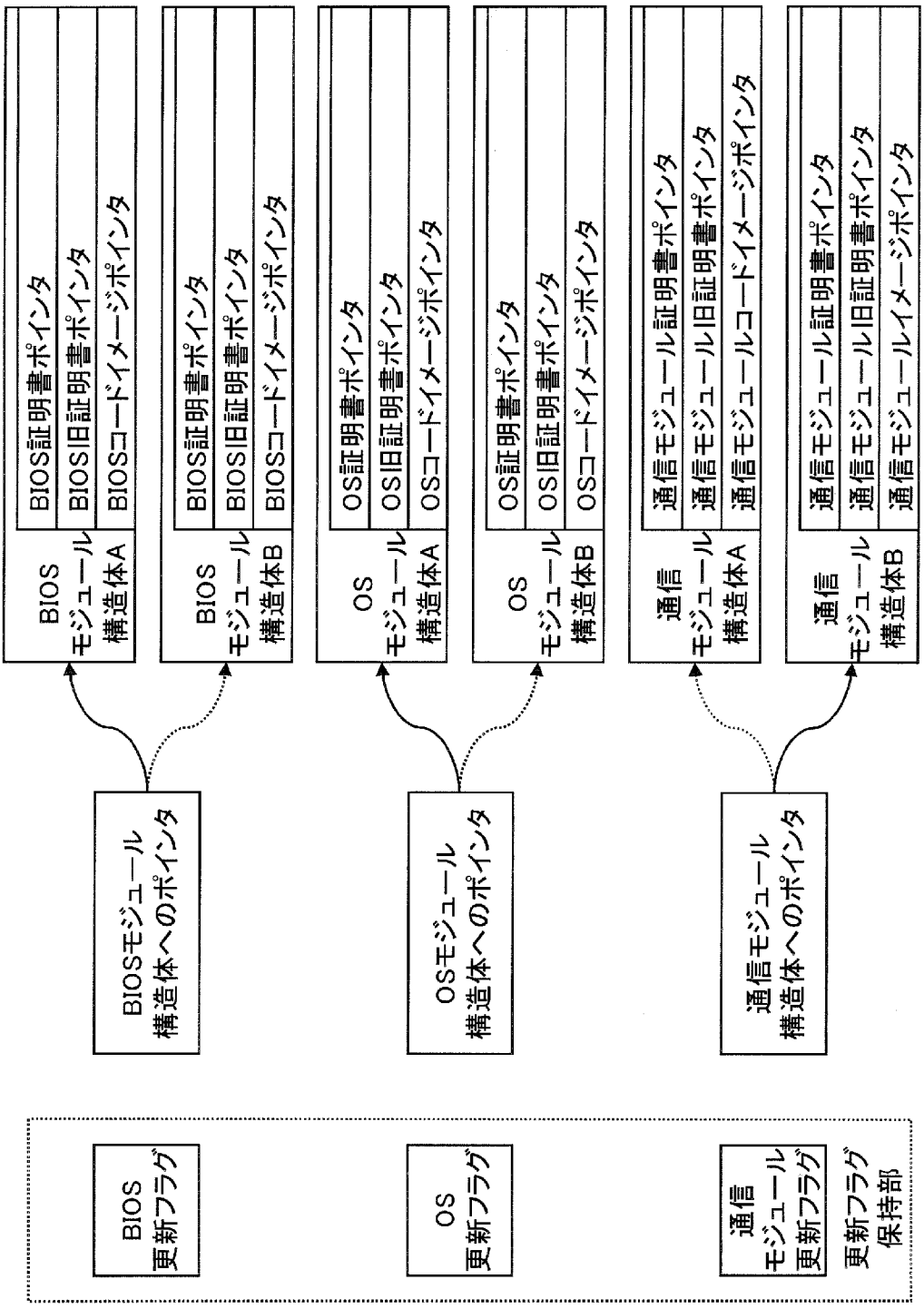
[図14]


セキュアブート処理
スタート
何れかの
更新フラグが
有効？
S401
Yes
No
通常
セキュアブート処理
S402
エンド
更新時
セキュアブート処理
S403
参照累積値
の照合に代替
構成情報累積部
を用いた
か？
S404
No
Yes
更新フラグをリセット
し、更新前の証明書
を消去
S406
ユーザに更新処理が
完了していないこと
を通知
S405
エンド
※この後、自動的に
更新処理を再開
セキュリティデバイス
のカウンタが示す値
と参照カウンタ値が
同じ証明書を既存の
証明書で更新
S1407
セキュリティデバイス
のカウンタをインクリ
メント
S1408
エンド

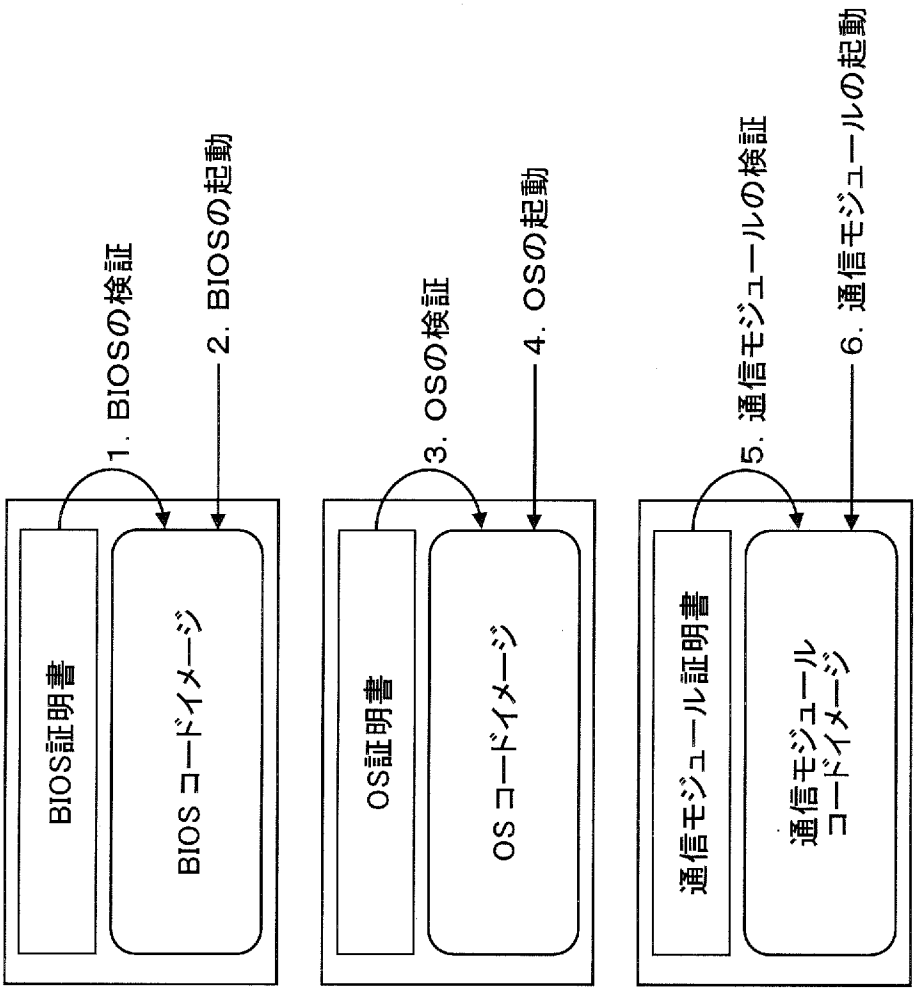
[図15]


(a)
BIOS証明書
・参照計測値:Hash(BIOS)
・参照累積値:A(=0)
・参照カウンタ値:1
BIOS コードイメージ
(BIOS)
OS証明書
・参照計測値:Hash(OS)
・参照累積値:B
・参照カウンタ値:1
OS コードイメージ
(OS)
通信モジュール証明書
・参照計測値:Hash(CM)
・参照累積値:C
・参照カウンタ値:1
通信モジュール
コードイメージ(CM)
更新前の構成
(b)
BIOS証明書
・参照計測値:Hash(BIOS)
・参照累積値:A(=0)
・参照カウンタ値:2
BIOS コードイメージ
(BIOS)
OS証明書´
・参照計測値:Hash(New_OS)
・参照累積値:B
・参照カウンタ値:2
OS コードイメージ
(New_OS)
通信モジュール証明書´
・参照計測値:Hash(CM)
・参照累積値:C´
・参照カウンタ値:2
通信モジュール
コードイメージ(CM)
更新を完了した場合の構成
(c)
BIOS証明書
・参照計測値:Hash(BIOS)
・参照累積値:A(=0)
・参照カウンタ値:1
BIOS コードイメージ
(BIOS)
OS証明書´
・参照計測値:Hash(New_OS)
・参照累積値:B
・参照カウンタ値:2
OS コードイメージ
(New_OS)
通信モジュール証明書
・参照計測値:Hash(CM)
・参照累積値:C
・参照カウンタ値:1
通信モジュール
コードイメージ(CM)
更新の途中における構成の一例

[図16]


BIOS証明書ポインタ
BIOS旧証明書ポインタ
BIOSコードイメージポインタ
BIOS モジュール 構造体A
BIOS証明書ポインタ
BIOS旧証明書ポインタ
BIOSコードイメージポインタ
BIOS モジュール 構造体B
OS証明書ポインタ
OS旧証明書ポインタ
OSコードイメージポインタ
OS モジュール 構造体A
OS証明書ポインタ
OS旧証明書ポインタ
OSコードイメージポインタ
OS モジュール 構造体B
通信モジュール証明書ポインタ
通信モジュール旧証明書ポインタ
通信モジュールコードイメージポインタ
通信 モジュール 構造体A
通信モジュール証明書ポインタ
通信モジュール旧証明書ポインタ
通信モジュールイメージポインタ
通信 モジュール 構造体B
BIOSモジュール 構造体へのポインタ
OSモジュール 構造体へのポインタ
通信モジュール 構造体へのポインタ
BIOS 更新フラグ
OS 更新フラグ
通信 モジュール 更新フラグ
更新フラグ 保持部

[図17]


1. BIOSの検証
2. BIOSの起動
BIOS証明書
BIOS コードイメージ
3. OSの検証
4. OSの起動
OS証明書
OS コードイメージ
5. 通信モジュールの検証
6. 通信モジュールの起動
通信モジュール証明書
通信モジュール
コードイメージ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/002728

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/22(2006.01)i, *G06F9/445*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/22, G06F9/445

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2008
Kokai Jitsuyo Shinan Koho	1971-2008	Toroku Jitsuyo Shinan Koho	1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-072909 A (International Business Machines Corp.), 22 March, 2007 (22.03.07), Full text; all drawings (Family: none)	1-13
A	US 2005/0108564 A1 (International Business Machines Corp.), 19 May, 2005 (19.05.05), Par. Nos. [0020], [0035]; Fig. 2 (Family: none)	1-13

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 23 October, 2008 (23.10.08)	Date of mailing of the international search report 04 November, 2008 (04.11.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/002728

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2005-523537 A (International Business Machines Corp.), 04 August, 2005 (04.08.05), Par. Nos. [0007], [0058]; Fig. 16 & US 2003/0200454 A1 & EP 1500225 A1 & WO 2003/090402 A1	7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／００２７２８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/22(2006.01)i, G06F9/445(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/22, G06F9/445

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2007-072909 A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2007.03.22, 全文, 全図（ファミリーなし）	1-13
A	US 2005/0108564 A1 (International Business Machines Corp.) 2005.05.19, [0020], [0035], Fig.2（ファミリーなし）	1-13
A	JP 2005-523537 A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2005.08.04, 段落【0007】,【0058】, 図16 & US 2003/0200454 A1 & EP 1500225 A1 & WO 2003/090402 A1	7

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ２３．１０．２００８	国際調査報告の発送日 ０４．１１．２００８
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３１４５ 赤穂　州一郎 電話番号　０３－３５８１－１１０１　内線　３５４６