(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
2006 年12 月7 日 (07.12.2006)

PCT

(10) 国際公開番号
WO 2006/129654 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G06F 13/00* (2006.01)
G06F 11/00 (2006.01) *G06F 21/22* (2006.01)
G06F 12/00 (2006.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2006/310764

(22) 国際出願日: 2006 年5 月30 日 (30.05.2006)

(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2005-161358 2005 年6 月1 日 (01.06.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [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): 松島 秀樹 (MATSUSHIMA, Hideki). 賀川 貴文 (KAGAWA, Takafumi). 芳賀 智之 (HAGA, Tomoyuki). 奥山 洋 (OKUYAMA, Hiroshi). 木村 重彦 (KIMURA, Shigehiko). 大岩 保樹 (OIWA, Yasuki). 井藤 好克 (ITO, Yoshikatsu).

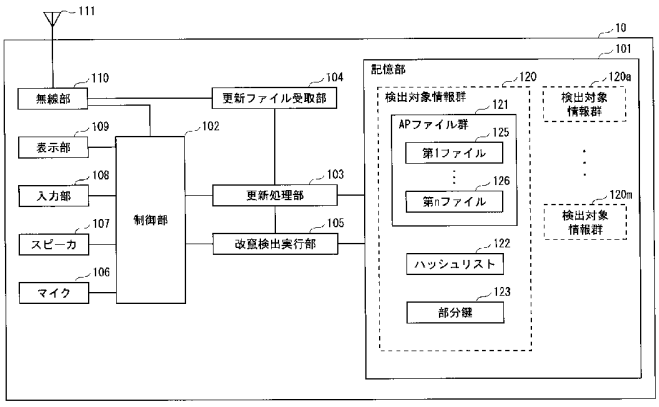
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,

[続葉有]

(54) **Title:** ELECTRONIC DEVICE, UPDATE SERVER DEVICE, KEY UPDATE DEVICE

(54) 発明の名称: 電子機器、更新サーバ装置、鍵更新装置



110 RADIO UNIT
109 DISPLAY UNIT
108 INPUT UNIT
107 SPEAKER
106 MICROPHONE
102 CONTROL UNIT
104 UPDATE FILE RECEPTION UNIT
103 UPDATE PROCESSING UNIT
105 TAMPER DETECTION EXECUTION UNIT
101 STORAGE UNIT
120 DETECTION OBJECT INFORMATION GROUP
121 AP FILE GROUP
125 FIRST FILE
126 n-TH FILE
122 HASH LIST
123 PARTIAL KEY
120a DETECTION OBJECT INFORMATION GROUP
120m DETECTION OBJECT INFORMATION GROUP

(57) **Abstract:** There is provided an electronic device capable of suppressing a data amount associated with communication when updating a file concerning software and performing tamper detection. The electronic device includes an application file associated with operation of application software and updating the application file via a network. The electronic device stores the application file having at least one data set, receives update data and position information indicating the position to be updated by the update data in the application file, from an external device via the network, rewrites the data existing at the position indicated by the position information into the update data, and updates only a part of the application file, thereby checking whether the application file has been tampered.

[続葉有]

WO 2006/129654 A1

RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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
— 補正書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: ソフトウェアに係るファイルを更新する場合に通信に係るデータ量を従来よりも抑えることのでき、且つ改竄検出を行う電子機器を提供する。 アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器であって、１つ以上のデータからなるアプリケーションファイルを記憶し、更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取り、前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新し、更新された前記アプリケーションファイルが改竄されているか否かの確認を行う。

明 細 書

電子機器、更新サーバ装置、鍵更新装置

技術分野

[0001] 電子機器が保持するソフトウェアをネットワークを介して更新し、改竄の有無を検出する技術に関する。

背景技術

[0002] プログラムの不正な改竄や解析を防止する技術は従来から研究されている。たとえば、非特許文献1では、ソフトウェアの解析を防ぐための基本原則や具体的手法に関して記述している。また、非特許文献2では、ソフトウェアの解析を防ぐためのツールとして開発したTRCS(Tamper Resistant Coding System)の技術課題とその対策について記述している。このようなソフトウェアの不正な解析や改竄を防ぐ技術を、「耐タンパー技術」と呼ぶ。以降、不正な改竄を、単に「改竄」といい、正当な改竄を「更新」という。

[0003] 以上のような耐タンパー技術は既に実用化されている。例えば、PC上で市販のDVDコンテンツを再生するソフトウェアがそれである。DVDのコンテンツは不正コピーを防止するために暗号化されており、この再生を行うには復号化するための鍵が必要となる。この鍵が悪意のあるユーザの手に渡ると、DVDコンテンツは容易にコピーされインターネットを通じて不正にばら撒かれる可能性がある。このため、前述のソフトウェアは耐タンパー技術によって保護されている。

[0004] このように、近年DVDに代表されるようにデジタルコンテンツが普及し、それらをコンピュータのような仕様の公開されたシステム上で再生するソフトウェアには耐タンパー技術が必要不可欠となっている。

携帯電話などの電子機器においても耐タンパー技術の適用が行われている。特許文献1では、電子機器内のメモリに対する改竄を防止するために、ハッシュ関数を用いた耐タンパー技術の一つである改竄検出方式が開示されている。

[0005] また、近年、携帯電話をはじめとした電子機器はネットワーク化が進み、既に組み込まれたソフトウェアに対して製品の出荷後も不具合を修正するソフトウェアを、ネット

ワークを通じて配布し更新することが可能となってきている。

非特許文献1:「逆解析や改変からソフトを守る」 日経エレクトロニクス 1998.1.5 (P209－220)

非特許文献2:「ソフトウェアの耐タンパー化技術」 富士ゼロックス テクニカル レポート No.13 (P20－28)

特許文献1:特表2001－500293号公報

特許文献2:特開2005－018725号公報

発明の開示

発明が解決しようとする課題

[0006] 改竄検出を行う電子機器がネットワークを通じてソフトウェアを更新する場合、更新されたソフトウェア自体が、ネットワークを通じて電子機器に配布されるので、更新されたソフトウェアのサイズが大きくなればなるほど、電子機器が更新されたソフトウェアを受信する時間が長くなる。つまり、ソフトウェアの更新時間が長くなるので、利用者にとっては不満が生じてしまうという問題がある。

[0007] そこで、本発明は、ソフトウェアに係るファイルを更新する場合に通信に係るデータ量を従来よりも抑えることのでき、且つ改竄検出を行う電子機器、更新サーバ装置、鍵更新装置、更新方法、更新プログラム、ソフトウェアの更新に必要な情報を取得する取得方法及び取得プログラムを提供することを目的とする。

課題を解決するための手段

[0008] 上記目的を達成するために、本発明は、アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器であって、1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段と、更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取手段と、前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新する更新処理手段と、更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行手段とを備えることを特徴とする。

発明の効果

[0009] 上記に示した構成によると、電子機器は、ネットワークを介してアプリケーションファイルに含まれるデータに対する更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを受け取り、受け取った位置情報に基づいて前記データを前記更新データに書き換えて、アプリケーションファイルの一部のみを更新するので、外部装置から更新されたアプリケーションファイルを受け取る場合よりも通信に係るデータ量を少なくすることができる。

[0010] ここで、前記受取手段は、更新データと位置情報との組を少なくとも1つ以上受け取り、前記更新処理手段は、前記位置情報にて示される位置に基づいて、前記アプリケーションファイルの更新位置を決定する位置決定部と、決定された前記更新位置を前記更新データの書き込み開始位置として、前記更新データを書き込む書込部と、前記受取手段にて受け取った1つ以上の更新データ全ての書き込みが完了するまで、前記位置決定部と前記書込部の処理を行うように制御する更新制御部とを備えるとしてもよい。

[0011] この構成によると、電子機器は、受け取った位置情報にて示される位置に基づいて、更新データの書込開始位置を決定し、決定した書込開始位置から前記更新データを書き込むことができる。

ここで、前記更新制御部は、全ての更新データの書き込みが完了すると、前記改竄検出実行手段の処理を開始するように制御するとしてもよい。

[0012] この構成によると、電子機器は、アプリケーションファイルの更新後に、更新したアプリケーションファイルが改竄されているか否かの確認を行うことができるので、更新後のアプリケーションファイルの正当性を保証することができる。

ここで、前記更新処理手段は、さらに、アプリケーションファイルの更新中であることを示す第1の情報、又は更新中でないことを示す第2の情報の何れかを示すフラグを記憶しているフラグ記憶部と、前記フラグが示す情報を変更するフラグ変更部とを備え、前記フラグ変更部は、前記受取手段が更新データと位置情報との組を少なくとも1つ以上受け取るときに、前記フラグの情報を、前記第1の情報に変更し、前記改竄検出実行手段にて改竄が検出されなかった場合に、前記フラグの情報を、前記第2

の情報に変更するとしてもよい。

[0013] この構成によると、電子機器は、フラグを用いることによりアプリケーションファイルの更新中であるか否かを識別することができる。

ここで、前記更新制御部は、さらに、前記電子機器に電源が投入されると、前記フラグが示す情報を確認し、第1の情報である場合には、前記位置決定部と前記書込部の処理を行うように制御するとしてもよい。

[0014] この構成によると、電子機器は、電源投入時にフラグが示す情報が第1の情報である場合には、再度、アプリケーションファイルの更新を行う。これにより、電子機器は、アプリケーションファイルの更新中に電源が切られも、その後電源が投入されることにより、確実にアプリケーションファイルの更新を行うことができる。

ここで、前記アプリケーションファイルは、1つ以上のブロックに分割されており、前記更新データは、前記1以上のブロックのうち少なくとも1つ以上の更新対象ブロックに含まれ、前記記憶手段は、1つ以上の前記ブロックそれぞれに対する基準改竄検出値を有する改竄検出リストを記憶しており、前記受取手段は、さらに、1つ以上の前記更新対象ブロックそれぞれに対する新たな基準改竄検出値と、前記1つ以上の前記更新対象ブロックそれぞれに対する基準改竄検出値の、前記改竄検出リストにおける位置を示す改竄検出位置情報とからなる組を受け取り、前記更新処理手段は、さらに、1つ以上の新たな基準改竄検出値と、前記改竄検出値位置情報とを用いて、前記改竄検出リストを更新し、前記改竄検出実行手段は、前記更新された改竄検出リストが正当なものである場合にのみ、前記更新された改竄検出リストが有する少なくとも1つ以上の基準改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認するとしてもよい。

[0015] この構成によると、電子機器は、改竄検出リストの正当性を確認しているので、改竄検出値自体を改竄することで不正なブロックを正当であると誤認させる行為を防止することができる。

ここで、前記アプリケーションファイルは、1つ以上のブロックに分割されており、前記記憶手段は、1つ以上の前記ブロックそれぞれに対する基準改竄検出値を有する改竄検出リストを記憶しており、前記改竄検出実行手段は、前記アプリケーションソフ

トウェアの起動時に処理を開始し、前記改竄検出リストが正当なものである場合にのみ、前記改竄検出リストが有する少なくとも1つ以上の改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認するとしてもよい。

[0016] この構成によると、電子機器は、改竄検出リストの正当性を確認しているので、改竄検出値自体を改竄することで不正なブロックを正当であると誤認させる行為を防止することができる。

ここで、前記改竄検出手段は、改竄検出対象であるブロックに対する検出用改竄検出値を算出し、算出した検出用改竄検出値と、改竄検出対象であるブロックに対する改竄検出値とが一致するか否かを判断し、一致すると判断する場合には前記アプリケーションファイルは改竄されていないとし、一致しない場合には前記アプリケーションファイルは改竄されているとするとしてもよい。

[0017] この構成によると、電子機器は、改竄検出対象のブロックに対する検出用改竄検出値と、改竄検出リストに含まれる前記ブロックに対する改竄検出値とを用いて、前記ブロックが改竄されているか否かを確認することができる。

ここで、前記記憶部は、部分鍵を記憶しており、前記改竄検出実行手段は、耐タンパ化されており、マスタ鍵を記憶し、前記部分鍵と前記マスタ鍵とを用いて、改竄検出鍵を生成し、生成した改竄検出鍵を用いて、前記検出用改竄検出値を算出するとしてもよい。

[0018] この構成によると、電子機器は、改竄検出実行手段が耐タンパ化されており、且つマスタ鍵を記憶しているので、改竄検出鍵の生成、及び生成した改竄検出鍵を不正解析者に解析されないようにすることができる。

ここで、前記受取手段は、前記部分鍵とは異なる別の部分鍵と、前記部分鍵が前記記憶部にて記憶されている位置を示す鍵位置情報とを受け取り、前記更新処理手段は、前記鍵位置情報に基づいて、前記部分鍵を前記別の部分鍵に更新するとしてもよい。

[0019] この構成によると、電子機器は、部分鍵を更新することができる。これにより、電子機器は、改竄検出鍵が不正解析者に知られたとしても、部分鍵を更新することにより、新たな改竄検出鍵を生成することができる。

ここで、前記改竄検出リストは、前記1つ以上のブロックそれぞれに対する基準改竄検出値を含むデータ部と、前記データ部に対する基準データ部改竄検出値を含むヘッダ部とから構成され、前記改竄検出実行手段は、前記データ部に対する検出用データ部改竄検出値を算出し、算出した前記検出用データ部改竄検出と前記基準データ部改竄検出値とが一致する場合に、前記改竄検出リストが正当なものであるとするとしてもよい。

[0020] この構成によると、電子機器は、改竄検出リストに含まれるデータ部に対する改竄検出値を確認することにより、改竄検出リストの正当性を保証することができる。これにより、アプリケーションファイルの改竄検出をより正確に行うことができる。

ここで、前記データ部は暗号化されており、前記改竄検出実行手段は、暗号化された前記データ部に対する検出用改竄検出値を算出し、前記改竄検出リストが正当なものである場合に、暗号化された前記データ部を復号するとしてもよい。

[0021] この構成によると、電子機器は、データ部が暗号化されているので、改竄検出リストに含まれる各ブロックの改竄検出値を不正解析者に知られないようにすることができる。

ここで、前記改竄検出リストにおいて、基準改竄検出値のそれぞれに対して、対応するブロックが改竄検出の対象として使用すべきか否かを示す判断情報が対応付けられており、前記改竄検出実行手段は、前記判断情報がブロックを改竄検出の対象としない旨を示す場合には、当該ブロックに対する改竄検出は行わないとしてもよい。

[0022] この構成によると、電子機器は、判断情報が改竄検出の対象としない旨を示す場合にはそのブロックに対する改竄検出を行わないようにすることができる。これにより、アプリケーションファイルが更新された結果、一部のブロックが不要となった場合、不要となったブロックに対しての改竄検出を省略することができる。

ここで、前記改竄検出リストは、前記1つ以上のブロックそれぞれに対する基準改竄検出値と、改竄検出の対象となるアプリケーションソフトウェアの種別を示すアプリケーション種別とが対応付けられた組を1つ以上含み、前記改竄検出実行手段は、起動されたアプリケーションソフトウェアに対するアプリケーション種別に対応する基準

改竄検出値それぞれのうち少なくとも1つ以上の改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認するとしてもよい。

[0023] この構成によると、電子機器は、起動されたアプリケーションソフトウェアのアプリケーション種別に対応する1つ以上の改竄検出値を用いて、改竄検出を行うことができる。

ここで、前記アプリケーションソフトウェアの動作に係るアプリケーションファイルは複数個あり、前記アプリケーションファイルのそれぞれは、1つ以上のブロックに分割されており、前記改竄検出リストは、アプリケーションファイルそれぞれに対して、1つ以上のブロックそれぞれに対する基準改竄検出値を基準値群として格納し、1つ以上の前記基準値群のうち前記アプリケーションソフトウェアの起動時に改竄検出に用いる少なくとも1つ以上の基準値群の範囲を示す範囲情報を有し、前記改竄検出実行手段は、前記アプリケーションソフトウェアの起動時に、前記改竄検出リストが有する前記範囲情報にて示される少なくとも1つ以上の基準値群を用いて、改竄検出の対象となるブロックが改竄されているか否かを確認するとしてもよい。

[0024] この構成によると、電子機器は、アプリケーションソフトウェアの起動時に、範囲情報に示される少なくとも1つ以上基準値群を用いて優先的に改竄の検出を行うので、アプリケーションソフトウェアの起動にかかる時間を、すべての基準値群を用いて改竄検出を行う場合に比べて短くすることができる。

ここで、前記更新処理手段及び前記改竄検出実行手段は、耐タンパ化されているとしてもよい。

[0025] この構成によると、電子機器は、更新処理手段及び改竄検出実行手段が耐タンパ化されているので、更新処理の動作、改竄検出の動作を不正解析者に解析されないようにすることができる。

また、本発明は、ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置であって、更新後のアプリケーションファイルを取得する第1取得手段と、取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを第2取得手段

と、取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信手段とを備えることを特徴とする。

[0026] この構成によると、更新サーバ装置は、アプリケーションファイルに含まれるデータに対する更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを取得し、取得した更新データ及び位置情報とを、ネットワークを介して電子機器に送信するので、アプリケーションファイルを送信する場合よりも通信に係るデータ量を少なくすることができる。

[0027] ここで、前記更新前のアプリケーションファイルは、所定の大きさからなる1つ以上の更新前ブロックに分割されており、前記第1取得手段は、さらに、1つ以上の前記更新前ブロックそれぞれと、前記更新前ブロック毎に対する基準改竄検出値とからなる更新前改竄検出リストを取得し、前記更新サーバ装置は、さらに、前記更新後のアプリケーションファイルを前記所定の大きさに分割された1つ以上の更新後ブロックを取得し、取得した1つ以上の更新後ブロックそれぞれに対して基準改竄検出値を再計算して新たな改竄検出リストを生成する改竄検出リスト生成手段を備え、前記第2取得手段は、さらに、前記改竄検出リスト生成手段にて生成された新たな改竄検出リストから、前記更新データを含む更新後ブロックと、その更新後ブロックに対応する再計算された基準改竄検出値と、その更新後ブロックに対応する更新前ブロックの前記更新前改竄検出リストにおける位置を示す改竄検出値位置情報とを取得し、前記送信手段は、さらに、前記第2取得手段にて取得された更新後ブロックと前記基準改竄検出値と前記改竄検出値位置情報とを前記電子機器に送信するとしてもよい。

[0028] この構成によると、更新サーバ装置は、第2取得手段にて取得された更新後ブロックと、その基準改竄検出値と、改竄検出値位置情報と電子機器に送信するので、電子機器では、更新されたブロックに対する基準改竄検出値を、常に最新の値とすることができる。

ここで、前記改竄検出リスト生成手段は、外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、前記1以上の更新後ブロックそれぞれに対する基準改竄検出値を算出するとしてもよい。

[0029] この構成によると、更新サーバ装置は、部分鍵とマスタ鍵とを用いて生成された改

竄検出鍵を用いて、基準改竄検出値を計算することができる。

ここで、前記更新サーバ装置は、前記外部装置によって更新された部分鍵と前記マスタ鍵とを用いて更新された改竄検出鍵を受け取ると、記憶している前記改竄検出鍵を、受け取った前記更新された改竄検出鍵に更新し、さらに、前記更新された部分鍵を前記外部装置から受け取り、前記改竄検出リスト生成手段は、前記更新された改竄検出鍵を用いて、前記1以上の更新後ブロックのそれぞれに対する基準改竄検出値を算出し、前記第2取得手段は、さらに、前記電子機器にて前記部分鍵が記憶されている位置を示す鍵位置情報を取得し、前記送信手段は、さらに、前記更新された部分鍵と、前記鍵位置情報とを前記電子機器に送信するとしてもよい。

[0030] この構成によると、更新サーバ装置は、改竄検出鍵を更新することができる。これにより、更新サーバ装置は、改竄検出鍵が不正解析者に知られたとしても、新たな改竄検出鍵を外部装置から受け取ることにより、不正解析者に知られた改竄検出鍵を用いることなく新たな基準改竄検出値を算出することができる。

ここで、前記改竄検出リストは、前記1つ以上の更新後ブロックそれぞれと、前記更新後ブロック毎に対する基準改竄検出値とからなるデータ部を有し、前記改竄検出リスト生成手段は、生成した新たな改竄検出リストのデータ部を暗号化するとしてもよい。

[0031] この構成によると、更新サーバ装置は、データ部が暗号化されているので、改竄検出リストに含まれる各ブロックの改竄検出値を不正解析者に知られないようにすることができる。

ここで、前記更新後改竄検出リストは、ヘッダ部を有し、前記改竄検出リスト生成手段は、外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、暗号化されたデータ部に対するデータ部改竄検出値を算出し、算出したデータ部改竄検出値を前記ヘッダ部へ格納するとしてもよい。

[0032] この構成によると、更新サーバ装置は、暗号化されたデータ部に対するデータ部改竄検出値を算出するので、暗号化されたデータ部に対する正当性を保証することができる。

ここで、前記改竄検出リストは、ヘッダ部と、前記1つ以上の前記更新後ブロックそれぞれと、前記更新後ブロック毎に対する基準改竄検出値とからなるデータ部とを有し、前記改竄検出リスト生成手段は、外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、前記データ部に対するデータ部改竄検出値を算出し、算出したデータ部改竄検出値を前記ヘッダ部へ格納するとしてもよい。

[0033] この構成によると、更新サーバ装置は、データ部に対するデータ部改竄検出値を算出するので、データ部に対する正当性を保証することができる。

ここで、前記改竄検出リスト生成手段は、前記データ部改竄検出値の算出後、前記データ部を暗号化するとしてもよい。

この構成によると、更新サーバ装置は、データ部が暗号化されているので、改竄検出リストに含まれる各ブロックの改竄検出値を不正解析者に知られないようにすることができる。

[0034] また、本発明は、1つ以上のブロックに分割されたアプリケーションファイルに対してブロック毎に改竄検出値を算出するために用いられる改竄検出鍵を生成する鍵生成装置であって、前記改竄検出鍵は、マスタ鍵と、部分鍵とから生成され、前記鍵生成装置は、前記マスタ鍵と、更新された部分鍵とを取得する鍵取得手段と、前記マスタ鍵と前記更新された部分鍵とを用いて新たな改竄検出鍵を生成する鍵生成手段と、前記鍵生成手段にて生成された改竄検出鍵を、前記改竄検出値を含む改竄検出リストを生成する外部装置へ配布する配布手段とを備えることを特徴とする。

[0035] この構成によると、鍵更新装置は、外部装置から改竄検出鍵が漏洩したとしても、部分鍵を更新するだけで、不正行為を行なった外部装置の持つ改竄検出鍵とは異なる新たな改竄検出鍵を生成することができる。

ここで、前記配布手段は、前記更新された部分鍵を、前記外部装置を介して前記アプリケーションファイルが改竄されているか否かの確認を行う電子機器へ配布するとしてもよい。

[0036] この構成によると、更新された部分鍵を電子機器に、外部装置を介して配布することができる。

図面の簡単な説明

[0037] [図1]プログラム更新システム1の概要を示す図である。

[図2]携帯電話機10の構成を示すブロック図である。

[図3]ハッシュリスト122のデータ構造の一例を示す図である。

[図4]更新データリスト150のデータ構造の一例を示す図である。

[図5]更新処理部103の構成を示すブロック図である。

[図6]改竄検出実行部105構成を示すブロック図である。

[図7]更新サーバ装置20の構成を示すブロック図である。

[図8]ハッシュリスト生成部203の構成を示すブロック図である。

[図9]鍵更新装置30の構成を示すブロック図である。

[図10]更新サーバ装置20にて行われる更新データリスト、及びハッシュリストの生成の動作を示す流れ図である。

[図11]ハッシュリスト更新時の動作概要を示す流れ図である。

[図12]携帯電話機10にて行われる更新処理の動作を示す流れ図である。図13へ続く。

[図13]携帯電話機10にて行われる更新処理の動作を示す流れ図である。図12から続く。

[図14]携帯電話機10にて行われるAP起動時の動作を示す流れ図である。

[図15]携帯電話機10にて行われる改竄検出処理の動作を示す流れ図である。図16へ続く。

[図16]携帯電話機10にて行われる改竄検出処理の動作を示す流れ図である。図15から続く。

[図17]第1の実施の形態で用いられる各鍵の関係と、鍵が利用される場面との関係を示す図である。

[図18]ハッシュリスト122aのデータ構造の一例を示す図である。

[図19]ハッシュリスト122bのデータ構造の一例を示す図である。

[図20]ファイルのブロック数が「8」から「7」に減少した場合のハッシュ情報1030の一例を示す。

[図21]ハッシュリスト122cのデータ構造の一例を示す図である。

[図22]ハッシュリスト122dのデータ構造の一例を示す図である。

[図23]1以上のAPファイル群に対して、1つのハッシュリスト及び部分鍵を与える場合における記憶部101構成を示すブロック図である。

符号の説明

[0038] 1 プログラム更新システム

10 携帯電話機

20 更新サーバ装置

30 鍵更新装置

40 携帯網

50 インターネット

101 記憶部

102 制御部

103 更新処理部

104 更新ファイル受取部

105 改竄検出実行部

106 マイク

107 スピーカ

108 入力部

109 表示部

110 無線部

111 アンテナ

161 フラグ記憶部

162 更新制御部

163 更新データ読取部

164 更新データ解析部

165 書込位置決定部

166 更新データ書込部

167 更新確認部

171 検出制御部

172 改竄検出呼出部

173 改竄検出処理部

174 ファイル読込部

175 マスタ鍵記憶部

176 マスタ鍵

201 記憶部

202 データ取得部

203 ハッシュリスト生成部

204 ハッシュリスト書込部

205 更新要求処理部

206 入力部

207 送受信部

210 改竄検出鍵記憶部

211 データ受取部

212 ハッシュリスト生成処理部

213 暗号化処理部

214 更新データリスト生成部

215 改竄検出鍵

301 鍵取得部

302 改竄検出鍵生成部

303 改竄検出鍵配布部

304 出力部

発明を実施するための最良の形態

[0039] 1. 第1の実施の形態

以下、本発明における第1の実施の形態について、図面を参照しながら説明する。

1. 1 プログラム更新システム1の概要

図1は、第1の実施の形態におけるプログラム更新システム1の全体構成を示す図である。

[0040] プログラム更新システム1は、携帯電話機10、更新サーバ装置20、及び鍵更新装置30から構成されている。

鍵更新装置30は、更新サーバ装置20や携帯電話機10で用いられる改竄検出鍵を更新する。改竄検出鍵が不正に流出したときは、新しい改竄検出鍵の発行を行う。鍵更新装置30は、改竄検出鍵を生成する機関により厳重に管理されている。改竄検出鍵は、マスタ鍵と部分鍵とから生成される。マスタ鍵は、一度生成されると変更されない鍵であり、部分鍵は、改竄検出鍵の更新を行う際に、更新される鍵である。

[0041] 携帯電話機10は、更新サーバ装置20に、アプリケーションソフトウェア(以下、APという。)に係るファイルの更新を要求する更新要求情報を送信し、更新に係るデータである更新データリストを受信する。携帯電話機10は、受信した更新データリストに基づいて、ファイルの更新を行う。ここで、APとは、具体的には音楽録音・再生ソフトウェアや動画録画・再生ソフトウェアのようなアプリケーションである。また、APに係るファイルとは、APそのものや、APから呼び出されるエンコーダ、デコーダ、ドライバ、APが動作する環境を提供するJava(登録商標)VMのような仮想実行環境などであり、1つ以上のデータからなる。

[0042] また、携帯電話機10は、アプリケーションソフトウェア更新時、及び起動時にAPに係るファイルが改竄されているか否かの確認を行う。ここで、改竄とは、不正にファイルを書き換えることをいう。

更新サーバ装置20は、更新データリストを保持しており、携帯電話機10からの更新要求情報を受け付けると、更新要求の対象であるファイルに対応する更新データリストを携帯電話機10に送信する。

[0043] 携帯電話機10と更新サーバ装置20とは、携帯網40及びインターネット50を介して、通信を行う。

1．2 携帯電話機10の構成

携帯電話機10は、図2にて示すように、記憶部101、制御部102、更新処理部103、更新ファイル受取部104、改竄検出実行部105、マイク106、スピーカ107、入力

部108、表示部109、無線部110、及びアンテナ111から構成されている。

[0044] (1)記憶部101

記憶部101は、図2に示すように、検出対象情報群120、120a、・・・、102mを記憶している。なお、検出対象情報群120、120a、・・・、102mは全て同じ構成であるので、ここでは、検出対象情報群120の構成について説明する。

検出対象情報群120は、図2に示すように、APファイル群121、ハッシュリスト122、及び部分鍵を記憶している。

[0045] (APファイル群121)

APファイル群121は、第1ファイル125、・・・、第nファイル126を有している。第1ファイル125、・・・、第nファイル126は、改竄検出の対象となるファイルであり、具体的には、上述したように、APそのものや、APから呼び出されるエンコーダ、デコーダ、ドライバ、APが動作する環境を提供するJava(登録商標)VMのような仮想実行環境などである。ここで、nは1以上の整数である。つまり、APファイル群121には、1つ以上のファイルが格納されている。

[0046] なお、以降では、第1ファイル125、・・・、第nファイル126それぞれのファイル名を「file__1」、・・・、「file__n」とする。なお、各ファイルは、局所的な更新が可能となるように、携帯電話機の製造時において固定されたアドレスに記録されている。

(ハッシュリスト122)

ハッシュリスト122は、第1ファイル125、・・・、第nファイル126の改竄検出用のハッシュ値をリストとして保持している。ハッシュリスト122は局所的な更新が可能となるように、携帯電話機の製造時において固定されたアドレスに記録されている。

[0047] ここで、ハッシュリスト122について説明する。

図3は、ハッシュリスト122のデータ構造の一例を示す図である。

ハッシュリスト122は、暗号化されていないヘッダ部130と暗号化されているデータ部131とから構成されている。ここで、暗号化に用いられるアルゴリズムは、例えば、XORのような論理演算もしくはDES(Data Encryption Standard)、AES(Advanced Encryption Standard)といった暗号アルゴリズムである。暗号アルゴリズムDES、AESは、公知であるため説明は省略する。

[0048] ヘッダ部130は、ハッシュリストファイルサイズ132とデータ部ハッシュ値133とから構成されている。ハッシュリストファイルサイズ132は、ヘッダ部130とデータ部131を合わせたハッシュリスト122全体のデータサイズを示す。データ部ハッシュ値133は、データ部131に対してハッシュ計算アルゴリズムを適用して算出されたハッシュ値を示す。ここで、ハッシュ計算アルゴリズムは、SHA－1やMD5などの一方向性関数に鍵値をからめるHMAC(Keyed－Hashing for Message Authentication)アルゴリズムであるとする。以降において、ハッシュ値を算出するハッシュ計算アルゴリズムは、HMACアルゴリズムであるとする。

[0049] データ部131は、1つ以上のハッシュ情報から構成されている。ここでは、データ部131は、ハッシュ情報134、・・・、ハッシュ情報135から構成されているものとする。ハッシュ情報は、改竄検出対象となるファイルに対して、少なくとも1つ存在する。

ハッシュ情報134は、1つのファイル情報140と複数のMAC情報141とから構成されている。

[0050] ファイル情報140は、改竄検出対象となるファイルを分割して生成したブロックの数を示すブロック数142と、改竄検出対象となるファイルを示すファイル名とから構成されている。ここで、ファイル名は、改竄検出対象となるファイルのファイルシステム上の絶対パスや相対パスなど場所を特定できるパスを含めた形式で示されている。

MAC情報141は、1個以上のエントリで構成されている。ここで、エントリの数は、ブロック数142にて示される値＋1である。

[0051] エントリ144は、ファイル名143にて示されるファイルの分割されたブロックについての先頭アドレスからのオフセットと、ブロックのサイズと、ブロックに対してハッシュ計算アルゴリズムを適用して算出されたハッシュ値とから構成されている。なお、(n－1)番目までのエントリの構成については、同様であるため説明は省略する。ハッシュリスト122に格納されているハッシュ値は、改竄検出時において、改竄がされているか否かを判断するための基準となる基準値である。

[0052] MAC情報141の最後に位置するエントリ145は、更新用に予約された空エントリであり、オフセット、サイズ、及びハッシュ値が記述される代わりに、“Reserved”がそれぞれ記述されている。なお、MAC情報141の最後に位置するエントリを最終エントリと

もいう。

データ部131の最後の位置するハッシュ情報における最終エントリには、ハッシュリスト122における最後のエントリであることを示す情報“end of entry”が埋められている。ここでは、ハッシュ情報135が、データ部131の最後に位置するハッシュ情報であるので、その最終エントリ146には、“end of entry”が埋められている。なお、ハッシュ情報135の他の構成要素は、ハッシュ情報134において最終エントリ145を除く他の構成要素と同様であるため説明は省略する。

[0053] また、上述したように、データ部131は、暗号化されている。暗号化は、ファイル情報140やMAC情報141の1エントリの単位で行われる。このため、ハッシュリスト122の更新は、ファイル情報140やMAC情報141の1エントリの単位で可能となる。

なお、ここでは、ハッシュリスト122は、ハッシュリスト122が属する検出対象情報群120に含まれるAPを識別するAP識別情報と対応付けがされているものとする。

[0054] (部分鍵123)

部分鍵123は、改竄検出を行われる実行するときにマスタ鍵とともに改竄検出鍵の算出に用いられる。部分鍵123は更新が可能となるように、携帯電話機の製造時において固定されたアドレスに記録されている。

なお、ここでは、ハッシュリスト122と同様に、部分鍵123は、部分鍵123が属する検出対象情報群120に含まれるAPを識別するAP識別情報と対応付けがされているものとする。

[0055] (2)制御部102

制御部102は、携帯電話機10の全体の制御を行う。

制御部102は、無線部110から通話に係る信号(音声信号)を受け取ると、受け取った信号をスピーカ107へ出力するための信号処理を行う。

制御部102は、マイク106から通話に係る信号(音声信号)を無線部110へ出力するための信号処理を行う。

[0056] 制御部102は、入力部108からAPに係るファイルの更新の更新指示を受け取ると、ファイルの更新処理の開始を示す更新開始命令を更新処理部103へ出力する。ここで、更新指示、及び更新開始命令には、更新対象となるAPを示すAP識別情報が

含まれる。

制御部102は、更新処理部103からファイルの更新完了の通知を受け取ると、表示部109を介して、更新完了のメッセージを表示する。

[0057] 制御部102は、更新処理部103からファイルの更新失敗の通知を受け取ると、表示部109を介して、更新失敗のメッセージを表示する。また、制御部102は、入力部108から再更新の指示を受け取ると、ファイルの再更新の開始を示す再更新開始命令を更新処理部103へ出力する。制御部102は、入力部108から再更新を行わない指示を受け取ると、ファイルの更新処理の終了を示す更新終了命令を更新処理部103へ出力する。

[0058] 制御部102は、入力部108からAPの起動指示を受け取ると、起動の対象となるAPの起動を行う。このとき、起動されたAPは、自APが改竄検出対象である場合には、検出開始命令と、自APを識別するAP識別情報とを、制御部102により改竄検出実行部105へ出力する。なお、改竄検出実行部105では、検出開始命令を制御部102から受け取ることになる。

[0059] 制御部102は、改竄検出実行部105から改竄されていない通知を受け取ると、起動指示のあったAPに係る動作を実行する。

制御部102は、改竄検出実行部105から改竄が検出された通知を受け取ると、起動指示のあったAPの動作を終了する。

(3)更新処理部103

更新処理部103は、更新ファイル受取部104が更新サーバ装置20より受け取った更新データリスト150より更新対象となるファイルやリスト、もしくは鍵などのデータを更新する。

[0060] ここで、更新データリスト150は、図4に示すように、1つ以上の更新情報151、・・・、152から構成されている。更新情報151は、位置情報153、データサイズ154、及び更新データ155から構成されている。位置情報153は、更新するデータの位置を示す情報である。例えば、位置情報153は、ファイル名やファイルの先頭からのオフセット、アドレス情報などで表される。データサイズ154は、更新するデータのサイズを示す。更新データ155は、更新すべき情報であるファイルのうち更新対象となる1以

上のブロック、ハッシュリスト122におけるハッシュリストファイルサイズ132、データ部ハッシュ値133、ファイル情報、MAC情報に含まれるエントリなどが記録されている。ここで、更新データには、1つ以上のデータが含まれており、更新データに含まれるデータとは、ハッシュリストファイルサイズやデータ部ハッシュ値などのような値や、アプリケーションソフトウェアを実行するための命令文などである。

[0061] 例えば、ファイルを複数個のブロックに分割し、2～4番目のブロックを更新する場合には、位置情報には2番目のブロックの位置を示すオフセットが格納され、データサイズには2～4番目のブロックそれぞれのサイズを合計した合計サイズが格納され、更新データには、更新後の2～4番目のブロックが格納される。また、ハッシュリストも更新する必要があるため、この場合には、2番目のブロックのハッシュ値を含むエントリの位置を示すオフセットが位置情報に格納され、2～4番目のブロックのハッシュ値を含むエントリそれぞれのサイズの合計値がデータサイズに格納され、更新後の2～4番目のブロックに対応するエントリそれぞれが、更新データに格納される。

[0062] 更新処理部103は、更新データリスト150の内容に基づいて、ファイルやハッシュリスト122内のハッシュリストファイルサイズ132、データ部ハッシュ値133、ファイル情報、MAC情報に含まれるエントリ、部分鍵123の更新を行う。

更新処理部103は、図5に示すように、フラグ記憶部161、更新制御部162、更新データ読取部163、更新データ解析部164、書込位置決定部165、更新データ書込部166、及び更新確認部167から構成されている。

[0063] 更新処理部103は、悪意のあるユーザによる解析に対する耐性をもつよう耐タンパー技術で保護されている。耐タンパー技術は、公知であるため説明は省略する。

（フラグ記憶部161）

フラグ記憶部161は、APに係るファイルの更新を行っているか否かを示すフラグを記憶している。ここでは、フラグの値「0」である場合には、更新処理部103が、更新を行っていない旨を示し、値「1」である場合には、更新処理部103が、更新を行っている旨を示す。なお、フラグ記憶部161は、具体的には、不揮発性のメモリである。つまり、携帯電話機10の電源を切っても、フラグ記憶部161の記憶内容は保持される。

[0064] （更新制御部162）

更新制御部162は、制御部102から更新開始命令を受け取ると、他の命令による処理が割り込まないように、制御部102に対して割り込み禁止を設定する。

更新制御部162は、フラグ記憶部161に記憶されているフラグの値を「1」に設定する。

[0065] 更新制御部162は、受け取った更新開始命令に含まれるAP識別情報を更新データ読取部163へ出力する。

更新制御部162は、更新データ読取部163から全ての更新データの書き込みが完了した旨の書込完了命令を受け取ると、改竄検出の処理を開始する旨の検出開始命令と、AP識別情報とを改竄検出実行部105へ出力する。

[0066] 更新制御部162は、改竄検出実行部105から改竄されていない通知を受け取ると、更新完了の通知を制御部102へ出力する。更新制御部162は、制御部102に対する割り込み禁止を解除し、フラグ記憶部161に記憶されているフラグの値を「0」に設定する。

更新制御部162は、改竄検出実行部105から改竄が検出された通知を受け取ると、更新失敗の通知を制御部102へ出力する。更新制御部162は、制御部102から再更新開始命令を受け取ると、再度、AP識別情報を更新データ読取部163へ出力する。

[0067] 更新制御部162は、制御部102から更新終了命令を受け取ると、更新制御部162は、制御部102に対する割り込み禁止を解除し、フラグ記憶部161に記憶されているフラグの値を「0」に設定する。

携帯電話機10に電源が投入され、電源の供給が開始されると、更新制御部162は、フラグ記憶部161に記憶されているフラグの値をチェックする。値が「1」である場合には、更新処理中の状態であると判断し、制御部102に対して割り込み禁止を設定する。更新制御部162は、更新処理の再開始を示す再開始命令を更新データ読取部163へ出力する。更新制御部162は、更新データ読取部163から更新処理の再開始が不要である旨を示す再開始不要命令を受け取ると、制御部102に対する割り込み禁止を解除し、フラグ記憶部161に記憶されているフラグの値を「0」に設定する。

[0068] （更新データ読取部163）

更新データ読取部163は、更新制御部162からAP識別情報を受け取ると、受け取ったAP識別情報を更新ファイル受取部104へ出力する。

更新データ読取部163は、更新ファイル受取部104から更新サーバ装置20から更新データリスト150の受信が完了した旨の受信完了命令を受け取ると、受信した更新データリスト150から未読の更新情報を1つ読み出す。

[0069] 更新データ読取部163は、更新確認部167から更新データの書き込みが正常に終了した旨の正常終了命令を受け取ると、受信した更新データリスト150に未読の更新情報が存在するか否かを判断する。存在すると判断する場合には、更新データ読取部163は、未読の更新情報を取得する。存在しないと判断する場合には、更新データ読取部163は、書込完了命令を、更新制御部162及び更新ファイル受取部104へ出力する。更新データ読取部163は、更新確認部167から更新データの書き込みが失敗した旨の異常終了命令を受け取ると、前回読み出した更新情報を再度読み出す。

[0070] 更新データ読取部163は、更新制御部162から再開始命令を受け取ると、受け取った再開始命令を更新ファイル受取部104へ出力する。その後、更新データ読取部163は、更新ファイル受取部104から受信完了命令を受け取ると、上記と同様の動作を行う。

更新データ読取部163は、再開始不要命令を受け取ると、受け取った再開始不要命令を更新制御部162へ出力する。

[0071] （更新データ解析部164）

更新データ解析部164は、更新データ読取部163にて読み出された更新情報を、位置情報、データサイズ、及び更新データに分割する。これにより、更新データ解析部164は、更新情報から位置情報、データサイズ、及び更新データを取得することができる。

（書込位置決定部165）

書込位置決定部165は、更新データ解析部164にて取得された位置情報に基づいて、記憶部101における更新データの書込位置を決定する。

[0072] （更新データ書込部166）

更新データ書込部166は、書込位置決定部165にて決定された書込位置を書込開始の先頭位置として、更新データ解析部164にて取得された更新データを書き込む。

（更新確認部167）

更新確認部167は、更新データ書込部166による書き込みが正常に終了したか否かを確認する。

[0073] 正常に終了したと判定する場合には、正常終了命令を更新データ読取部163へ出力し、正常に終了していないと判断する場合には、異常終了命令を更新データ読取部163へ出力する。

（4）更新ファイル受取部104

更新ファイル受取部104は、携帯電話機10を識別する端末識別子を予め記憶している。

[0074] 更新ファイル受取部104は、更新処理部103から受け取ったAP識別情報を記憶するAP識別情報記憶領域、及び更新サーバ装置20から受信した更新データリスト150を記憶するリスト記憶領域を有している。ここで、AP識別情報記憶領域、及びリスト記憶領域は不揮発性メモリである。

更新ファイル受取部104は、更新処理部103の更新データ読取部163からAP識別情報を受け取ると、受け取ったAP識別情報と、端末識別子と、更新要求情報とを、無線部110を介して、更新サーバ装置20へ送信し、受け取ったAP識別情報をAP識別情報記憶領域へ格納する。

[0075] 更新ファイル受取部104は、更新サーバ装置20から無線部110を介して、更新データリスト150を受け取ると、受け取った更新データリスト150をリスト記憶領域へ格納する。さらに、更新ファイル受取部104は、受け取った更新データリスト150の格納が完了すると、AP識別情報記憶領域にて格納されているAP識別情報を消去し、受信完了命令を更新データ読取部163へ出力する。

[0076] 更新ファイル受取部104は、更新データ読取部163から書込完了命令を受け取ると、リスト格納領域に格納されている更新データリスト150を消去する。

更新ファイル受取部104は、更新データ読取部163から再開始命令を受け取ると、AP識別情報記憶領域に格納されているAP識別情報が存在するか否かを判断する。存在すると判断する場合には、更新ファイル受取部104は、格納しているAP識別情報と、端末識別子とを、無線部110を介して、更新サーバ装置20へ送信し、上記と同様の動作を行う。

[0077] AP識別情報記憶領域にAP識別情報が存在しないと判断する場合には、更新ファイル受取部104は、リスト記憶領域に更新データリスト150が格納されているか否かを判断する。格納されていると判断する場合には、受信完了命令を更新データ読取部163へ出力する。格納されていないと判断する場合には、再開始不要命令を更新データ読取部163へ出力する。

[0078] (5)改竄検出実行部105

改竄検出実行部105は、図6に示すように、検出制御部171、改竄検出呼出部172、改竄検出処理部173、及びファイル読込部174から構成されている。

改竄検出実行部105は、悪意のあるユーザによる解析に対する耐性をもつよう耐タンパー技術で保護されている。耐タンパー技術は、公知であるため説明は省略する。

[0079] (検出制御部171)

検出制御部171は、制御部102若しくは更新処理部103の更新制御部162のいずれかから検出開始命令とAP識別情報とを受け取ると、受け取った検出開始命令とAP識別情報とを改竄検出呼出部172へ出力する。

検出制御部171は、改竄検出処理部173から改竄されていない通知若しくは改竄が検出された通知のうちいずれかを受け取る。

[0080] 検出制御部171は、受け取った通知を、検出開始命令及びAP識別情報の出力元である制御部102若しくは更新処理部103の更新制御部162のいずれかへ出力する。具体的には、検出開始命令を制御部102から受け取った場合には、検出制御部171は、改竄検出処理部173から受け取った通知を制御部102へ出力する。また、検出開始命令を更新制御部162から受け取った場合には、検出制御部171は、改竄検出処理部173から受け取った通知を更新制御部162へ出力する。

[0081] （改竄検出呼出部172）

改竄検出呼出部172は、検出制御部171から検出開始命令とAP識別情報とを受け取ると、記憶部101から受け取ったAP識別情報に対応するハッシュリスト122を読み出す。

改竄検出呼出部172は、読み出したハッシュリスト122と、受け取った検出開始命令及びAP識別情報とを、改竄検出処理部173へ出力する。

[0082] （改竄検出処理部173）

改竄検出処理部173は、図6に示すように、マスタ鍵記憶部175を有している。マスタ鍵記憶部175は、マスタ鍵176を記憶している。

改竄検出処理部173は、改竄検出呼出部172からハッシュリスト122と、検出開始命令及びAP識別情報とを受け取ると、改竄検出の処理を開始する。

[0083] 改竄検出処理部173は、受け取ったAP識別情報に対応する部分鍵123を、記憶部101から読み出す。

改竄検出処理部173は、読み出した部分鍵123と、マスタ鍵176と、特定のアルゴリズムとを用いて改竄検出鍵を算出する。ここで、特定のアルゴリズムは、例えば、XOR（排他的論理和）のような論理演算、若しくはDES、AESといった暗号アルゴリズムであるとする。

[0084] 改竄検出処理部173は、算出した改竄検出鍵とハッシュ計算アルゴリズムとを用いて、受け取ったハッシュリスト122のデータ部131に対するハッシュ値を算出する。改竄検出処理部173は、算出したハッシュ値と、ハッシュリスト122のヘッダ部130に含まれるデータ部ハッシュ値133とが一致するか否かを判断する。

一致しないと判断する場合には、改竄検出処理部173は、改竄が検出された通知を検出制御部171へ出力する。

[0085] 一致すると判断する場合には、改竄検出処理部173は、改竄検出鍵を用いて、データ部131を復号する。なお、復号には、データ部131を暗号化したアルゴリズムに対応する復号アルゴリズムが用いられる。

改竄検出処理部173は、復号したデータ部から、未読のハッシュ情報を読み出す。改竄検出処理部173は、読み出したハッシュ情報に含まれるファイル情報をファイル

読込部174へ出力し、その後、ファイル読込部174からファイルの読み込みが完了した旨を示すファイル読込完了命令を受け取る。

[0086] 改竄検出処理部173は、読み出したハッシュ情報から未読のエントリを取得し、取得したエントリが最終エントリであるか否かを判断する。

最終エントリでないと判断する場合には、改竄検出処理部173は、取得したエントリに含まれるオフセット及びサイズとを読み出し、読み出したオフセット及びサイズに基づいて、ファイル読込部174にて読み込まれたファイルから検出対象のブロックを取得する。改竄検出処理部173は、算出した改竄検出鍵とハッシュ計算アルゴリズムとを用いて、取得したブロックに対する検出用ハッシュ値を算出する。改竄検出処理部173は、算出した検出用ハッシュ値と取得したエントリに含まれるハッシュ値とが一致するか否かを判断する。一致すると判断する場合には、改竄検出処理部173は、読み出したハッシュ情報から未読のエントリを取得し、上記動作を行う。一致しないと判断する場合には、改竄検出処理部173は、改竄が検出された通知を検出制御部171へ出力する。

[0087] 取得したエントリが最終エントリであると判断する場合には、改竄検出処理部173は、未読のハッシュ情報が存在するか否かを判断する。存在すると判断する場合には、改竄検出処理部173は、未読のハッシュ情報を読み出し、上記の動作を行う。存在しないと判断する場合には、改竄検出処理部173は、改竄されていない通知を検出制御部171へ出力する。

[0088] (ファイル読込部174)

ファイル読込部174は、読み込んだファイルを一時的に記憶するファイル記憶領域を有している。

ファイル読込部174は、改竄検出処理部173からファイル情報を受け取ると、受け取ったファイル情報に含まれるファイル名に基づいて、改竄検出対象のファイルを記憶部101から読み出す。

[0089] ファイル読込部174は、読み出したファイルをファイル記憶領域に格納し、ファイル読込完了命令を、改竄検出処理部173へ出力する。

(6)マイク106

マイク106は、使用者の音声を受け付け、受け付けた音声を音声信号に変換し、変換した音声信号を制御部102へ出力する。

[0090] (7)スピーカ107

スピーカ107は、制御部102にて処理された音声信号を音声として出力する。

(8)入力部108

入力部108は、使用者の操作により、更新指示を受け付けると、受け付けた更新指示を制御部102へ出力する。

[0091] 入力部108は、改竄検出対象のファイルの更新が失敗した場合に、使用者の操作により、再更新を行う指示を受け付けると、受け付けた再更新を行う指示を制御部102へ出力する。また、入力部108は、改竄検出対象のファイルの更新が失敗した場合に、使用者の操作により、再更新を行わない指示を受け付けると、受け付けた再更新を行わない指示を制御部102へ出力する。

[0092] 入力部108は、使用者の操作により、APの起動指示を受け付けると、受け付けた起動指示を制御部102へ出力する。

(9)表示部109

表示部109は、制御部102から更新完了のメッセージを受け取ると、受け取ったメッセージを表示する。

[0093] 表示部109は、制御部102から更新失敗のメッセージを受け取ると、受け取ったメッセージを表示する。

(10)無線部110

無線部110は、アンテナ111を備えており、無線信号の送受信を行う。

1．3 更新サーバ装置20の構成

更新サーバ装置20は、図7に示すように、記憶部201、データ取得部202、ハッシュリスト生成部203、ハッシュリスト書込部204、更新要求処理部205、入力部206、及び送受信部207から構成されている。

[0094] (1)記憶部201

記憶部201は、携帯電話機10にて記憶されている検出対象情報群に対する更新データリストを1以上記憶するための領域と、ハッシュリストを記憶するための領域とを

有している。

ここでは、検出対象情報群120に対する更新データリストを1つ以上記憶しているものとする。また、記憶されている更新データリストのそれぞれは、更新対象のファイルを含むAPのAP識別情報と対応付けられ、さらに、版数の管理がされている。また、携帯電話機10の端末識別子と、携帯電話機10に送信した更新データリストの版数とが対応付けられて管理されているものとする。また、ハッシュリストは、対応するAPのAP識別情報と対応付けがされている。

[0095] (2)データ取得部202

データ取得部202は、入力部206から初期設定指示を受け取ると、さらに、改竄検出対象となる1つ以上のファイル、及びターゲットパスリストを取得する。このとき、取得元は、例えば、外部装置である。データ取得部202は、受け取った初期設定指示と、取得した1つ以上のファイル、及びターゲットパスリストとをハッシュリスト生成部203へ出力する。ここで、ターゲットパスリストとは、改竄検出対象となる1つ以上のファイルそれぞれに対してのファイルシステム上にて格納されている格納場所を示す絶対パスや相対パスなどからなるパス名が格納されているリストである。なお、初期設定指示には、生成されるハッシュリストと対応するAPのAP識別情報が含まれる。

[0096] データ取得部202は、入力部206から検出対象のファイルの更新があった旨を示す第1更新指示を受け取ると、さらに、更新対象となる1つ以上のファイルそれぞれに対する更新ファイル、及び更新対象となる1つ以上のファイルのターゲットパスリストを取得する。なお、第1更新指示には、更新の対象となるAPのAP識別情報が含まれているものとする。このとき、取得元は、例えば、外部装置である。データ取得部202は、記憶部201から第1更新指示に含まれるAP識別情報に対応するハッシュリストを取得する。データ取得部202は、受け取った第1更新指示と、取得した1つ以上の更新ファイル、ターゲットパスリスト、及びハッシュリストとをハッシュリスト生成部203へ出力する。ここで、更新ファイルとは、元のファイルに存在する不具合が解消された最新ファイルである。

[0097] データ取得部202は、鍵更新装置30から部分鍵の更新があった旨を示す第2更新指示と、更新後の部分鍵とを受け取ると、さらに、更新された部分鍵を用いた改竄検

出の対象となる1つ以上のファイル、及びターゲットパスリストを取得する。なお、第2更新指示には、更新された部分鍵に対応するAPのAP識別情報が含まれているものとする。このとき、取得元は、例えば、外部装置である。データ取得部202は、記憶部201から第2更新指示に含まれるAP識別情報に対応するハッシュリストを取得する。データ取得部202は、受け取った第2更新指示及び部分鍵と、1つ以上のファイル、ターゲットパスリスト、及びハッシュリストとをハッシュリスト生成部203へ出力する。

[0098] (3)ハッシュリスト生成部203

ハッシュリスト生成部203は、図8に示すように、改竄検出鍵記憶部210、データ受取部211、ハッシュリスト生成処理部212、暗号化処理部213、及び更新データリスト生成部214から構成されている。

ここで、ハッシュリスト生成部203は、1つの装置(ハッシュリスト生成装置)としてもよい。

[0099] (改竄検出鍵記憶部210)

改竄検出鍵記憶部210は、改竄検出鍵215を記憶している。

(データ受取部211)

データ受取部211は、データ取得部202より初期設定指示、第1更新指示、及び第2更新指示の何れかを受け取る。

[0100] データ受取部211は、初期設定指示を受け取ると、さらに、改竄検出対象となる1つ以上のファイル、及びターゲットパスリストを受け取り、受け取った初期設定指示、1つ以上のファイル、及びターゲットパスリストをハッシュリスト生成処理部212に出力する。

データ受取部211は、第1更新指示を受け取ると、さらに、更新対象となる1つ以上のファイルそれぞれに対する更新ファイル、更新対象となる1つ以上のファイルのターゲットパスリスト、及びハッシュリストを受け取り、受け取った第1更新指示、1つ以上の更新ファイル、ターゲットパスリスト、及びハッシュリストをハッシュリスト生成処理部212に出力する。

[0101] データ受取部211は、第2更新指示を受け取ると、さらに、部分鍵、更新された部分鍵を用いた改竄検出の対象となる1つ以上のファイル、ターゲットパスリスト、及びハッ

シュリストを受け取り、受け取った第2更新指示、部分鍵、1つ以上のファイル、ターゲットパスリスト、及びハッシュリストをハッシュリスト生成処理部212に出力する。

（ハッシュリスト生成処理部212）

ハッシュリスト生成処理部212は、データ受取部211より初期設定指示、第1更新指示、及び第2更新指示の何れかを受け取る。

[0102] ＜初期設定指示を受け取った場合＞

ハッシュリスト生成処理部212は、初期設定指示を受け取ると、さらに、改竄検出対象となる1つ以上のファイル、及びターゲットパスリストを受け取る。

ハッシュリスト生成処理部212は、受け取った1つ以上のファイルのうち1つのファイルを所定のサイズからなる1以上のブロックに分割する。ハッシュリスト生成処理部212は、分割されたファイルが携帯電話機10において格納されている位置を示すパス名をターゲットパスリストから読み取り、分割したブロックの数と、読み取ったパス名とからなるファイル情報を生成する。また、ハッシュリスト生成処理部212は、改竄検出鍵記憶部210から改竄検出鍵215を読み出す。ハッシュリスト生成処理部212は、所定のサイズに分割したブロック単位で、読み出した改竄検出鍵215とハッシュ計算アルゴリズムとを用いてハッシュ値を算出し、各ブロックに対して、ブロックの先頭位置を示すオフセットと、ブロックのサイズと、算出したハッシュ値とからなるエントリを生成し、生成した各エントリを含むMAC情報を生成する。ハッシュリスト生成処理部212は、生成したファイル情報とMAC情報とからなるハッシュ情報を生成する。なお、このとき、ハッシュ情報は、未だ暗号化されていない。この動作を、受け取った全てのファイルに対して行う。

[0103] ハッシュリスト生成処理部212は、受け取った1つ以上のファイルそれぞれに対するハッシュ情報を生成すると、生成した全てのハッシュ情報からなるデータ部を生成する。このとき、データ部は暗号化されていない。以下、暗号化されたデータ部を区別するため、暗号化されていないデータ部を非暗号化データ部という。

ハッシュリスト生成処理部212は、生成した非暗号化データ部を暗号化処理部213へ出力する。

[0104] ハッシュリスト生成処理部212は、暗号化処理部213から暗号化されたデータ部を

受け取ると、暗号化されたデータ部に対して、ハッシュ計算アルゴリズムを適用してハッシュ値を算出し、ハッシュリストのデータ部ハッシュ値に記録する。ハッシュリスト生成処理部212は、ハッシュリストのサイズを算出し、算出結果をハッシュリストファイルサイズに記録する。これにより、ハッシュリスト生成処理部は、ハッシュリストのヘッダ部を生成することができる。

[0105] ハッシュリスト生成処理部212は、生成したヘッダ部と、暗号化処理部213から受け取った暗号化されたデータ部とからなるハッシュリストを生成する。

ハッシュリスト生成処理部212は、生成したハッシュリストを記憶部に格納するとともに、ハッシュリスト書込部204へ出力する。このとき、生成したハッシュリストと、初期設定指示に含まれるAP識別情報とが対応付けされる。

[0106] ＜第1更新指示を受け取った場合＞

ハッシュリスト生成処理部212は、データ受取部211から第1更新指示を受け取ると、さらに、更新対象となる1つ以上のファイルそれぞれに対する更新ファイル、更新対象となる1つ以上のファイルのターゲットパスリスト、及びハッシュリストを受け取る。以下において、データ受取部211から受け取ったハッシュリストを旧ハッシュリストという。

[0107] ハッシュリスト生成処理部212は、受け取った1つ以上の更新ファイルのうち1つの更新ファイルを所定のサイズからなる1以上のブロックに分割する。ハッシュリスト生成処理部212は、分割された更新ファイルが携帯電話機10において格納されている位置を示すパス名をターゲットパスリストから読み取り、分割したブロックの数と、読み取ったパス名とからなるファイル情報を生成する。また、ハッシュリスト生成処理部212は、改竄検出鍵記憶部210から改竄検出鍵215を読み出す。ハッシュリスト生成処理部212は、所定のサイズに分割したブロック単位で、読み出した改竄検出鍵215とハッシュ計算アルゴリズムとを用いてハッシュ値を算出し、各ブロックに対して、ブロックの先頭位置を示すオフセットと、ブロックのサイズと、算出したハッシュ値とからなるエントリを生成し、生成した各エントリを含むMAC情報を生成する。ハッシュリスト生成処理部212は、生成したファイル情報とMAC情報とからなるハッシュ情報を生成する。なお、このとき、ハッシュ情報は、未だ暗号化されていない。この動作を、受け

取った全ての更新ファイルに対して行う。

[0108] ハッシュリスト生成処理部212は、受け取った1つ以上の更新ファイルそれぞれに対するハッシュ情報を生成すると、生成した全てのハッシュ情報からなる非暗号化データ部を生成する。

ハッシュリスト生成処理部212は、生成した非暗号化データ部を暗号化処理部213へ出力する。

[0109] ハッシュリスト生成処理部212は、暗号化処理部213から暗号化されたデータ部を受け取ると、暗号化されたデータ部に対して、ハッシュ計算アルゴリズムを適用してハッシュ値を算出し、ハッシュリストのデータ部ハッシュ値に記録する。ハッシュリスト生成処理部212は、ハッシュリストのサイズを算出し、算出結果をハッシュリストファイルサイズに記録する。これにより、ハッシュリスト生成処理部は、ハッシュリストのヘッダ部を生成することができる。

[0110] ハッシュリスト生成処理部212は、生成したヘッダ部と、暗号化処理部213から受け取った暗号化されたデータ部とからなる新ハッシュリストを生成する。

ハッシュリスト生成処理部212は、第1更新指示、生成した新ハッシュリストと、データ受取部211から受け取った旧ハッシュリスト及び1以上の更新ファイルとを更新データリスト生成部214へ出力する。

[0111] ＜第2更新指示を受け取った場合＞

ハッシュリスト生成処理部212は、データ受取部211から第2更新指示を受け取ると、さらに、部分鍵、検出対象となる1つ以上のファイル、ターゲットパスリスト、及び旧ハッシュリストを受け取る。

ハッシュリスト生成処理部212は、受け取った1つ以上のファイルのうち1つのファイルを所定のサイズからなる1以上のブロックに分割する。ハッシュリスト生成処理部212は、分割された更新ファイルが携帯電話機10において格納されている位置を示すパス名をターゲットパスリストから読み取り、分割したブロックの数と、読み取ったパス名とからなるファイル情報を生成する。また、ハッシュリスト生成処理部212は、改竄検出鍵記憶部210から改竄検出鍵215を読み出す。ハッシュリスト生成処理部212は、所定のサイズに分割したブロック単位で、読み出した改竄検出鍵215とハッシュ

計算アルゴリズムとを用いてハッシュ値を算出し、各ブロックに対して、ブロックの先頭位置を示すオフセットと、ブロックのサイズと、算出したハッシュ値とからなるエントリを生成し、生成した各エントリを含むMAC情報を生成する。ハッシュリスト生成処理部212は、生成したファイル情報とMAC情報とからなるハッシュ情報を生成する。なお、このとき、ハッシュ情報は、未だ暗号化されていない。この動作を、受け取った全てのファイルに対して行う。

[0112] ハッシュリスト生成処理部212は、受け取った1つ以上のファイルそれぞれに対するハッシュ情報を生成すると、生成した全てのハッシュ情報からなる非暗号化データ部を生成する。

ハッシュリスト生成処理部212は、生成した非暗号化データ部を暗号化処理部213へ出力する。

[0113] ハッシュリスト生成処理部212は、暗号化処理部213から暗号化されたデータ部を受け取ると、暗号化されたデータ部に対して、ハッシュ計算アルゴリズムを適用してハッシュ値を算出し、ハッシュリストのデータ部ハッシュ値に記録する。ハッシュリスト生成処理部212は、ハッシュリストのサイズを算出し、算出結果をハッシュリストファイルサイズに記録する。これにより、ハッシュリスト生成処理部は、ハッシュリストのヘッダ部を生成することができる。

[0114] ハッシュリスト生成処理部212は、生成したヘッダ部と、暗号化処理部213から受け取った暗号化されたデータ部とからなる新ハッシュリストを生成する。

ハッシュリスト生成処理部212は、第2更新指示と、生成した新ハッシュリストと、データ受取部211から受け取った旧ハッシュリスト及び部分鍵とを更新データリスト生成部214へ出力する。

[0115] (暗号化処理部213)

暗号化処理部213は、ハッシュリスト生成処理部212から非暗号化データ部を受け取ると、改竄検出鍵記憶部210から改竄検出鍵215を読み出す。

暗号化処理部213は、読み出した改竄検出鍵を用いて、受け取った非暗号化データ部を暗号化する。暗号に用いられるアルゴリズムは例えばXORのような論理演算もしくはDES、AESといった暗号アルゴリズムであり、携帯電話機10にて用いられる復

号アルゴリズムに対応するものである。このとき、暗号化はファイル情報やMAC情報の1エントリを単位として行われる。

[0116] 暗号化処理部213は、暗号化されたデータ部をハッシュリスト生成処理部212へ出力する。

(更新データリスト生成部214)

更新データリスト生成部214は、第1更新指示及び第2更新指示のいずれかを受け取る。

[0117] <第1更新指示を受け取った場合>

更新データリスト生成部214は、さらに、ハッシュリスト生成処理部212から新ハッシュリストと、旧ハッシュリストと、1つ以上の更新ファイルとを受け取る。

更新データリスト生成部214は、受け取った旧ハッシュリスト、新ハッシュリストを比較し、情報の異なる箇所を新ハッシュリストから抽出する。ここで、抽出される情報は、データ部におけるエントリや、ヘッダ部におけるデータ部ハッシュ値である。

[0118] 更新データリスト生成部214は、抽出された情報と、1つ以上の更新ファイルとを用いて更新データリストを生成する。このとき、更新データリスト生成部214は、抽出された情報から更新ファイルの更新箇所が特定できる。なぜなら、ファイルを分割する際には、各ブロックは、所定のサイズとなるように分割されているので、変更が生じないブロックのハッシュ値は、以前のハッシュと同じとなる。変更が生じているブロックのハッシュ値は以前のハッシュ値と異なっているので、変更された箇所を含むブロックに対するエントリは、旧ハッシュリストと新ハッシュリストとの比較により抽出される。上述したように、ブロックは、所定のサイズとなるように分割されているので、抽出されたエントリから更新ファイルにおける更新箇所を特定することができる。更新データリスト生成部214は、特定した更新箇所を更新データとし、更新データ(つまり更新箇所を含むブロック)の位置情報及びブロックのサイズを取得する。なお、更新箇所を含むブロックが連続している場合には、1つの更新データとして結合してもよい。このときの位置情報は、連続するブロックのうち先頭に位置するブロックの位置情報となり、サイズは、連続するブロックの個数から算出することができる。

[0119] 更新データリスト生成部214は、更新データ、位置情報及びブロックのサイズからな

る更新情報を1個以上生成し、さらに、生成した1個以上の更新情報からなる更新データリストを生成する。

更新データリスト生成部214は、新ハッシュリストと、生成した更新データリストを記憶部201へ格納する。このとき、生成した更新データリストと、第1更新指示に含まれるAP識別情報とが対応付けされる。なお、記憶部201に記憶されている旧ハッシュリストは消去される。

[0120] ＜第2更新指示を受け取った場合＞

更新データリスト生成部214は、さらに、ハッシュリスト生成処理部212から新ハッシュリストと、旧ハッシュリストと、部分鍵とを受け取る。

更新データリスト生成部214は、受け取った旧ハッシュリスト、新ハッシュリストを比較し、情報の異なる箇所を新ハッシュリストから抽出する。ここで、抽出される情報は、データ部におけるエントリや、ヘッダ部におけるデータ部ハッシュ値である。

[0121] 更新データリスト生成部214は、抽出された情報、及び受け取った部分鍵のそれぞれを更新データとする更新データリストを生成する。部分鍵を更新データとする更新情報の生成は、以下のようにして行う。更新データリスト生成部214は、携帯電話機10における部分鍵の記憶位置を示す位置情報と、受け取った部分鍵のデータサイズとを取得する。更新データリスト生成部214は、取得した位置情報と、データサイズと、更新データである部分鍵とからなる更新情報を生成する。

[0122] なお、抽出された情報を更新データとする更新情報の生成は、第1更新指示を受け取った場合にて示す更新情報の生成と同様であるので、ここでの説明は省略する。

更新データリスト生成部214は、生成した1個以上の更新情報からなる更新データリストを生成する。

更新データリスト生成部214は、新ハッシュリストと、生成した更新データリストを記憶部201へ格納する。このとき、生成した更新データリストと、第2更新指示に含まれるAP識別情報とが対応付けされる。なお、記憶部201に記憶されている旧ハッシュリストは消去される。

[0123] (4)ハッシュリスト書込部204

ハッシュリスト書込部204は、携帯電話機の製造時において、製造中（出荷前）の携帯電話機と接続され、携帯電話機の記憶部へのアクセスが可能である。

ハッシュリスト書込部204は、ハッシュリスト生成部203からハッシュリストを受け取ると、受け取ったハッシュリストを、接続された携帯電話機の記憶部へ書き込む。ハッシュリストが書き込まれるアドレスは、上述したように固定されたアドレスである。

[0124] (5)更新要求処理部205

更新要求処理部205は、送受信部207を介して携帯電話機10から、AP識別情報と、端末識別子と、更新要求情報とを受け取ると、受け取ったAP識別情報と、端末識別子とを用いて、携帯電話機10に送信すべき更新データリストの版数を決定する。上述したように、更新サーバ装置20は、更新データリストのそれぞれを、更新対象のファイルを含むAPのAP識別情報と対応付け、及び版数の管理を行っており、また、携帯電話機10の端末識別子と、携帯電話機10に送信した更新データリストの版数とを対応付けて管理しているので、送信すべき更新データリストを決定することができる。

[0125] 更新要求処理部205は、送信すべき更新データリストを記憶部201から取得し、取得した更新データリストを、送受信部207を介して携帯電話機10へ送信する。

(6)入力部206

入力部206は、使用者の操作により、初期設定指示を受け付けると、受け付けた初期設定指示をデータ取得部202へ出力する。

[0126] 入力部206は、使用者の操作により、第1更新指示を受け付けると、受け付けた第1更新指示をデータ取得部202へ出力する。

(7)送受信部207

送受信部207は、携帯網40及びインターネット50を介して携帯電話機10から受信した情報を更新要求処理部205へ出力する。

[0127] 送受信部207は、更新要求処理部205から受け取った情報を、インターネット50及び携帯網40を介して携帯電話機10へ送信する。

1．4 鍵更新装置30の構成

鍵更新装置30は、図9に示すように、鍵取得部301、改竄検出鍵生成部302、改

竄検出鍵配布部303、及び出力部304から構成されている。

[0128] 鍵更新装置30は、改竄検出鍵が悪意のあるユーザによって解析され不正に流出した場合に、更新サーバ装置20に記憶されている改竄検出鍵を更新する。鍵更新装置30は鍵を正式に発行する機関によって厳重に管理されるものとする。

(1)鍵取得部301

鍵取得部301は、外部装置から、マスタ鍵、及び更新された部分鍵と、更新された部分鍵に対応するAPのAP識別情報とを取得する。なお、取得するマスタ鍵は、携帯電話機10にて記憶しているマスタ鍵と同一のものである。

[0129] 鍵取得部301は、受け取ったマスタ鍵及び更新された部分鍵を改竄検出鍵生成部302へ出力する。

鍵取得部301は、改竄検出鍵配布部303から更新サーバ装置20に対して改竄検出鍵の配布が完了した旨を示す配布完了命令を受け取ると、AP識別情報を含む第2更新指示と、更新された部分鍵とを出力部304へ出力する。

[0130] (2)改竄検出鍵生成部302

改竄検出鍵生成部302は、鍵取得部301からマスタ鍵及び更新された部分鍵を受け取ると、受け取ったマスタ鍵と、更新された部分鍵と、特定のアルゴリズムとを用いて改竄検出鍵を算出する。なお、ここで用いる特定のアルゴリズムは、携帯電話機10の改竄検出処理部173にて用いられるアルゴリズムと同一のものである。

[0131] 改竄検出鍵生成部302は、算出した改竄検出鍵を、改竄検出鍵配布部303へ出力する。

(3)改竄検出鍵配布部303

改竄検出鍵配布部303は、更新サーバ装置20と接続され、改竄検出鍵記憶部210にアクセス可能である。

[0132] 改竄検出鍵配布部303は、改竄検出鍵生成部302から改竄検出鍵を受け取ると、受け取った改竄検出鍵を、改竄検出鍵記憶部210に書き込む。このとき、改竄検出鍵記憶部210に記憶されていた以前の改竄検出鍵は消去される。

改竄検出鍵配布部303は、改竄検出鍵の書き込みが完了すると、配布完了命令を鍵取得部301へ出力する。

[0133] (4)出力部304

出力部304は、更新サーバ装置20のデータ取得部202と接続される。

出力部304は、鍵取得部301から第2更新指示と、更新された部分鍵とを受け取ると、受け取った、第2更新指示と、更新された部分鍵とをデータ取得部202へ出力する。

[0134] 1.5 更新サーバ装置20の動作

ここでは、更新サーバ装置20にて、更新データリスト、及びハッシュリストの生成の動作について、図10にて示す流れ図を用いて説明する。

データ受取部211は、データ取得部202より初期設定指示、第1更新指示、及び第2更新指示の何れかを受け取る(ステップS5)。

[0135] データ受取部211は、第1更新指示を受け取ると(ステップS10における「第1更新指示」)、更新対象となる1つ以上のファイルそれぞれに対する更新ファイル、更新対象となる1以上のファイルのターゲットパスリスト、及びハッシュリストを取得する(ステップS15)。

データ受取部211は、受け取った第1更新指示、1つ以上の更新ファイル、ターゲットパスリスト、及びハッシュリスト(以下、旧ハッシュリスト)をハッシュリスト生成処理部212に出力する。ハッシュリスト生成処理部212は、データ受取部211から第1更新指示、1つ以上のファイルそれぞれに対する更新ファイル、更新対象となる1つ以上のファイルのターゲットパスリスト、及び旧ハッシュリストを受け取る。

[0136] ハッシュリスト生成処理部212は、受け取った1以上の更新ファイルのうち1の更新ファイルを所定のサイズからなる1以上のブロックに分割する。ハッシュリスト生成処理部212は、分割された更新ファイルが携帯電話機10において格納されている位置を示すパス名をターゲットパスリストから読み取り、分割したブロックの数と、読み取ったパス名とからなるファイル情報を生成する。また、ハッシュリスト生成処理部212は、所定のサイズに分割したブロック単位でハッシュ計算アルゴリズムを適用してハッシュ値を算出し、各ブロックに対して、ブロックの先頭位置を示すオフセットと、ブロックのサイズと、算出したハッシュ値とからなるエントリを生成し、生成した各エントリを含むMAC情報を生成する。ハッシュリスト生成処理部212は、生成したファイル情報とMAC

情報とからなるハッシュ情報を生成する。なお、このとき、ハッシュ情報は、未だ暗号化されていない。この動作を、受け取った全ての更新ファイルに対して行う。

[0137] ハッシュリスト生成処理部212は、受け取った1以上の更新ファイルそれぞれに対するハッシュ情報を生成すると、生成した全てのハッシュ情報からなる非暗号化データ部を生成する(ステップS20)。

ハッシュリスト生成処理部212は、生成した非暗号化データ部を暗号化処理部213へ出力する。暗号化処理部213は、ハッシュリスト生成処理部212から非暗号化データ部を受け取ると、改竄検出鍵記憶部210から改竄検出鍵215を読み出す。暗号化処理部213は、読み出した改竄検出鍵を用いて、受け取った非暗号化データ部を暗号化する(ステップS25)。このとき、暗号化はファイル情報やMAC情報の1エントリを単位として行われる。

[0138] 暗号化処理部213は、暗号化されたデータ部をハッシュリスト生成処理部212へ出力する。ハッシュリスト生成処理部212は、暗号化処理部213から暗号化されたデータ部を受け取ると、暗号化されたデータ部に対して、ハッシュ計算アルゴリズムを適用してハッシュ値を算出し、ハッシュリストのデータ部ハッシュ値に記録する(ステップS30)。

[0139] ハッシュリスト生成処理部212は、ハッシュリストのサイズを算出し、算出結果をハッシュリストファイルサイズに記録する。これにより、ハッシュリスト生成処理部は、ハッシュリストのヘッダ部を生成することができる。

ハッシュリスト生成処理部212は、生成したヘッダ部と、暗号化処理部213から受け取った暗号化されたデータ部とからなる新ハッシュリストを生成する(ステップS35)。

[0140] ハッシュリスト生成処理部212は、第1更新指示、生成した新ハッシュリストと、データ受取部211から受け取った旧ハッシュリスト及び1以上の更新ファイルとを更新データリスト生成部214へ出力する。更新データリスト生成部214は、第1更新指示、ハッシュリスト生成処理部212から新ハッシュリストと、旧ハッシュリストと、1つ以上の更新ファイルとを受け取る。

[0141] 更新データリスト生成部214は、受け取った旧ハッシュリスト、新ハッシュリストを比較し、情報の異なる箇所を新ハッシュリストから抽出する。ここで、抽出される情報は、

データ部におけるエントリや、ヘッダ部におけるデータ部ハッシュ値である。更新データリスト生成部214は、抽出された情報と、1以上の更新ファイルとを用いて更新データリストを生成する(ステップS40)。

[0142] 更新データリスト生成部214は、新ハッシュリストと、生成した更新データリストを記憶部201へ格納する(ステップS45)。このとき、生成した更新データリストと、第1更新指示に含まれるAP識別情報とが対応付けされる。なお、記憶部201に記憶されている旧ハッシュリストは消去される。

データ受取部211は、第2更新指示を受け取ると(ステップS10における「第2更新指示」)、部分鍵、検出対象となる1つ以上のファイル、ターゲットパスリスト、及びハッシュリストを取得し(ステップS50)、ステップS20からステップS45までの動作を行う。なお、この場合、各構成要素が出力、及び受け取る指示は、第2更新指示となる。また、ステップS40で生成される更新データリストは、旧ハッシュリスト、新ハッシュリスト、及び部分鍵から生成される。また、ステップS45では、生成した更新データリストと、第2更新指示に含まれるAP識別情報とが対応付けされる。

[0143] データ受取部211は、初期設定指示を受け取ると(ステップS10における「初期設定指示」)、改竄検出対象となる1つ以上のファイル、及びターゲットパスリストを取得する(ステップS55)。

データ受取部211は、受け取った初期設定指示、1以上のファイル、及びターゲットパスリストをハッシュリスト生成処理部212に出力する。

[0144] ハッシュリスト生成処理部212は、初期設定指示を受け取ると、さらに、改竄検出対象となる1つ以上のファイル、及びターゲットパスリストを受け取ると、ハッシュリストを生成する(ステップS60)。なお、ハッシュリストの生成については、ステップS20からステップS35までの動作と概念的には同じであるので、ここでの詳細な説明は省略する。

[0145] ハッシュリスト生成処理部212は、生成したハッシュリストを記憶部に格納するとともに、ハッシュリスト書込部204へ出力する。ハッシュリスト書込部204は、ハッシュリスト生成部203からハッシュリストを受け取ると、受け取ったハッシュリストを、接続された携帯電話機の記憶部へ書き込む(ステップS65)。

1．6 ハッシュリスト更新時の動作概要

ここでは、ハッシュリスト更新時の動作概要について、図11にて示す流れ図を用いて説明する。

[0146] 携帯電話機10における更新処理部103の更新制御部162は、更新指示を受け付けと(ステップS100)、制御部102に対して割り込み禁止の設定を行う(ステップS105)。

更新制御部162は、フラグ記憶部161に記憶されているフラグの値を「1」に設定する(ステップS110)。

[0147] 更新制御部162は、受け取った更新開始命令に含まれるAP識別情報を更新データ読取部163へ出力する。

更新ファイル受取部104は、更新処理部103の更新データ読取部163からAP識別情報を受け取ると、受け取ったAP識別情報と、予め記憶している端末識別子と、更新要求情報とを、無線部110を介して、更新サーバ装置20へ送信する(ステップS115)。更新ファイル受取部104は、受け取ったAP識別情報をAP識別情報記憶領域へ格納する。

[0148] 更新サーバ装置20の更新要求処理部205は、送受信部207を介して携帯電話機10から、AP識別情報と、端末識別子と、更新要求情報とを受信する(ステップS120)。

更新要求処理部205は、受信したAP識別情報と、端末識別子とを用いて、携帯電話機10に送信すべき更新データリストの版数を決定する。更新要求処理部205は、送信すべき更新データリストを記憶部201から取得し(ステップS125)、取得した更新データリストを、送受信部207を介して携帯電話機10へ送信する(ステップS130)。

[0149] 携帯電話機10は、更新サーバ装置20から更新データリストを受信し、更新処理を行う(ステップS135)。

1．7 更新処理の動作

ここでは、図11のステップS135にて示す更新処理の動作について、図12、及び図13にて示す流れ図を用いて説明する。

[0150] 更新ファイル受取部104は、更新サーバ装置20から無線部110を介して、更新データリストを受信すると、受信した更新データリストをリスト記憶領域へ格納する(ステップS200)。

更新ファイル受取部104は、受け取った更新データリストの格納が完了すると、AP識別情報記憶領域にて格納されているAP識別情報を消去し、受信完了命令を更新データ読取部163へ出力する。更新データ読取部163は、更新ファイル受取部104から更新サーバ装置20から更新データリストの受信が完了した旨の受信完了命令を受け取る。

[0151] 更新データ読取部163は、更新ファイル受取部104のリスト記憶領域にて記憶されている更新データリストから未読の更新情報を1つ読み出す(ステップS205)。

更新データ解析部164は、更新データ読取部163にて読み出された更新情報を、位置情報、データサイズ、及び更新データに分割する(ステップS210)。

書込位置決定部165は、更新データ解析部164にて取得された位置情報に基づいて、記憶部101における更新データの書込位置を決定する(ステップS215)。

[0152] 更新データ書込部166は、書込位置決定部165にて決定された書込位置を書込開始の先頭位置として、更新データ解析部164にて取得された更新データを書き込む(ステップS220)。

更新確認部167は、更新データ書込部166による書き込みが正常に終了したか否かを確認する(ステップS225)。

[0153] 正常に終了していないと判断する場合には(ステップS225における「YES」)、更新確認部167は、異常終了命令を更新データ読取部163へ出力する。更新データ読取部163は、更新確認部167から異常終了命令を受け取ると、ステップS205にて読み出した更新情報と同一の更新情報を再度読み出し(ステップS230)、ステップS210へ戻る。

[0154] 正常に終了したと判定する場合には(ステップS225における「YES」)、更新確認部167は、正常終了命令を更新データ読取部163へ出力する。更新データ読取部163は、更新確認部167から正常終了命令を受け取ると、更新ファイル受取部104のリスト記憶領域にて記憶されている更新データリストに未読の更新情報が存在するか

否かを判断する(ステップS235)。

[0155] 存在すると判断する場合には(ステップS235における「YES」)、更新データ読取部163は、ステップS205へ戻る。存在しないと判断する場合には(ステップS235における「NO」)、更新データ読取部163は、書込完了命令を、更新制御部162及び更新ファイル受取部104へ出力する。更新ファイル受取部104は、更新データ読取部163から書込完了命令を受け取ると、リスト格納領域に格納されている更新データリスト150を消去する。更新制御部162は、更新データ読取部163から書込完了命令を受け取ると、改竄検出の処理を開始する旨の検出開始命令と、AP識別情報とを改竄検出実行部105へ出力する。

[0156] 改竄検出実行部105は、更新制御部162から検出開始命令と、AP識別情報とを受け取ると、改竄検出処理を行う(ステップS240)。

更新制御部162は、改竄検出実行部105から改竄検出処理の処理結果を受け取ると、受け取った処理結果が、改竄されていない通知であるか、改竄が検出された通知であるかを判断する(ステップS245)。

[0157] 改竄が検出されていない、つまり改竄されていない通知を受け取ったと判断する場合には(ステップS245における「NO」)、更新制御部162は、更新完了の通知を制御部102へ出力する。制御部102は、更新処理部103からファイルの更新完了の通知を受け取ると、表示部109を介して更新完了のメッセージを表示する(ステップS250)。

[0158] 更新制御部162は、制御部102に対する割り込み禁止を解除し(ステップS255)、フラグ記憶部161に記憶されているフラグの値を「0」に設定する(ステップS260)。

改竄が検出された、つまり改竄が検出された通知を受け取ったと判断する場合には(ステップS245における「YES」)、更新制御部162は、更新失敗の通知を制御部102へ出力する。制御部102は、更新処理部103からファイルの更新失敗の通知を受け取ると、表示部109を介して、更新失敗のメッセージを表示する(ステップS265)。また、制御部102は、入力部108から再更新の指示を受け取ると、再更新開始命令を更新処理部103へ出力する。制御部102は、入力部108から再更新を行わない指示を受け取ると、更新終了命令を更新処理部103へ出力する。

[0159] 更新制御部162は、制御部102から再更新開始命令及び更新終了命令のうち何れかを受け取ると、受け取った命令が再更新開始命令か否かを判断する(ステップS270)。再更新開始命令である、つまり再更新を行うと判断する場合には(ステップS270における「YES」)、更新制御部162は、再度、AP識別情報を更新データ読取部163へ出力し、ステップS200へ戻る。この場合、更新データ読取部163は、再度、更新データリストの受信を行う。

[0160] 更新制御部162は、受け取った命令が更新終了命令である、つまり再更新を行わないと判断する場合には(ステップS270における「NO」)、更新制御部162は、制御部102に対する割り込み禁止を解除し(ステップS255)、フラグ記憶部161に記憶されているフラグの値を「0」に設定する(ステップS260)。

1．8 AP起動時の動作

ここでは、AP起動時の動作について、図14にて示す流れ図を用いて説明する。

[0161] 制御部102は、入力部108から改竄検出対象のAPの起動指示を受け取る(ステップS300)。制御部102は、APの起動を行う。このとき、起動されたAPは、自APが改竄検出対象である場合には、検出開始命令と、自APを識別するAP識別情報とを、制御部102により改竄検出実行部105へ出力する。

改竄検出実行部105は、制御部102から検出開始命令と、AP識別情報とを受け取ると、改竄検出処理を行う(ステップS305)。

[0162] 制御部102は、改竄検出実行部105から改竄検出処理の処理結果を受け取ると、受け取った処理結果が、改竄されていない通知であるか、改竄が検出された通知であるかを判断する(ステップS310)。

改竄が検出されていない、つまり改竄されていない通知を受け取ったと判断する場合には(ステップS310における「NO」)、制御部102は、起動指示のあったAPに係る動作を実行する(ステップS315)。

[0163] 改竄が検出された、つまり改竄が検出された通知を受け取ったと判断する場合には(ステップS310における「YES」)、制御部102は、起動指示のあったAPの動作を終了する(ステップS320)。

1．9 改竄検出処理の動作

ここでは、図12のステップS240、及び図14のステップS305のそれぞれにて示す改竄検出処理の動作について、図15及び図16にて示す流れ図を用いて説明する。

[0164] 検出制御部171は、制御部102若しくは更新処理部103の更新制御部162のいずれかから検出開始命令とAP識別情報とを受け取ると、受け取った検出開始命令とAP識別情報とを改竄検出呼出部172へ出力する。

改竄検出呼出部172は、検出制御部171から検出開始命令とAP識別情報とを受け取ると、記憶部101から受け取ったAP識別情報に対応するハッシュリストを読み出す(ステップS400)。

[0165] 改竄検出呼出部172は、読み出したハッシュリスト122と、受け取った検出開始命令及びAP識別情報とを、改竄検出処理部173へ出力する。改竄検出処理部173は、改竄検出呼出部172からハッシュリスト122と、検出開始命令及びAP識別情報とを受け取ると、改竄検出処理部173は、受け取ったAP識別情報に対応する部分鍵123を、記憶部101から読み出す。改竄検出処理部173は、読み出した部分鍵123と、マスタ鍵176と、特定のアルゴリズムとを用いて改竄検出鍵を算出する(ステップS405)。

[0166] 改竄検出処理部173は、算出した改竄検出鍵とハッシュ計算アルゴリズムとを用いて、受け取ったハッシュリストのデータ部に対するハッシュ値を算出する(ステップS410)。改竄検出処理部173は、算出したハッシュ値と、ハッシュリストのヘッダ部に含まれるデータ部ハッシュ値とが一致するか否かを判断する(ステップS415)。

一致しないと判断する場合には(ステップS415における「NO」)、改竄検出処理部173は、改竄が検出された通知を検出制御部171へ出力する。検出制御部171は、改竄検出処理部173から改竄が検出された通知のうちいずれかを受け取る。検出制御部171は、受け取った通知を、呼出元(つまり、検出開始命令及びAP識別情報の出力元)である制御部102若しくは更新処理部103の更新制御部162のいずれかへ出力する(ステップS420)。

[0167] 一致すると判断する場合には(ステップS415における「YES」)、改竄検出処理部173は、改竄検出鍵を用いて、データ部131を復号する(ステップS425)。なお、復号には、データ部を暗号化したアルゴリズムに対応する復号アルゴリズムが用いられる

。

改竄検出処理部173は、復号したデータ部から、未読のハッシュ情報を読み出す(ステップS430)。

[0168] 改竄検出処理部173は、読み出したハッシュ情報に含まれるファイル情報をファイル読込部174へ出力する。ファイル読込部174は、改竄検出処理部173からファイル情報を受け取ると、受け取ったファイル情報に含まれるファイル名に基づいて、改竄検出対象のファイルを記憶部101から読み出す(ステップS435)。

ファイル読込部174は、読み出したファイルをファイル記憶領域に格納し、ファイル読込完了命令を、改竄検出処理部173へ出力する。ファイル読込部174からファイルの読み込みが完了した旨を示すファイル読込完了命令を受け取る。

[0169] 改竄検出処理部173は、読み出したハッシュ情報から未読のエントリを取得し(ステップS440)、取得したエントリが最終エントリであるか否かを判断する(ステップS445)。

最終エントリでないと判断する場合には(ステップS445における「NO」)、改竄検出処理部173は、取得したエントリに含まれるオフセット及びサイズとを読み出し、読み出したオフセット及びサイズに基づいて、ファイル読込部174にて読み込まれたファイルから検出対象のブロックを取得する(ステップS450)。改竄検出処理部173は、算出した改竄検出鍵とハッシュ計算アルゴリズムとを用いて、取得したブロックに対する検出用ハッシュ値を算出する(ステップS455)。改竄検出処理部173は、算出した検出用ハッシュ値と取得したエントリに含まれるハッシュ値とが一致するか否かを判断する(ステップS460)。一致すると判断する場合には(ステップS460における「YES」)、改竄検出処理部173は、ステップS440へ戻る。一致しないと判断する場合には(ステップS460における「NO」)、ステップS420へ戻る。

[0170] 取得したエントリが最終エントリであると判断する場合には(ステップS445における「YES」)、改竄検出処理部173は、未読のハッシュ情報が存在するか否かを判断する(ステップS465)。存在すると判断する場合には(ステップS465における「YES」)、ステップS430へ戻る。存在しないと判断する場合には(ステップS465における「NO」)、改竄検出処理部173は、改竄されていない通知を検出制御部171へ出力する

。検出制御部171は、改竄検出処理部173から改竄されていない通知を受け取る。検出制御部171は、受け取った通知を、呼出元(つまり、検出開始命令及びAP識別情報の出力元)である制御部102若しくは更新処理部103の更新制御部162のいずれかへ出力する(ステップS470)。

[0171] 1．10 携帯電話機10の起動時の動作

携帯電話機10の起動時における更新処理及び改竄検出処理の動作について説明する。

携帯電話機10に電源が投入され、電源の供給が開始されると、更新制御部162は、フラグ記憶部161に記憶されているフラグの値をチェックする。

フラグの値が「0」である場合には、携帯電話機10は、前回の更新処理は完了していると判断し、更新処理及び改竄検出処理は行わない。

[0172] フラグの値が「1」である場合には、更新処理中の状態であると判断し、制御部102に対して割り込み禁止を設定する。更新制御部162は、更新処理の再開始を示す再開始命令を更新データ読取部163へ出力する。

更新データ読取部163は、更新制御部162から再開始命令を受け取ると、受け取った再開始命令を更新ファイル受取部104へ出力する。

[0173] 更新ファイル受取部104は、更新データ読取部163から再開始命令を受け取ると、AP識別情報記憶領域に格納されているAP識別情報が存在するか否かを判断する。存在すると判断する場合には、携帯電話機10は、図11にて示すステップS115以降の動作を行う。

AP識別情報記憶領域に格納されているAP識別情報が存在しないと判断する場合には、更新ファイル受取部104は、リスト記憶領域に更新データリストが格納されているか否かを判断する。

[0174] 更新データリストが格納されていると判断する場合には、受信完了命令を更新処理部103へ出力する。更新処理部103の更新データ読取部163は、更新ファイル受取部104から受信完了命令を受け取る。更新処理部103は、図12にて示すステップS205以降の動作を行う。

更新データリストが格納されていないと判断する場合には、再開始不要命令を更新

データ読取部163へ出力する。更新データ読取部163は、再開始不要命令を受け取ると、受け取った再開始不要命令を更新制御部162へ出力する。更新制御部162は、更新データ読取部163から更新処理の再開始が不要である旨を示す再開始不要命令を受け取ると、制御部102に対する割り込み禁止を解除し、フラグ記憶部161に記憶されているフラグの値を「0」に設定する。

[0175] 2. 検出鍵と各動作との関係

図17は、本実施の形態で用いられる各鍵の関係と、鍵が利用される場面との関係を示す。

改竄検出鍵は、マスタ鍵、部分鍵、及び特定のアルゴリズムとを用いて算出される。この生成作業は、鍵更新装置30の改竄検出鍵生成部302、及び図15にて示すステップS405により携帯電話機10にて行われる。

[0176] 生成された改竄検出鍵は、以下のようにハッシュリスト生成時、及びハッシュリストを用いた改竄検出処理時に用いられる。

(ハッシュリスト生成時)

改竄検出鍵は、検出対象のファイルにおける1以上のブロックそれぞれに対するハッシュ値を算出する場合に用いられる。具体的には、図10にて示すステップS20の動作に対応する。

[0177] また、改竄検出鍵は、ハッシュリストのデータ部を暗号化する場合に用いられる。具体的には、図10にて示すステップS25の動作に対応する。

また、改竄検出鍵は、ハッシュリストのデータ部のハッシュ値(データ部ハッシュ値)を算出する場合に用いられる。算出されたハッシュ値はハッシュリストのヘッダ部に埋め込まれる。具体的には、図10にて示すステップS30の動作に対応する。

[0178] (改竄検出処理時)

改竄検出鍵は、ハッシュリストのデータ部のハッシュ値を算出する場合に用いられる。具体的には、図15にて示すステップS410の動作に対応する。このとき、携帯電話機10は、算出されたハッシュ値と、あらかじめ埋め込まれたハッシュ値(データ部ハッシュ値)とを比較することで改竄の有無をチェックする。

[0179] また、改竄検出鍵は、ハッシュリストのデータ部を復号する場合に用いられる。具体

的には、図15にて示すステップS425の動作に対応する。

また、改竄検出鍵は、検出対象のファイルにおける各ブロックのハッシュ値（検出用ハッシュ値）を算出場合に用いられる。具体的には、図16にて示すステップS455の動作に対応する。このとき、携帯電話機10は、算出された検出用ハッシュ値と、予め格納されているハッシュ値とを比較することで改竄の有無をチェックする。

[0180] 3. 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。

（1）上記第1の実施の形態では、改竄を検出する装置として携帯電話機を用いたが、これに限定されない。

[0181] 改竄を検出する装置は、通信機能を具備したHDDレコーダ／DVDレコーダ、ゲーム機器、PDAのような機器であってもよい。つまり、更新サーバ装置とネットワーク等により接続可能な電子機器であればよい。

（2）ハッシュリストのデータ部の暗号化は、セキュリティ強度を考慮して、データ部131の暗号化単位はデータ部全体に共通鍵暗号方式における連鎖のような暗号アルゴリズムを適用してもよい。このときのハッシュリストの更新単位はハッシュリスト全体となる。

[0182] （3）上記第1の実施の形態において、ハッシュリストの更新時に、改竄検出対象のファイルのサイズが増大して、更新前のMAC情報のエントリ数が増加した場合は、更新サーバ装置は、図18にて示すハッシュリスト122aを生成してもよい。図18においてファイル情報140aに対応するMAC情報141aの最後のエントリは、MAC情報1000に含まれるエントリ1001のアドレスを指すリンクエントリ144aとなっている。通常のエントリと、リンクエントリとは、サイズ及びハッシュとが異なる。リンクエントリのそれぞれには、数値が格納されずに、「—」が格納される。これにより、通常のエントリとリンクエントリとを区別することができる。

[0183] リンクエントリ144aのオフセットには、エントリ1001のアドレスを指す値として、ハッシュリスト内でのファイルからのオフセットが格納される。

このとき、ファイル情報140aに含まれるブロック数142aは、MAC情報141aとMAC情報1000とにおいて、リンクエントリ144aと、MAC情報1000の空エントリ1002(最終エントリ)とを除いたエントリ数である“4”となっている。

[0184] この場合のハッシュリストの生成方法の一例を以下に示す。

ハッシュリスト生成処理部212は、改竄検出鍵215を読み出す。そして、改竄検出鍵215を用いて、旧ハッシュリストのデータ部の復号を行い復号された旧ハッシュリストを生成する。以下復号された旧ハッシュリストを復号ハッシュリストという。

ハッシュリスト生成処理部212は、データ受取部211から受け取った1つ以上の更新ファイルに対して、所定のサイズに分割したブロック単位で、改竄検出処理部173と同一のハッシュ計算アルゴリズムを適用してハッシュ値を算出し、ターゲットパスリストから携帯電話機10におけるファイルパスを読み取り、復号ハッシュリストと比較して、データ部が暗号化されていないハッシュリストを生成する。このとき、生成したハッシュリストのサイズが復号ハッシュリストよりも大きくなるようなファイルの更新であった場合は、ハッシュリスト生成処理部212は、生成したハッシュリストを、図18に示すようなリンクエントリを用いたハッシュリストに変換する。

[0185] (4)上記第1の実施の形態において、改竄検出実行部105の改竄検出処理部173とファイル読込部174とを個別の構成としたが、これに限定されない。

改竄検出処理部173とファイル読込部174とを1つの構成要素としてもよい。

(5)上記第1の実施の形態において、ファイルの更新時には、指定されたAPを含む検出対象情報群を更新の対象としたが、これに限定されない。

[0186] 1回の更新指示により、全ての検出対象情報群を更新の対象としてもよい。

(6)上記第1の実施の形態において、更新データリストのみを利用して、APに係るファイルを更新したが、これに限定されない。

更新サーバ装置は、携帯電話機へ、更新データリストとともに、更新対象となる1以上の更新ファイルを送信してもよい。このとき、送信される更新データリストには、ハッシュリストに係る更新情報のみから構成される。

[0187] (7)上記第1の実施の形態において、検出対象のファイルは、予め決められたサイズのブロック単位で分割されたが、これに限定されない。

更新サーバ装置は、ユーザの操作により入力値として、分割されるブロックのサイズを受け付ける構成であってもよい。これにより、ブロックのサイズを柔軟に設定できる。

(8)上記第1の実施の形態において、更新サーバ装置は、データ部ハッシュ値の算出を、データ部の暗号化後に行ったが、これに限定されない。

[0188] 更新サーバ装置は、データ部の暗号化の前に、データ部ハッシュ値の算出を行ってもよい。

このとき、改竄検出の実行時には、データ部の復号後に、データ部に対するハッシュ値を算出し、ハッシュリスト自体の改竄検出を行うことになる。

(9)上記第1の実施の形態において、ハッシュリストのデータ部の暗号化に用いられる鍵と、ハッシュ計算に用いられる鍵とは、同一の鍵(改竄検出鍵)としたが、同一でなくてもよい。

[0189] (10)上記第1の実施の形態において、更新データリストは、ハッシュリストの更新内容とともに、更新ファイルの更新内容、及び更新された部分鍵を含めるとしたが、これに限定されない。

更新データリストは、ハッシュリスト用の更新データリスト、更新ファイル用の更新データリスト、及び部分鍵用の更新データリストに分けてもよい。

[0190] (11)上記第1の実施の形態において、ハッシュリストの更新は、携帯電話機を使用する使用者の要求によるものとしたが、更新サーバ装置からの強制アップデートであってもよい。

例えば、鍵更新装置で、更新サーバ装置に新たな改竄検出鍵が埋め込まれた場合には、更新サーバ装置は、更新された部分鍵を携帯電話機に送付するため、更新データリストを生成し、生成した更新データリストを、直ちに、携帯電話機へ送信する。

[0191] (12)上記第1の実施の形態において、他の携帯電話機は、携帯電話機10と同一のマスタ鍵を有してもよいし、異なるマスタ鍵を有してもよい。

携帯電話機間で異なるマスタ鍵を有する場合には、鍵更新装置は、複数のマスタ鍵を管理しており、更新された部分鍵から算出される改竄検出鍵も異なるため、更新サーバ装置においても複数の改竄検出鍵を管理することとなる。

[0192] (13)上記第1の実施の形態にて示すハッシュリストを、図19にて示すハッシュリスト122bとしてもよい。図19に示すハッシュリスト122bは、ヘッダ部130bにハッシュリストの版数を示すハッシュリストバージョン番号1010を有する。

この場合、携帯電話機は、更新サーバ装置に更新要求情報を送信するとき、ハッシュリストバージョン番号1010をも送信する。

[0193] 更新サーバ装置は、生成したハッシュリストのハッシュリストバージョン番号毎に更新データリストを管理しておき、携帯電話機から受信したハッシュリストバージョン番号1010に応じた更新データリストを携帯電話機へ送信する。

(14)上記第1の実施の形態において、改竄検出処理は、ハッシュリストに含まれるMAC情報が有する全てのエントリを用いて、改竄検出を行ったがこれに限定されない。

[0194] より速度の求められる場合では、各MAC情報において、オフセットが0番のエントリのみをチェックするような手順であってもよい。また、ファイル情報のブロック数を読み込み、その半分のブロック数をチェックするような手順であってもよい。

つまり、改竄検出処理は、各MAC情報において、1つ以上のエントリをチェックするような手順であればよい。

[0195] (15)上記第1の実施の形態において、改竄検出の実行は、ハッシュリストの更新時、及び検出対象のAPの起動時としたが、これに限定されない。

改竄検出の実行は、携帯電話機の起動中に行ってもよいし、検出対象のAPを実行しているときに、バックグラウンドで実行してもよい。

または、携帯電話機は、当該携帯電話機の起動中に、定期的に改竄検出を実行してもよいし、検出対象のAPが起動している間に、起動しているAPに対する改竄検出を定期的に実行してもよい。

[0196] (16)図15にて示すステップS425において、携帯電話機は、データ部全体を復号しているが、これに限定されない。

携帯電話機は、MAC情報の1エントリ毎に復号を行うような構成であってもよい。

このとき、携帯電話機は、図15にて示すステップS415を実行後、ステップS425を省略し、ステップS430からステップS440までを実行する。このとき、読み出したエン

トリは暗号化されている。携帯電話機は、その後、読み出したエントリを復号し、ステップS445以降を行う。または、携帯電話機は、図15にて示すステップS415を実行後、ステップS425を省略し、ステップS430からステップS445までを実行し、その後、復号してもよい。

[0197] (17)上記第1の実施の形態において、ハッシュリストの更新時に、改竄検出対象のファイルのサイズが小さくなった場合には、不要となるエントリに含まれるサイズを「0」に設定する。

図20に、ファイルのブロック数が「8」から「7」に減少した場合の一例を示す。

この場合、更新前であるハッシュ情報1020において、8番目のブロックのエントリ1021に含まれるサイズは120が格納されている。ファイルの更新により、ブロック数が「8」から「7」に減少すると、8番目のブロックのエントリ1031に含まれるサイズを「0」として、ハッシュ情報1030が生成される。このとき、エントリ1031も更新の対象となることは言うまでもない。

[0198] 改竄検出を実行する際には、携帯電話機は、エントリに含まれるサイズが「0」である場合には、そのエントリを無視、そのエントリに対する改竄のチェックは行わない。

なお、エントリ1031に含まれるハッシュ値は、更新前の値としているが、ハッシュ値を“0”にしてもよい。

これによると、携帯電話機は、サイズに格納される値を、当該サイズを含むエントリが改竄検出の対象であるか否かを判断する判断情報として用いることができる。つまり、値が「0」であると改竄検出の対象でないと判断し、「0」以外の値である場合には改竄検出の対象であると判断することができる。

[0199] (18)2つの携帯電話機(ここでは、携帯電話機11、12とする)において、携帯電話機11が機能A(例えば、オーディオデータの再生機能)を含む第1APと、機能B(例えば、コンテンツを暗号化しSDカードに格納するSD－Binding機能)を含む第2APとを具備し、携帯電話機12が機能A及び機能Bの双方を含む統合APを具備する場合、上記の第1の実施の形態にて示すように、AP毎に異なるハッシュリストが与えられてもよいし、以下に示すように1つのハッシュリストが与えられてもよい。

[0200] 図21に、第1AP、第2AP、及び統合APに対して与えられた1つのハッシュリスト12

2cのデータ構成の一例を示す。なお、ヘッダ部130cのデータ構成は、第1の実施の形態にて示すハッシュリスト122のヘッダ部130のデータ構成と同様であるため、ここでの説明は省略する。

第1の実施の形態にて示すハッシュリスト122と異なる点は、ファイル情報に種別が追加されている点である。種別は、改竄検出の実行時に使用するハッシュ情報を識別するためのものであり、例えば、数値1、2、・・・、及びALLからなる。種別にALLが設定されると、ハッシュリストに含まれる全てのハッシュ情報が検出に用いられることを示し、数値が設定されると、設定された種別(数値)を含むファイル情報を有するハッシュ情報が検出の対象となる。

[0201] この場合、各AP(第1AP、第2AP、及び統合AP)は、自身の種別を記憶しており、起動時に記憶している種別を改竄検出実行部へ渡す。ここで、第1AP、第2AP、及び統合APのそれぞれには、種別1、2、ALLが設定されているものとする。

携帯電話機11において、第1APが起動されると、図21に示すように、種別「1」を含むファイル情報1040を有するハッシュ情報134cが、改竄検出の対象となる。

[0202] また、携帯電話機11において、第2APが起動されると、種別「2」を含むファイル情報1041を有するハッシュ情報135cが、改竄検出の対象となる。

携帯電話機12において、統合APが起動されると、統合APは種別「ALL」を記憶しているので、データ部131cに含まれる全てのハッシュ情報が、改竄検出の対象となる。

[0203] (19)上記第1の実施の形態にて示すハッシュリストにおいて改竄検出の対象のとなる少なくとも1つ以上のファイルを優先的に改竄検出を実行する優先度を設けてもよい。このとき、例えば、優先的に改竄検出されるファイルに対しては、APの起動時に改竄検出が実行され、他の改竄検出対象のファイルに対しては、APの起動が完了し、APが有する機能の動作中にバックグラウンドで改竄検出が実行される。

[0204] 図22に、優先度を用いたハッシュリスト122dのデータ構成の一例を示す。なお、ヘッダ部130dのデータ構成は、第1の実施の形態にて示すハッシュリスト122のヘッダ部130のデータ構成と同様であるため、ここでの説明は省略する。

第1の実施の形態にて示すハッシュリスト122と異なる点は、データ部131dに第1

オフセット1050と第2オフセット1051とからなる組みが追加されている点である。

[0205] 第1オフセットは、優先的に改竄検出を行うハッシュ情報の先頭位置を示すオフセット値であり、第2オフセットは、優先的に改竄検出を行うハッシュ情報の最終位置を示すオフセット値である。

例えば、第1オフセットにハッシュ情報134dの先頭位置を示すオフセット値が格納され、第2オフセットにハッシュ情報134dの最終位置を示すオフセット値が格納されている場合には、ファイル名「file__1」であるファイルに対する改竄検出は、AP起動時に行われ、他のファイルに対する改竄検出は、動作中にバックグラウンドで行われる。

[0206] また、第1オフセットにハッシュ情報134dの先頭位置を示すオフセット値が格納され、第2オフセットにハッシュ情報136dの最終位置を示すオフセット値が格納されている場合には、ファイル名「file__1」であるファイル及びファイル名「file__2」であるファイルそれぞれに対する改竄検出は、AP起動時に行われ、他のファイルに対する改竄検出は、動作中にバックグラウンドで行われる。

[0207] (20)上記第1の実施の形態において、1つのAPファイル群、つまり1つのAPに対して、1つのハッシュリストが与えられたが、これに限定されない。

1以上のAPファイル群に対して、1つのハッシュリスト及び部分鍵を与えてもよい。

この場合における記憶部101構成を図23に示す。

図23において、記憶部101は1つの検出対象情報群1200を有している。

[0208] 検出対象情報群1200は、1以上のAPファイル群1060、1061、・・・、1062と、ハッシュリスト122eと、部分鍵123eとを有している。

ハッシュリスト122eのデータ部には、APファイル群1060、1061、・・・、1062のそれぞれに含まれる各ファイルに対するハッシュ情報が含まれている。

検出対象情報群1200に含まれる1のAPが起動された場合、携帯電話機は、検出対象情報群1200に含まれる全てのファイルを改竄検出対象としてもよいし、起動されたAPに係る1以上のファイルのみを改竄検出の対象としてもよい。

[0209] (21)上記第1の実施の形態において、携帯電話機10の電源投入時に、更新制御部162は、フラグの値のチェックを行い、フラグの値が「1」である場合には、ファイル

の更新を自動的に行ったが、これに限定されない。

携帯電話機10は、更新制御部162がフラグの値が「1」であると判断する場合には、ファイルの更新を再度行うか否かを通知し、ユーザから再度更新を行うとの指示を受け取った場合にファイルの更新を再度行ってもよい。

[0210] または、ファイルの更新を自動的に行う場合において、再度更新を行う旨をユーザに通知してもよい。

または、携帯電話機10の電源投入時に、更新制御部162は、フラグの値のチェックを行い、フラグの値が「1」である場合には、未更新のデータのみに対して更新を行ってもよい。つまり、携帯電話機10は、更新処理の途中（電源が落とされたときに動作していた時点）から更新の動作を行ってもよい。

[0211] (22)上記第1の実施の形態において、ハッシュリストのデータ部は暗号化されているとしたが、これに限定されない。

データ部は暗号化しなくてもよい。

(23)本発明におけるアプリケーションファイルとは、アプリケーションソフトウェアそのものや、アプリケーションソフトウェアから呼び出されるエンコーダ、デコーダ、ドライバ、アプリケーションソフトウェアが動作する環境を提供するJava（登録商標）VMのような仮想実行環境などである。また、アプリケーションファイルの概念に、部分鍵を含めてもよい。

[0212] (24)上記第1の実施の形態において、鍵更新装置は、外部装置から更新された部分鍵を取得するとしたが、これに限定されない。

鍵更新装置にて新たな部分鍵を生成して取得してもよい。

また、マスタ鍵は、鍵更新装置で記憶しておいてもよいし、外部装置から取得してもよい。

[0213] (25)上記第1の実施の形態において、更新データリストに含まれる更新データは、更新すべき情報であるファイルのうち更新対象となる1以上のブロック、ハッシュリストにおけるハッシュリストファイルサイズ、データ部ハッシュ値、ファイル情報、MAC情報に含まれるエントリなどが記録されているとしたが、これに限定されない。

更新すべき情報であるファイルのうち更新対象となる1以上のブロックを更新データ

として記録する代わりに、アプリケーションソフトウェアを実行するための命令文などのような更新されたデータのみを記録してもよい。

[0214] また、更新対象となるブロックを、本願発明の「データ」の概念に含めてもよい。

(26)上記第1の実施の形態において、改竄検出用の値(改竄検出値)として、ハッシュ値を用いて改竄の検出を行ったが、これに限定されない。

ハッシュ値とは異なる値、データを用いてもよい。例えば、検証対象のデータを暗号化した結果等を改竄検出値として用いることができる。

[0215] (27)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。

[0216] (28)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。

[0217] ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、システム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。

[0218] 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。バイオ技術の適応等が可能性としてありえる。

(29)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。

[0219] (30)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。

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。

[0220] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリと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従って動作するとしてもよい。

[0221] また、前記プログラム又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、又は前記プログラム又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。

(31)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。

4. まとめ

本発明によれば、プログラム更新可能な電子機器においても実現可能な改竄検出方式の提供が可能となる。また、更新時の更新箇所を最小限にとどめ、更新時にかかる通信コストをおさえることができる。さらに電子機器の持つスペックに応じて、実行時の速度チューニングが可能な改竄検出方式の提供が可能となる。

[0222] また、改竄検出時に必要な鍵の生成に必要な情報を、更新サーバとは別の場所で管理することが可能であるため、万が一その鍵が漏洩しても鍵の発行および電子機器の鍵の更新が可能な改竄検出方式の提供が可能となる。

産業上の利用可能性

[0223] 上記にて示したプログラム更新システムを構成する各装置は、電器機器製造産業において、経営的、つまり反復的かつ継続的に利用されうる。

また、本発明にかかるプログラム更新可能な電子機器における改竄検出方式は、セキュアなプログラムの実行を必要とする携帯電話をはじめとした組み込み機器がプログラムの更新機能を備えている場合に有用である。

請求の範囲

[1] アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器であって、

1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段と、

更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取手段と、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新する更新処理手段と、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行手段と

を備えることを特徴とする電子機器。

[2] 前記受取手段は、更新データと位置情報との組を少なくとも1つ以上受け取り、

前記更新処理手段は、

前記位置情報にて示される位置に基づいて、前記アプリケーションファイルの更新位置を決定する位置決定部と、

決定された前記更新位置を前記更新データの書き込み開始位置として、前記更新データを書き込む書込部と、

前記受取手段にて受け取った1つ以上の更新データ全ての書き込みが完了するまで、前記位置決定部と前記書込部の処理を行うように制御する更新制御部と

を備えることを特徴とする請求項1に記載の電子機器。

[3] 前記更新制御部は、

全ての更新データの書き込みが完了すると、前記改竄検出実行手段の処理を開始するように制御する

ことを特徴とする請求項2に記載の電子機器。

[4] 前記更新処理手段は、さらに、

アプリケーションファイルの更新中であることを示す第1の情報、又は更新中でないことを示す第2の情報の何れかを示すフラグを記憶しているフラグ記憶部と、

前記フラグが示す情報を変更するフラグ変更部とを備え、

前記フラグ変更部は、

前記受取手段が更新データと位置情報との組を少なくとも1つ以上受け取るときに、前記フラグの情報を、前記第1の情報に変更し、前記改竄検出実行手段にて改竄が検出されなかった場合に、前記フラグの情報を、前記第2の情報に変更する

ことを特徴とする請求項3に記載の電子機器。

[5] 前記更新制御部は、さらに、

前記電子機器に電源が投入されると、前記フラグが示す情報を確認し、第1の情報である場合には、前記位置決定部と前記書込部の処理を行うように制御する

ことを特徴とする請求項4に記載の電子機器。

[6] 前記アプリケーションファイルは、1つ以上のブロックに分割されており、

前記更新データは、前記1以上のブロックのうち少なくとも1つ以上の更新対象ブロックに含まれ、

前記記憶手段は、1つ以上の前記ブロックそれぞれに対する基準改竄検出値を有する改竄検出リストを記憶しており、

前記受取手段は、さらに、1つ以上の前記更新対象ブロックそれぞれに対する新たな基準改竄検出値と、前記1つ以上の前記更新対象ブロックそれぞれに対する基準改竄検出値の、前記改竄検出リストにおける位置を示す改竄検出位置情報とからなる組を受け取り、

前記更新処理手段は、さらに、1つ以上の新たな基準改竄検出値と、前記改竄検出値位置情報とを用いて、前記改竄検出リストを更新し、

前記改竄検出実行手段は、

前記更新された改竄検出リストが正当なものである場合にのみ、前記更新された改竄検出リストが有する少なくとも1つ以上の基準改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認する

ことを特徴とする請求項3に記載の電子機器。

[7] 前記アプリケーションファイルは、1つ以上のブロックに分割されており、

前記記憶手段は、1つ以上の前記ブロックそれぞれに対する基準改竄検出値を有

する改竄検出リストを記憶しており、

前記改竄検出実行手段は、前記アプリケーションソフトウェアの起動時に処理を開始し、前記改竄検出リストが正当なものである場合にのみ、前記改竄検出リストが有する少なくとも1つ以上の改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認する

ことを特徴とする請求項1に記載の電子機器。

[8] 前記改竄検出手段は、

改竄検出対象であるブロックに対する検出用改竄検出値を算出し、算出した検出用改竄検出値と、改竄検出対象であるブロックに対する改竄検出値とが一致するか否かを判断し、一致すると判断する場合には前記アプリケーションファイルは改竄されていないとし、一致しない場合には前記アプリケーションファイルは改竄されているとする

ことを特徴とする請求項7に記載の電子機器。

[9] 前記記憶部は、部分鍵を記憶しており、

前記改竄検出実行手段は、耐タンパ化されており、マスタ鍵を記憶し、前記部分鍵と前記マスタ鍵とを用いて、改竄検出鍵を生成し、生成した改竄検出鍵を用いて、前記検出用改竄検出値を算出する

ことを特徴とする請求項8に記載の電子機器。

[10] 前記受取手段は、前記部分鍵とは異なる別の部分鍵と、前記部分鍵が前記記憶部にて記憶されている位置を示す鍵位置情報とを受け取り、

前記更新処理手段は、前記鍵位置情報に基づいて、前記部分鍵を前記別の部分鍵に更新する

ことを特徴とする請求項9に記載の電子機器。

[11] 前記改竄検出リストは、前記1つ以上のブロックそれぞれに対する基準改竄検出値を含むデータ部と、前記データ部に対する基準データ部改竄検出値を含むヘッダ部とから構成され、

前記改竄検出実行手段は、前記データ部に対する検出用データ部改竄検出値を算出し、算出した前記検出用データ部改竄検出と前記基準データ部改竄検出値と

が一致する場合に、前記改竄検出リストが正当なものであるとする

ことを特徴とする請求項7に記載の電子機器。

[12] 前記データ部は暗号化されており、

前記改竄検出実行手段は、暗号化された前記データ部に対する検出用改竄検出値を算出し、前記改竄検出リストが正当なものである場合に、暗号化された前記データ部を復号する

ことを特徴とする請求項11に記載の電子機器。

[13] 前記改竄検出リストにおいて、基準改竄検出値のそれぞれに対して、対応するブロックが改竄検出の対象として使用すべきか否かを示す判断情報が対応付けられており、

前記改竄検出実行手段は、前記判断情報がブロックを改竄検出の対象としない旨を示す場合には、当該ブロックに対する改竄検出は行わない

ことを特徴とする請求項7に記載の電子機器。

[14] 前記改竄検出リストは、前記1つ以上のブロックそれぞれに対する基準改竄検出値と、改竄検出の対象となるアプリケーションソフトウェアの種別を示すアプリケーション種別とが対応付けられた組を1つ以上含み、

前記改竄検出実行手段は、起動されたアプリケーションソフトウェアに対するアプリケーション種別に対応する基準改竄検出値それぞれのうち少なくとも1つ以上の改竄検出値に基づいて、改竄検出の対象となるブロックが改竄されているか否かを確認する

ことを特徴とする請求項7に記載の電子機器。

[15] 前記アプリケーションソフトウェアの動作に係るアプリケーションファイルは複数個あり、

前記アプリケーションファイルのそれぞれは、1つ以上のブロックに分割されており、

前記改竄検出リストは、アプリケーションファイルそれぞれに対して、1つ以上のブロックそれぞれに対する基準改竄検出値を基準値群として格納し、1つ以上の前記基準値群のうち前記アプリケーションソフトウェアの起動時に改竄検出に用いる少なくとも1つ以上の基準値群の範囲を示す範囲情報を有し、

前記改竄検出実行手段は、前記アプリケーションソフトウェアの起動時に、前記改竄検出リストが有する前記範囲情報にて示される少なくとも1つ以上の基準値群を用いて、改竄検出の対象となるブロックが改竄されているか否かを確認する

ことを特徴とする請求項7に記載の電子機器。

[16] 前記更新処理手段及び前記改竄検出実行手段は、耐タンパ化されている

ことを特徴とする請求項2に記載の電子機器。

[17] ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置であって、

更新後のアプリケーションファイルを取得する第1取得手段と、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを第2取得手段と、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信手段とを備えることを特徴とする更新サーバ装置。

[18] 前記更新前のアプリケーションファイルは、所定の大きさからなる1つ以上の更新前ブロックに分割されており、

前記第1取得手段は、さらに、

1つ以上の前記更新前ブロックそれぞれと、前記更新前ブロック毎に対する基準改竄検出値とからなる更新前改竄検出リストを取得し、

前記更新サーバ装置は、さらに、

前記更新後のアプリケーションファイルを前記所定の大きさに分割された1つ以上の更新後ブロックを取得し、取得した1つ以上の更新後ブロックそれぞれに対して基準改竄検出値を再計算して新たな改竄検出リストを生成する改竄検出リスト生成手段を備え、

前記第2取得手段は、さらに、

前記改竄検出リスト生成手段にて生成された新たな改竄検出リストから、前記更新データを含む更新後ブロックと、その更新後ブロックに対応する再計算された基準改竄検出値と、その更新後ブロックに対応する更新前ブロックの前記更新前改竄検出リ

ストにおける位置を示す改竄検出値位置情報とを取得し、

前記送信手段は、さらに、

前記第2取得手段にて取得された更新後ブロックと前記基準改竄検出値と前記改竄検出値位置情報とを前記電子機器に送信する

ことを特徴とする請求項17に記載の更新サーバ装置。

[19] 前記改竄検出リスト生成手段は、

外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、前記1以上の更新後ブロックそれぞれに対する基準改竄検出値を算出する

ことを特徴とする請求項18に記載の更新サーバ装置。

[20] 前記更新サーバ装置は、

前記外部装置によって更新された部分鍵と前記マスタ鍵とを用いて更新された改竄検出鍵を受け取ると、記憶している前記改竄検出鍵を、受け取った前記更新された改竄検出鍵に更新し、さらに、前記更新された部分鍵を前記外部装置から受け取り、

前記改竄検出リスト生成手段は、

前記更新された改竄検出鍵を用いて、前記1以上の更新後ブロックのそれぞれに対する基準改竄検出値を算出し、

前記第2取得手段は、さらに、

前記電子機器にて前記部分鍵が記憶されている位置を示す鍵位置情報を取得し、

前記送信手段は、さらに、

前記更新された部分鍵と、前記鍵位置情報とを前記電子機器に送信する

ことを特徴とする請求項19に記載の更新サーバ装置。

[21] 前記改竄検出リストは、前記1つ以上の更新後ブロックそれぞれと、前記更新後ブロック毎に対する基準改竄検出値とからなるデータ部を有し、

前記改竄検出リスト生成手段は、生成した新たな改竄検出リストのデータ部を暗号化する

ことを特徴とする請求項19に記載の更新サーバ装置。

[22] 前記更新後改竄検出リストは、ヘッダ部を有し、

前記改竄検出リスト生成手段は、

外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、暗号化されたデータ部に対するデータ部改竄検出値を算出し、算出したデータ部改竄検出値を前記ヘッダ部へ格納する

ことを特徴とする請求項21に記載の更新サーバ装置。

[23] 前記改竄検出リストは、ヘッダ部と、前記1つ以上の前記更新後ブロックそれぞれと、前記更新後ブロック毎に対する基準改竄検出値とからなるデータ部とを有し、

前記改竄検出リスト生成手段は、

外部装置によって部分鍵とマスタ鍵とを用いて生成された改竄検出鍵を記憶しており、前記改竄検出鍵を用いて、前記データ部に対するデータ部改竄検出値を算出し、算出したデータ部改竄検出値を前記ヘッダ部へ格納する

ことを特徴とする請求項19に記載の更新サーバ装置。

[24] 前記改竄検出リスト生成手段は、

前記データ部改竄検出値の算出後、前記データ部を暗号化する

ことを特徴とする請求項23に記載の更新サーバ装置。

[25] 前記更新サーバ装置は、外部の改竄検出リスト生成装置を前記改竄検出リスト生成手段として用いる

ことを特徴とする請求項19に記載の更新サーバ装置。

[26] 1つ以上のブロックに分割されたアプリケーションファイルに対してブロック毎に改竄検出値を算出するために用いられる改竄検出鍵を生成する鍵生成装置であって、

前記改竄検出鍵は、マスタ鍵と、部分鍵とから生成され、

前記鍵生成装置は、

前記マスタ鍵と、更新された部分鍵とを取得する鍵取得手段と、

前記マスタ鍵と前記更新された部分鍵とを用いて新たな改竄検出鍵を生成する鍵生成手段と、

前記鍵生成手段にて生成された改竄検出鍵を、前記改竄検出値を含む改竄検出

リストを生成する外部装置へ配布する配布手段と

を備えることを特徴とする鍵生成装置。

[27] 前記配布手段は、前記更新された部分鍵を、前記外部装置を介して前記アプリケーションファイルが改竄されているか否かの確認を行う電子機器へ配布する

ことを特徴とする請求項26に記載の鍵生成装置。

[28] アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器で用いられる更新方法であって、

前記電子機器は

1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段を備え、

前記更新方法は、

更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取ステップと、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルを更新する更新処理ステップと、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行ステップと

を含むことを特徴とする更新方法。

[29] アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器で用いられる更新プログラムであって、

前記電子機器は

1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段を備え、

前記更新プログラムは、

更新データと、前記アプリケーションファイルにおいて前記更新データによって更新

する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取ステップと、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルを更新する更新処理ステップと、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行ステップと

を含むことを特徴とする更新プログラム。

[30] 前記更新プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項29に記載の更新プログラム。

[31] ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置で用いられ、更新に必要な情報を取得する取得方法であって、

更新後のアプリケーションファイルを取得する第1取得ステップと、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを第2取得ステップと、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信ステップと

を含むことを特徴とする取得方法。

[32] ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置で用いられ、更新に必要な情報を取得する取得プログラムであって、

更新後のアプリケーションファイルを取得する第1取得ステップと、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを第2取得ステップと、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信ステップと

を含むことを特徴とする取得プログラム。

[33] 前記取得プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項32に記載の取得プログラム。

[34] アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器の集積回路であって、

前記電子機器は

1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段を備え、

前記集積回路は、

更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取手段と、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新する更新処理手段と、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行手段と

を備えることを特徴とする集積回路。

[35] ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置の集積回路であって、

更新後のアプリケーションファイルを取得する第1取得手段と、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを第2取得手段と、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信手段と

を備えることを特徴とする集積回路。

補正書の請求の範囲

[2006年9月18日（18．09．2006）国際事務局受理]

前記改竄検出実行手段は、前記アプリケーションソフトウェアの起動時に、前記改竄検出リストが有する前記範囲情報にて示される少なくとも1つ以上の基準値群を用いて、改竄検出の対象となるブロックが改竄されているか否かを確認する

ことを特徴とする請求項7に記載の電子機器。

[16] 前記更新処理手段及び前記改竄検出実行手段は、耐タンパ化されている

ことを特徴とする請求項2に記載の電子機器。

[17] （補正後）ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置であって、

更新後のアプリケーションファイルを取得する第1取得手段と、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを取得する第2取得手段と、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信手段とを備えることを特徴とする更新サーバ装置。

[18] 前記更新前のアプリケーションファイルは、所定の大きさからなる1つ以上の更新前ブロックに分割されており、

前記第1取得手段は、さらに、

1つ以上の前記更新前ブロックそれぞれと、前記更新前ブロック毎に対する基準改竄検出値とからなる更新前改竄検出リストを取得し、

前記更新サーバ装置は、さらに、

前記更新後のアプリケーションファイルを前記所定の大きさに分割された1つ以上の更新後ブロックを取得し、取得した1つ以上の更新後ブロックそれぞれに対して基準改竄検出値を再計算して新たな改竄検出リストを生成する改竄検出リスト生成手段を備え、

前記第2取得手段は、さらに、

前記改竄検出リスト生成手段にて生成された新たな改竄検出リストから、前記更新データを含む更新後ブロックと、その更新後ブロックに対応する再計算された基準改竄検出値と、その更新後ブロックに対応する更新前ブロックの前記更新前改竄検出リ

する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取ステップと、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルを更新する更新処理ステップと、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行ステップと

を含むことを特徴とする更新プログラム。

[30] 前記更新プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項29に記載の更新プログラム。

[31] (補正後)ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置で用いられ、更新に必要な情報を取得する取得方法であって、

更新後のアプリケーションファイルを取得する第1取得ステップと、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを取得する第2取得ステップと、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信ステップと

を含むことを特徴とする取得方法。

[32] (補正後)ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置で用いられ、更新に必要な情報を取得する取得プログラムであって、

更新後のアプリケーションファイルを取得する第1取得ステップと、

取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを取得する第2取得ステップと、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信ステップと

を含むことを特徴とする取得プログラム。

[33] 前記取得プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項32に記載の取得プログラム。

[34] アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する電子機器の集積回路であって、

前記電子機器は

1つ以上のデータからなるアプリケーションファイルを記憶している記憶手段を備え、

前記集積回路は、

更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る受取手段と、

前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新する更新処理手段と、

更新された前記アプリケーションファイルが改竄されているか否かの確認を行う改竄検出実行手段と

を備えることを特徴とする集積回路。

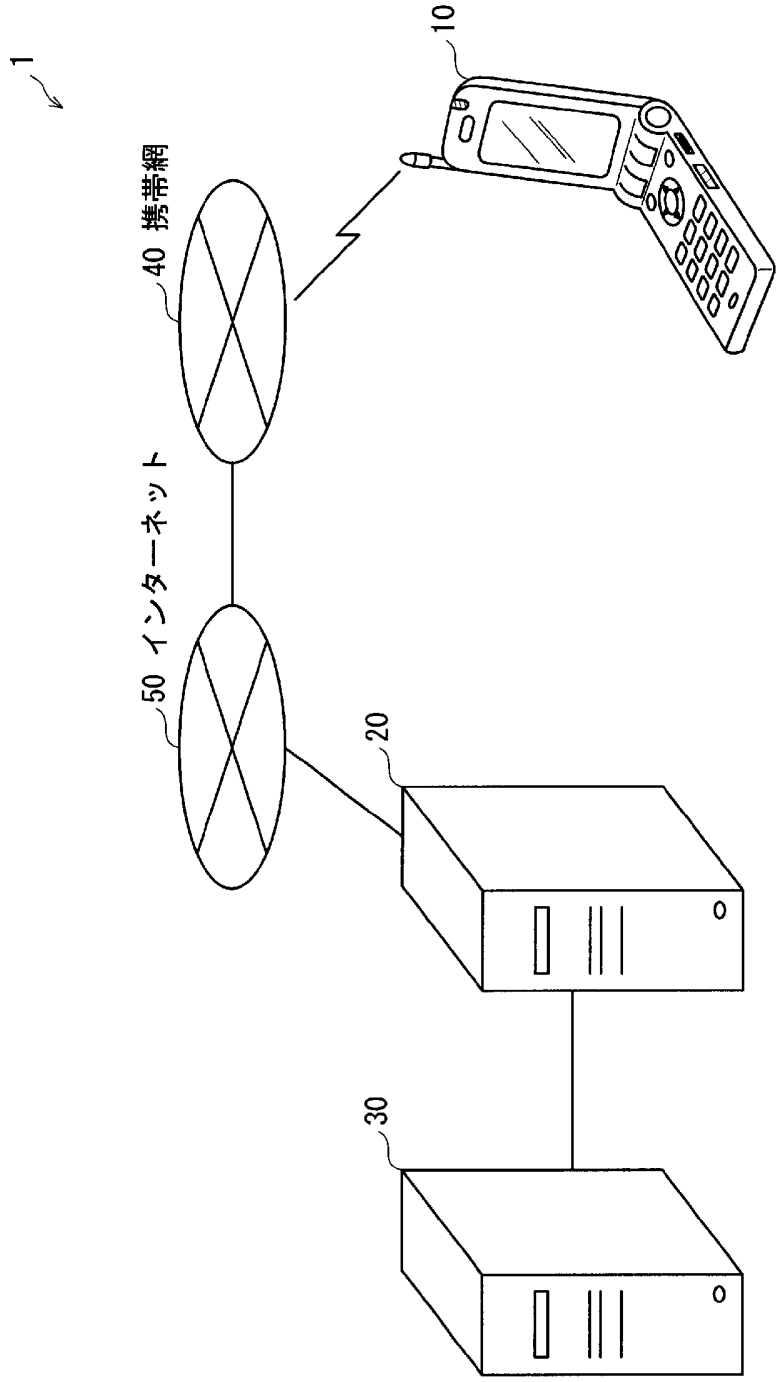
[35] (補正後)ネットワークを介して電子機器に、前記電子機器が有し、且つ1つ以上のデータからなるアプリケーションファイルの更新を行わせる更新サーバ装置の集積回路であって、

更新後のアプリケーションファイルを取得する第1取得手段と、

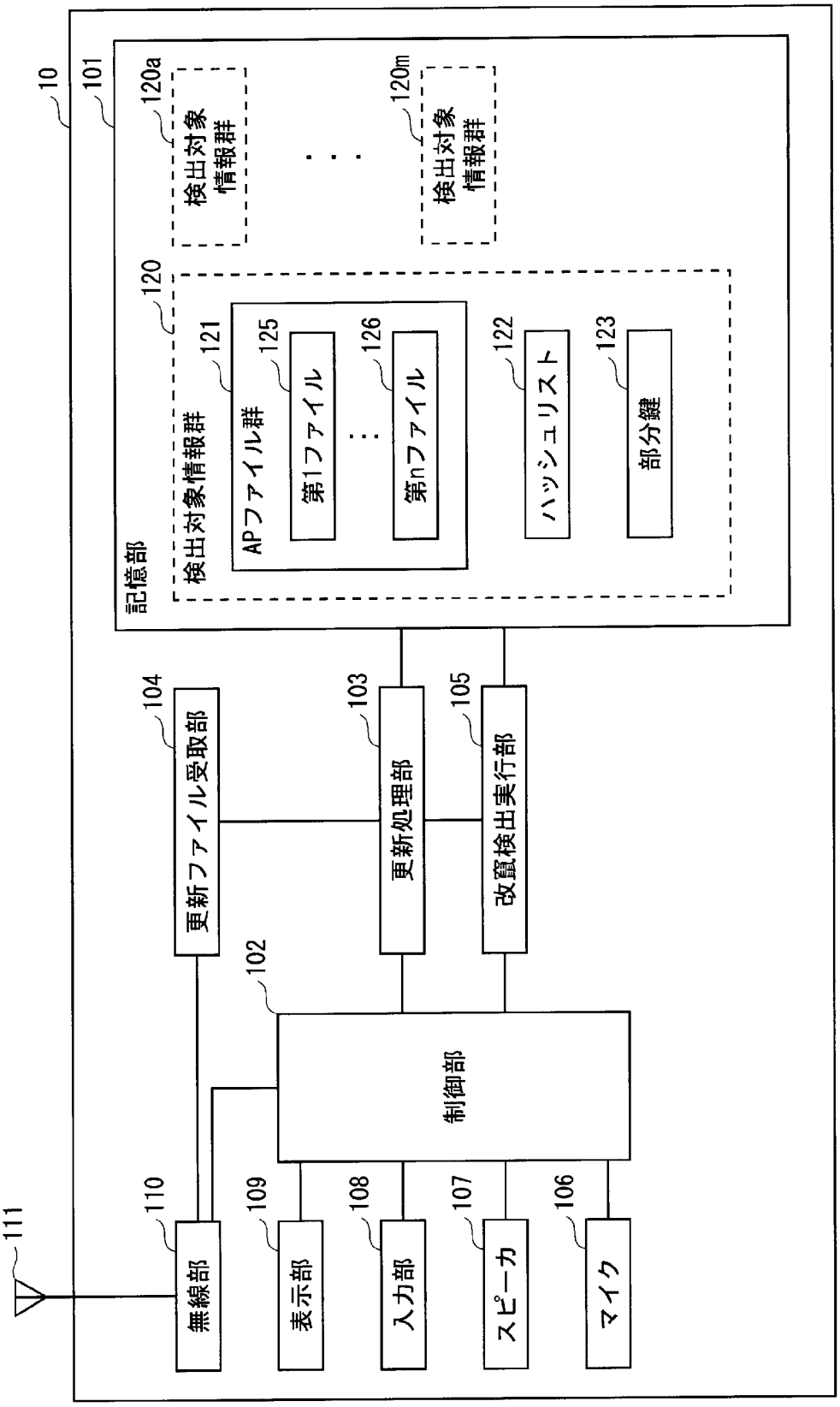
取得した前記更新後のアプリケーションファイルから更新データと、更新前のアプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを取得する第2取得手段と、

取得した前記更新データと前記位置情報とを前記電子機器へ送信する送信手段とを備えることを特徴とする集積回路。

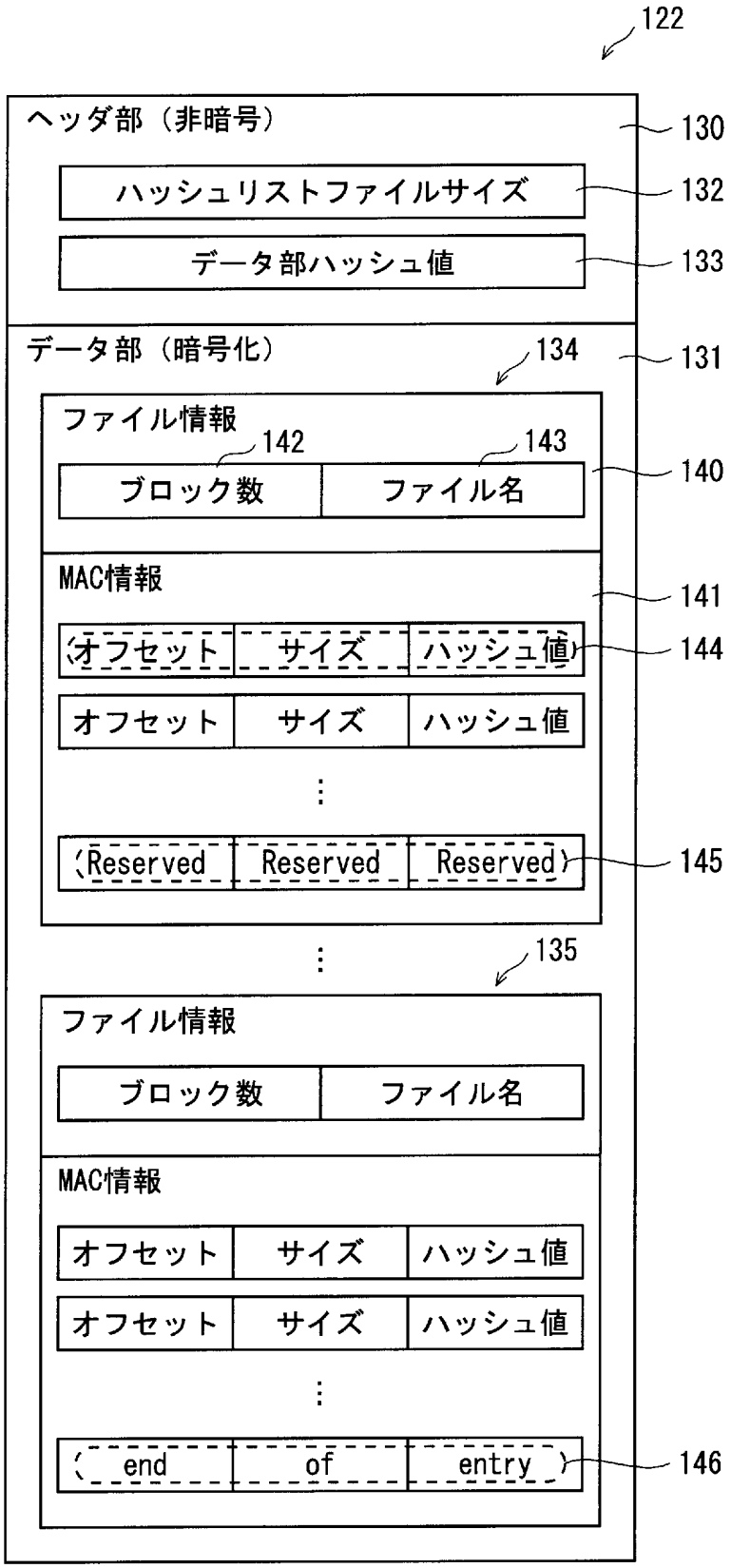
[図1]



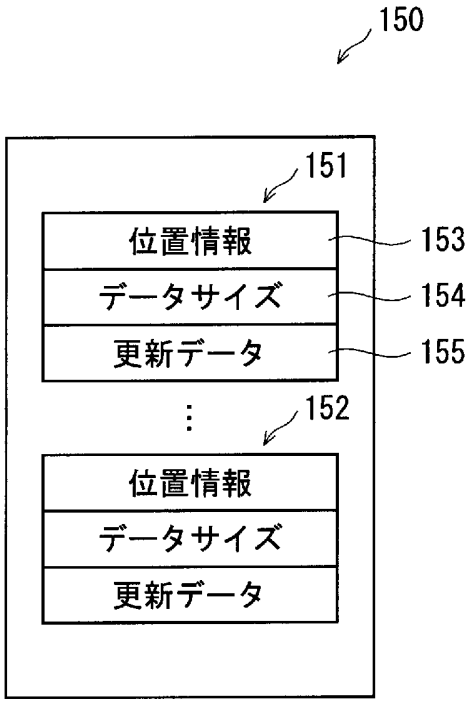
[図2]


10
101
記憶部
120
検出対象情報群
121
APファイル群
125
第1ファイル
126
第nファイル
122
ハッシュリスト
123
部分鍵
120a
検出対象情報群
120m
検出対象情報群
104
更新ファイル受取部
103
更新処理部
105
改竄検出実行部
102
制御部
110
無線部
109
表示部
108
入力部
107
スピーカ
106
マイク
111

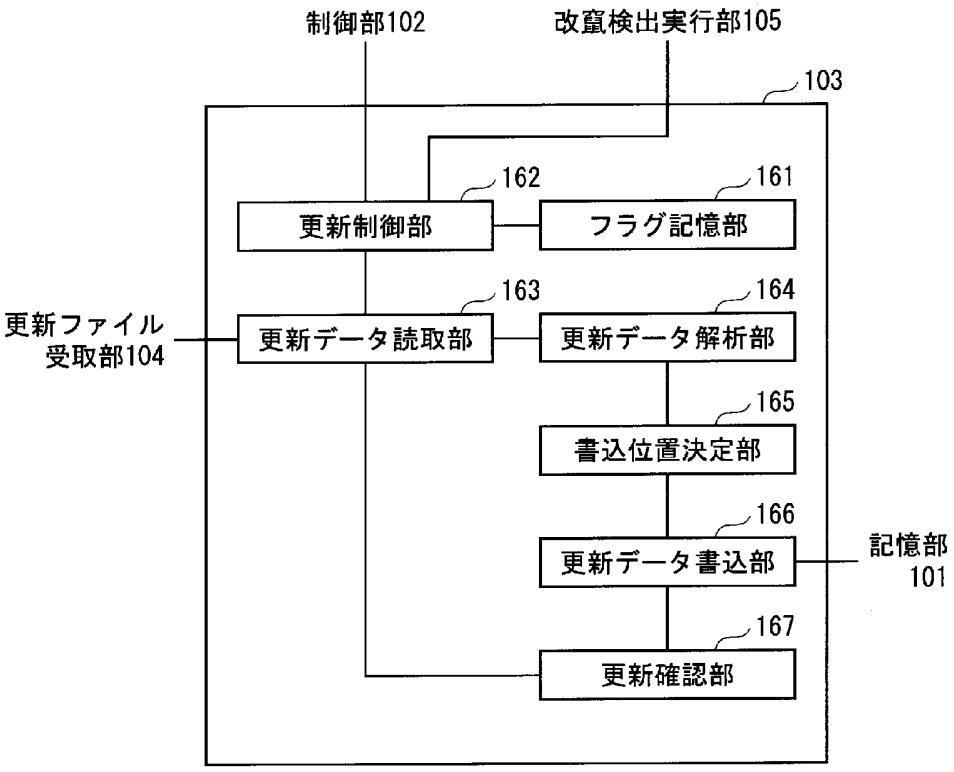
[図3]


122
ヘッダ部（非暗号）
130
ハッシュリストファイルサイズ
132
データ部ハッシュ値
133
データ部（暗号化）
134
131
ファイル情報
142
143
ブロック数
ファイル名
140
MAC情報
141
オフセット
サイズ
ハッシュ値
144
オフセット
サイズ
ハッシュ値
Reserved
Reserved
Reserved
145
135
ファイル情報
ブロック数
ファイル名
MAC情報
オフセット
サイズ
ハッシュ値
オフセット
サイズ
ハッシュ値
end
of
entry
146

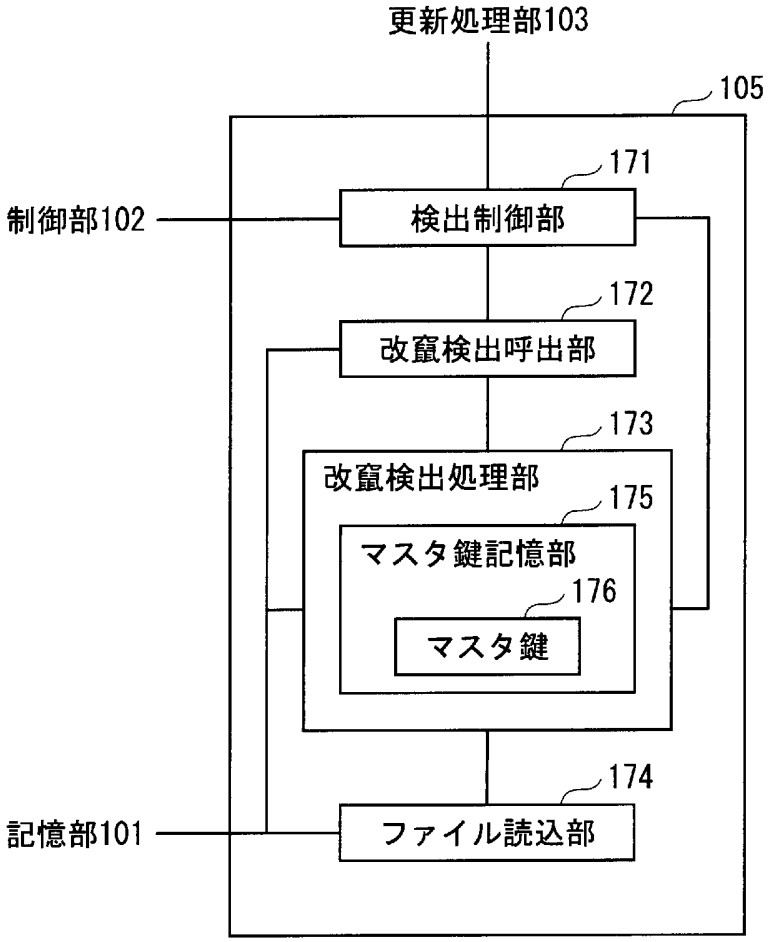
[図4]



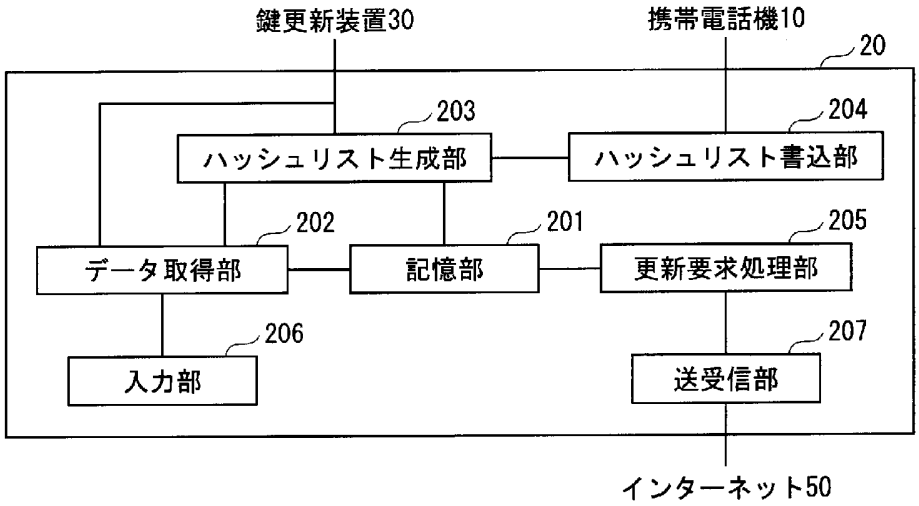
[図5]


制御部102
改竄検出実行部105
103
162
161
更新制御部
フラグ記憶部
163
164
更新ファイル
受取部104
更新データ読取部
更新データ解析部
165
書込位置決定部
166
記憶部
101
更新データ書込部
167
更新確認部

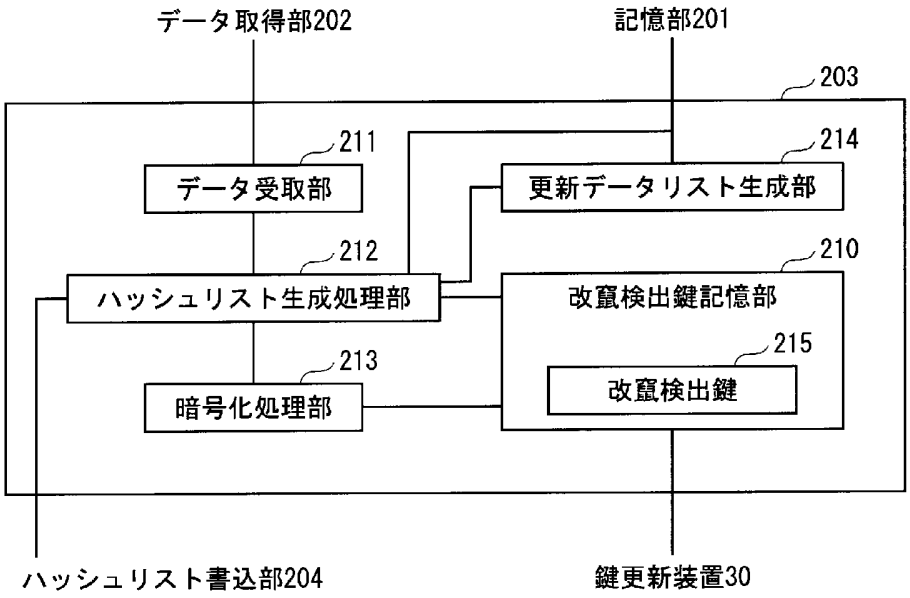
[図6]


更新処理部103
105
171
制御部102
検出制御部
172
改竄検出呼出部
173
改竄検出処理部
175
マスタ鍵記憶部
176
マスタ鍵
174
記憶部101
ファイル読込部

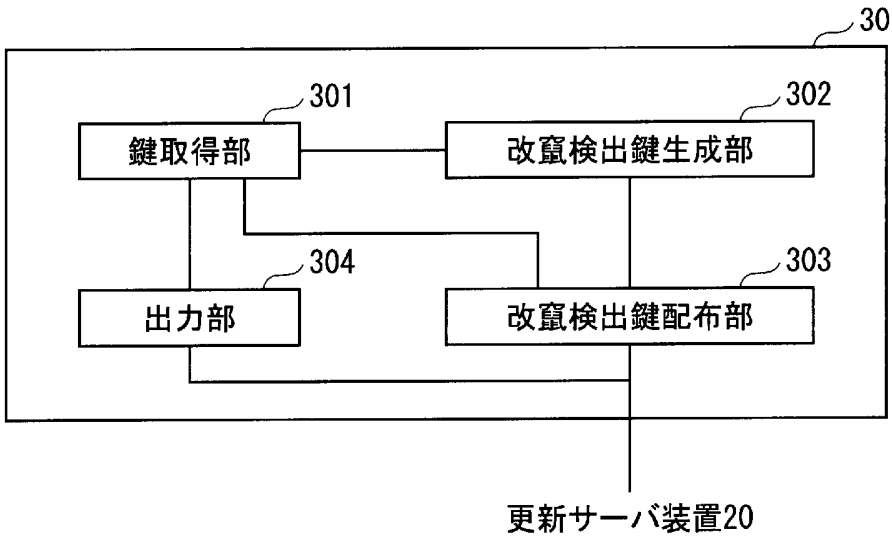
[図7]


鍵更新装置30
携帯電話機10
20
203
ハッシュリスト生成部
204
ハッシュリスト書込部
202
201
205
データ取得部
記憶部
更新要求処理部
206
207
入力部
送受信部
インターネット50

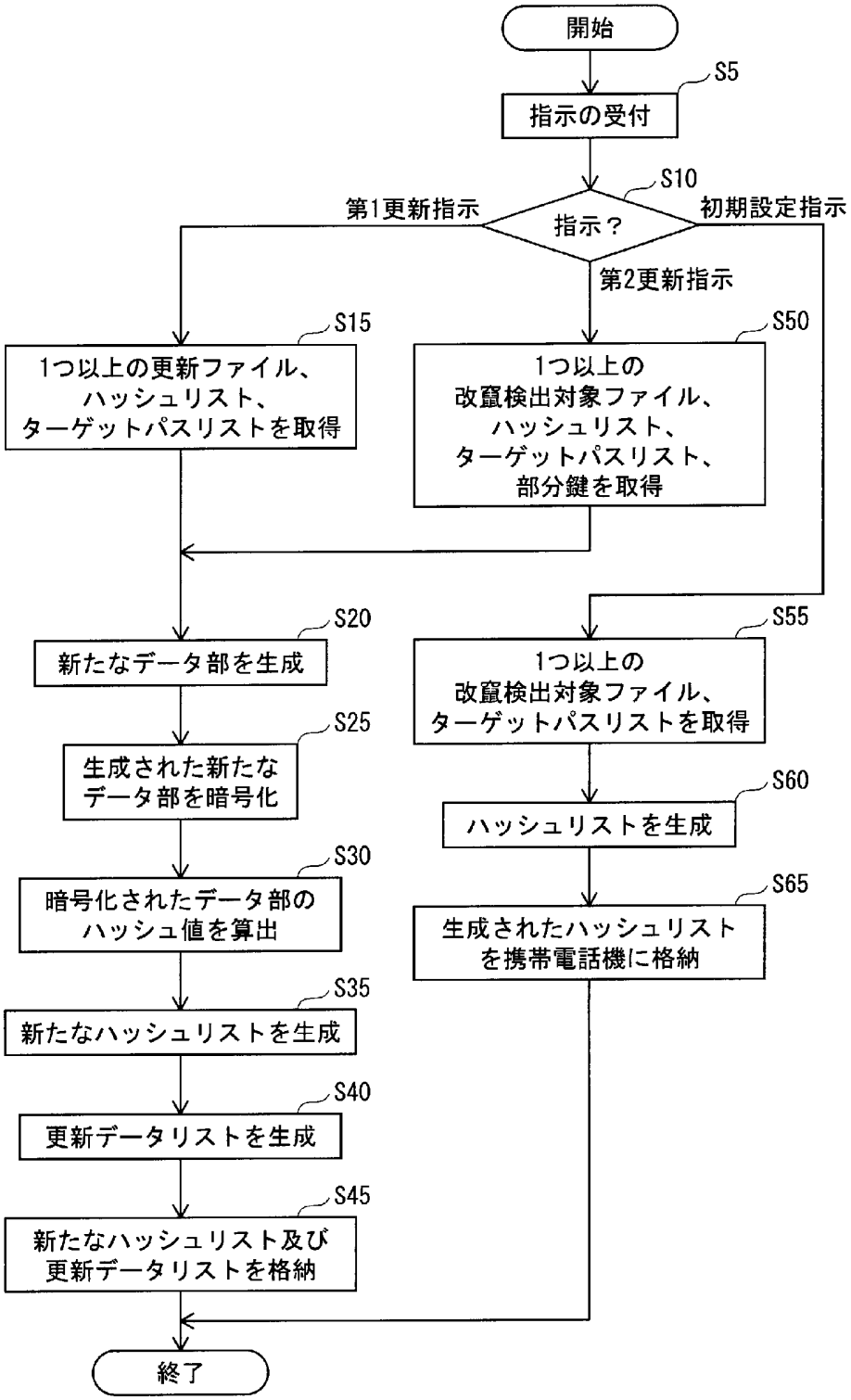
[図8]


データ取得部202
記憶部201
203
211
データ受取部
214
更新データリスト生成部
212
ハッシュリスト生成処理部
210
改竄検出鍵記憶部
215
改竄検出鍵
213
暗号化処理部
ハッシュリスト書込部204
鍵更新装置30

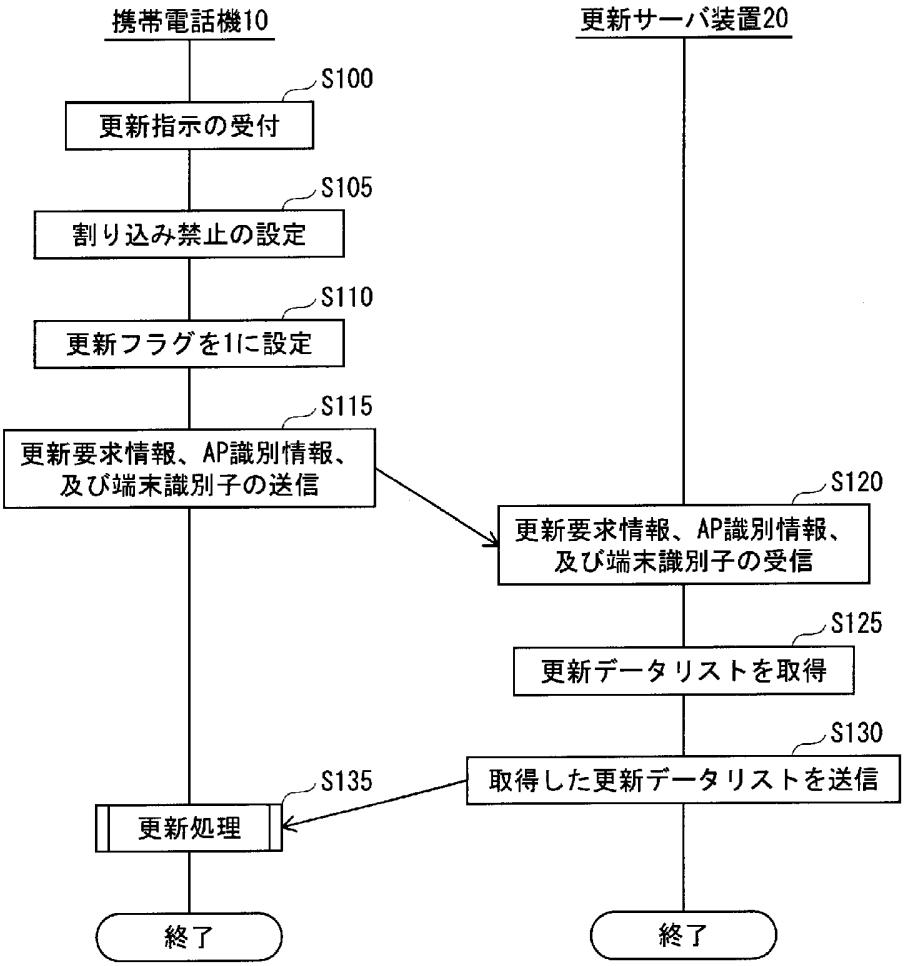
[図9]



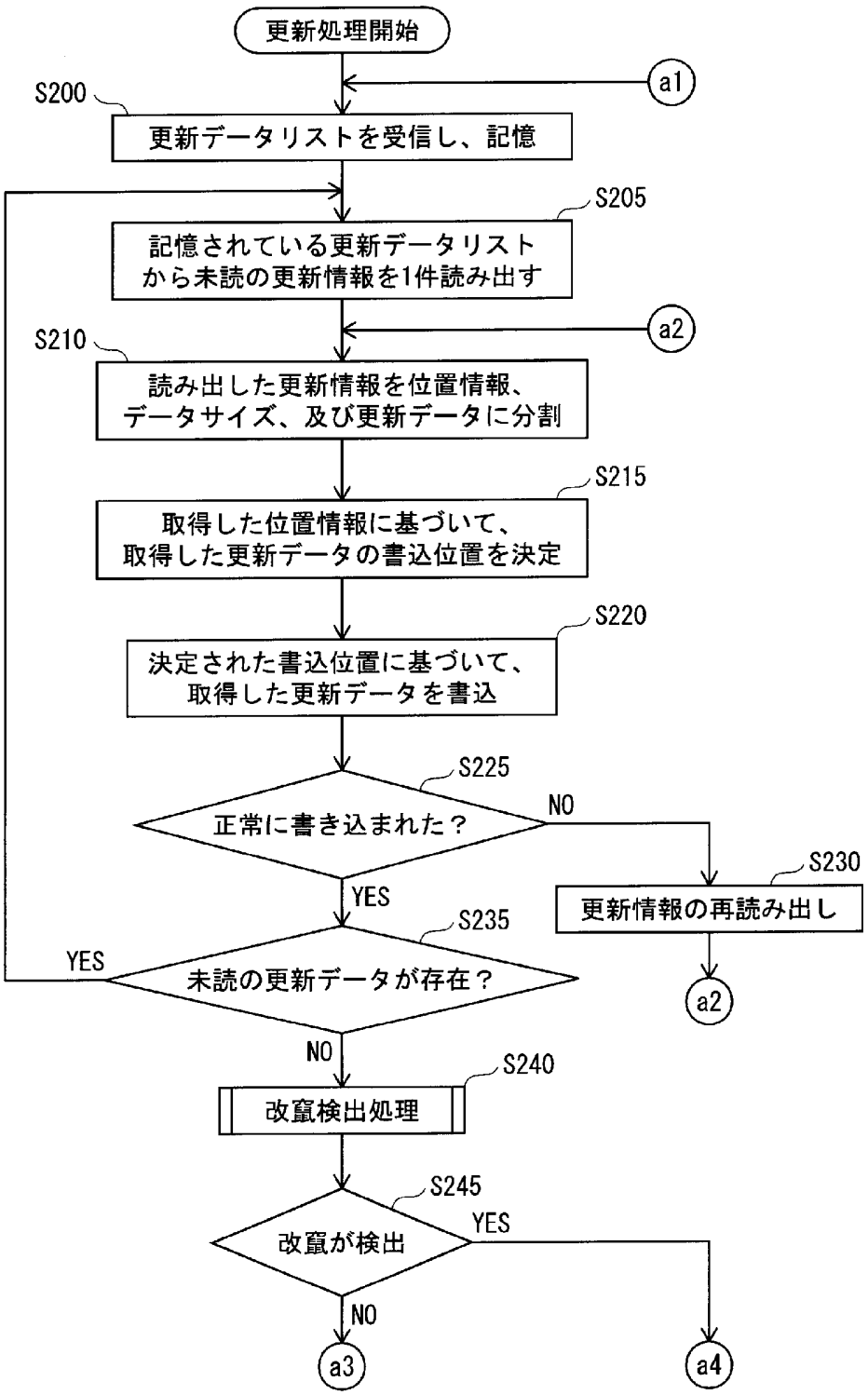
[図10]


開始
S5
指示の受付
S10
指示？
第1更新指示
初期設定指示
第2更新指示
S15
1つ以上の更新ファイル、
ハッシュリスト、
ターゲットパスリストを取得
S50
1つ以上の
改竄検出対象ファイル、
ハッシュリスト、
ターゲットパスリスト、
部分鍵を取得
S20
新たなデータ部を生成
S25
生成された新たな
データ部を暗号化
S30
暗号化されたデータ部の
ハッシュ値を算出
S35
新たなハッシュリストを生成
S40
更新データリストを生成
S45
新たなハッシュリスト及び
更新データリストを格納
S55
1つ以上の
改竄検出対象ファイル、
ターゲットパスリストを取得
S60
ハッシュリストを生成
S65
生成されたハッシュリスト
を携帯電話機に格納
終了

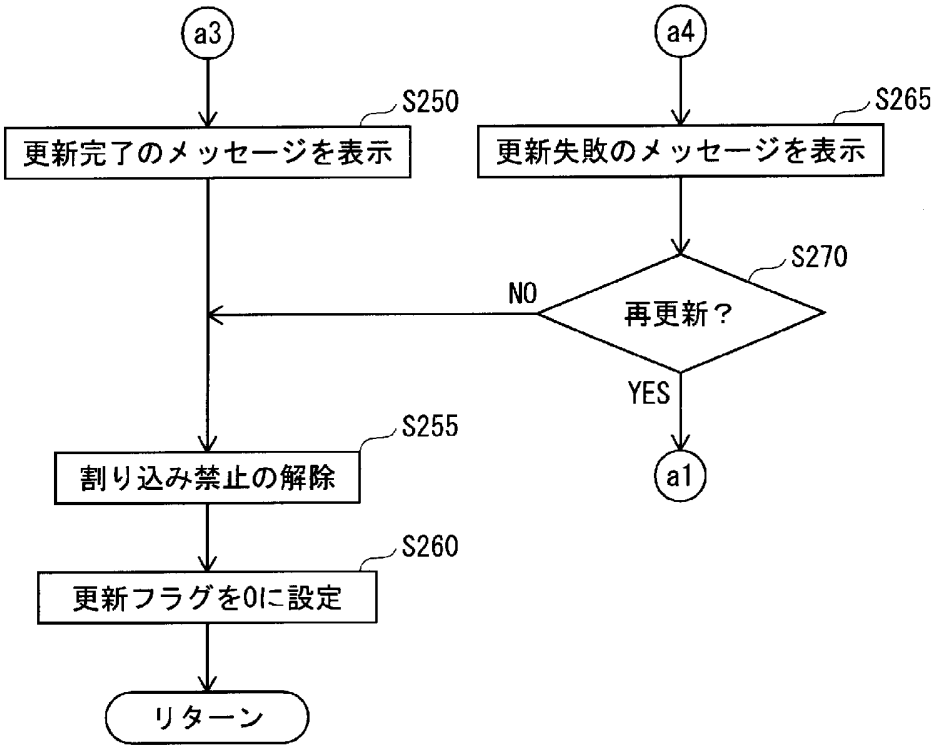
[図11]


携帯電話機10
更新サーバ装置20
S100
更新指示の受付
S105
割り込み禁止の設定
S110
更新フラグを1に設定
S115
更新要求情報、AP識別情報、
及び端末識別子の送信
S120
更新要求情報、AP識別情報、
及び端末識別子の受信
S125
更新データリストを取得
S130
取得した更新データリストを送信
S135
更新処理
終了
終了

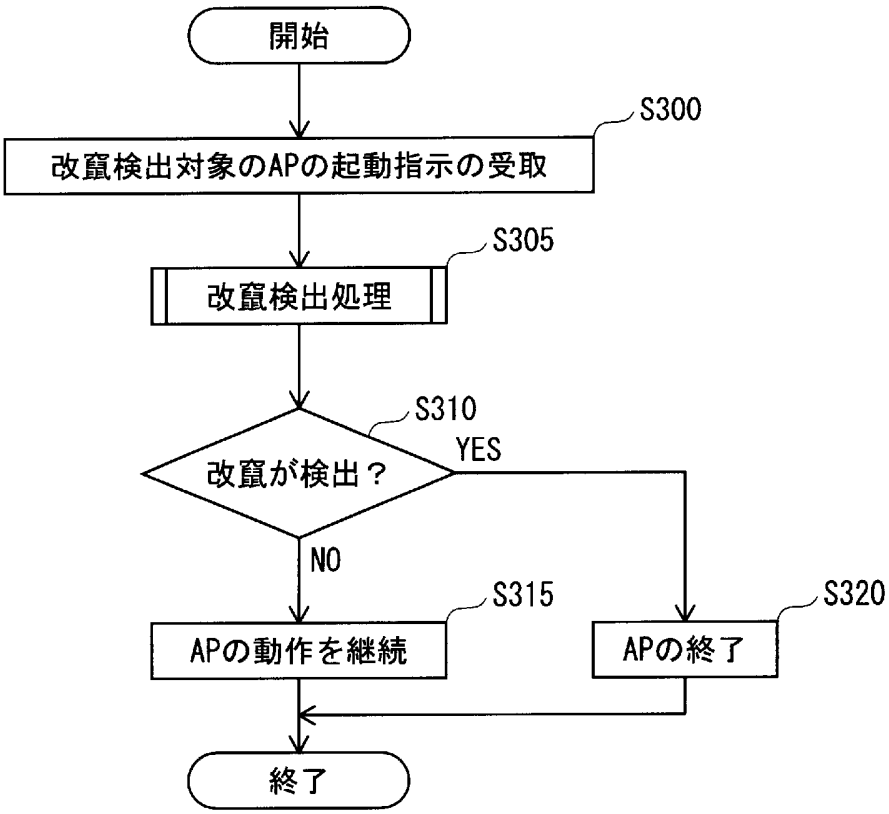
[図12]


更新処理開始
a1
S200
更新データリストを受信し、記憶
S205
記憶されている更新データリスト
から未読の更新情報を1件読み出す
a2
S210
読み出した更新情報を位置情報、
データサイズ、及び更新データに分割
S215
取得した位置情報に基づいて、
取得した更新データの書込位置を決定
S220
決定された書込位置に基づいて、
取得した更新データを書込
S225
正常に書き込まれた？
NO
S230
更新情報の再読み出し
a2
YES
S235
未読の更新データが存在？
YES
NO
S240
改竄検出処理
S245
改竄が検出
YES
NO
a3
a4

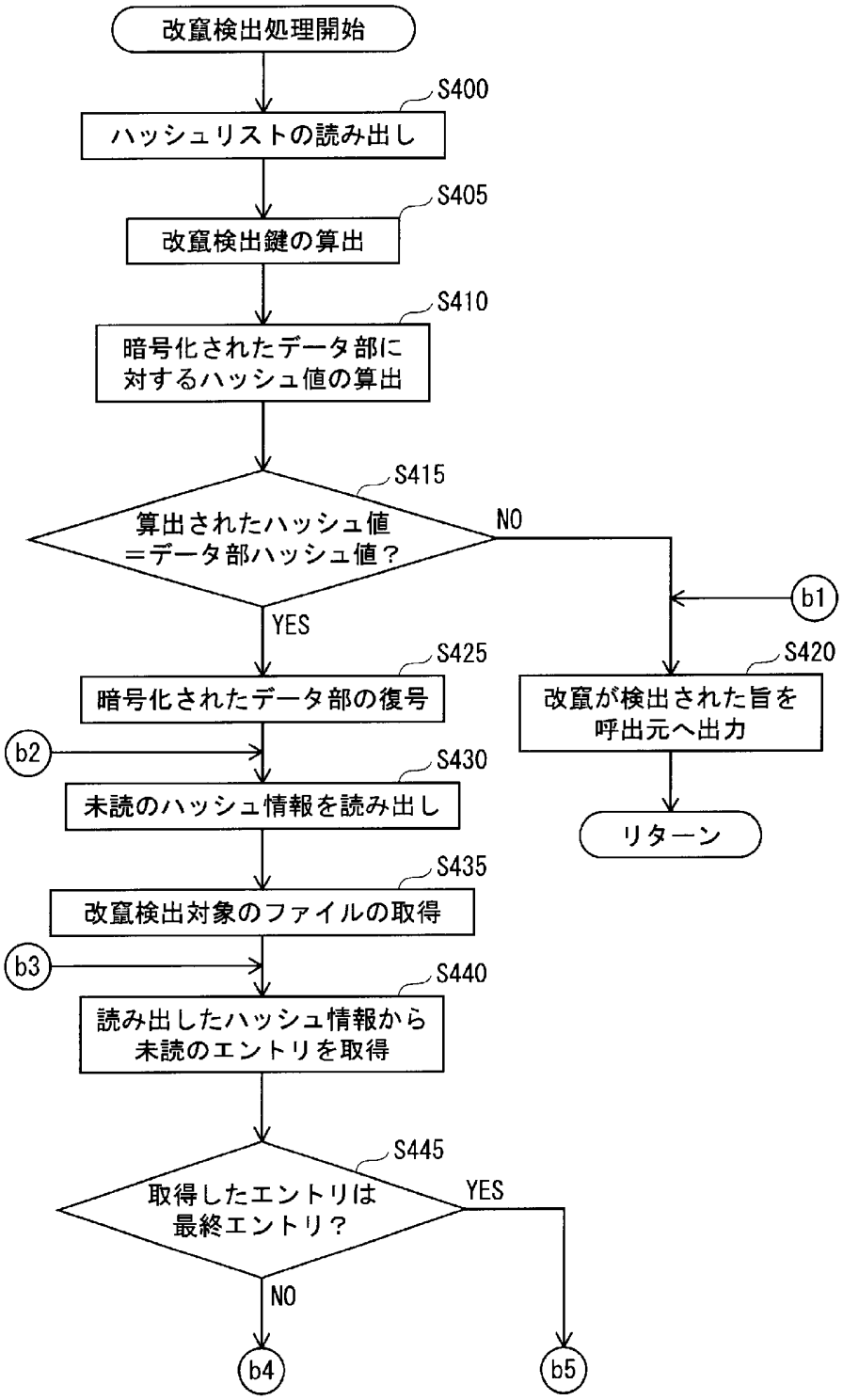
[図13]


a3
a4
S250
更新完了のメッセージを表示
S265
更新失敗のメッセージを表示
S270
NO
再更新？
YES
S255
割り込み禁止の解除
a1
S260
更新フラグを0に設定
リターン

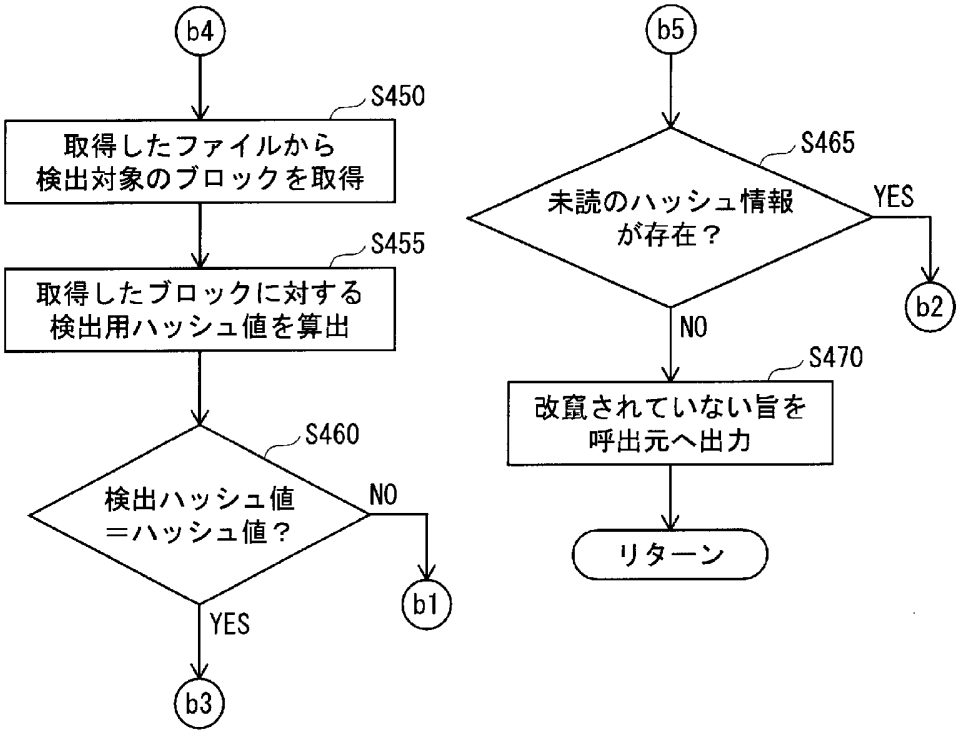
[図14]


開始
S300
改竄検出対象のAPの起動指示の受取
S305
改竄検出処理
S310
改竄が検出？
YES
NO
S315
APの動作を継続
S320
APの終了
終了

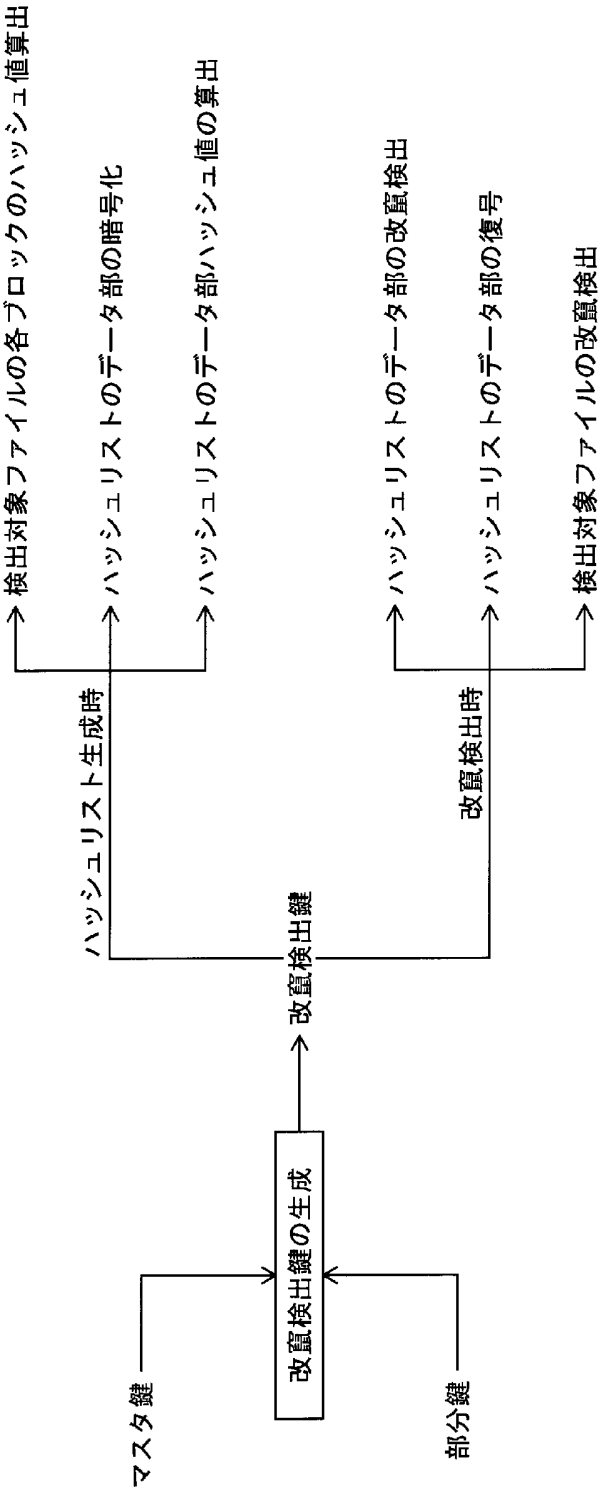
[図15]


改竄検出処理開始
S400
ハッシュリストの読み出し
S405
改竄検出鍵の算出
S410
暗号化されたデータ部に
対するハッシュ値の算出
S415
算出されたハッシュ値
＝データ部ハッシュ値？
NO
YES
b1
S420
改竄が検出された旨を
呼出元へ出力
リターン
S425
暗号化されたデータ部の復号
b2
S430
未読のハッシュ情報を読み出し
S435
改竄検出対象のファイルの取得
b3
S440
読み出したハッシュ情報から
未読のエントリを取得
S445
取得したエントリは
最終エントリ？
YES
NO
b4
b5

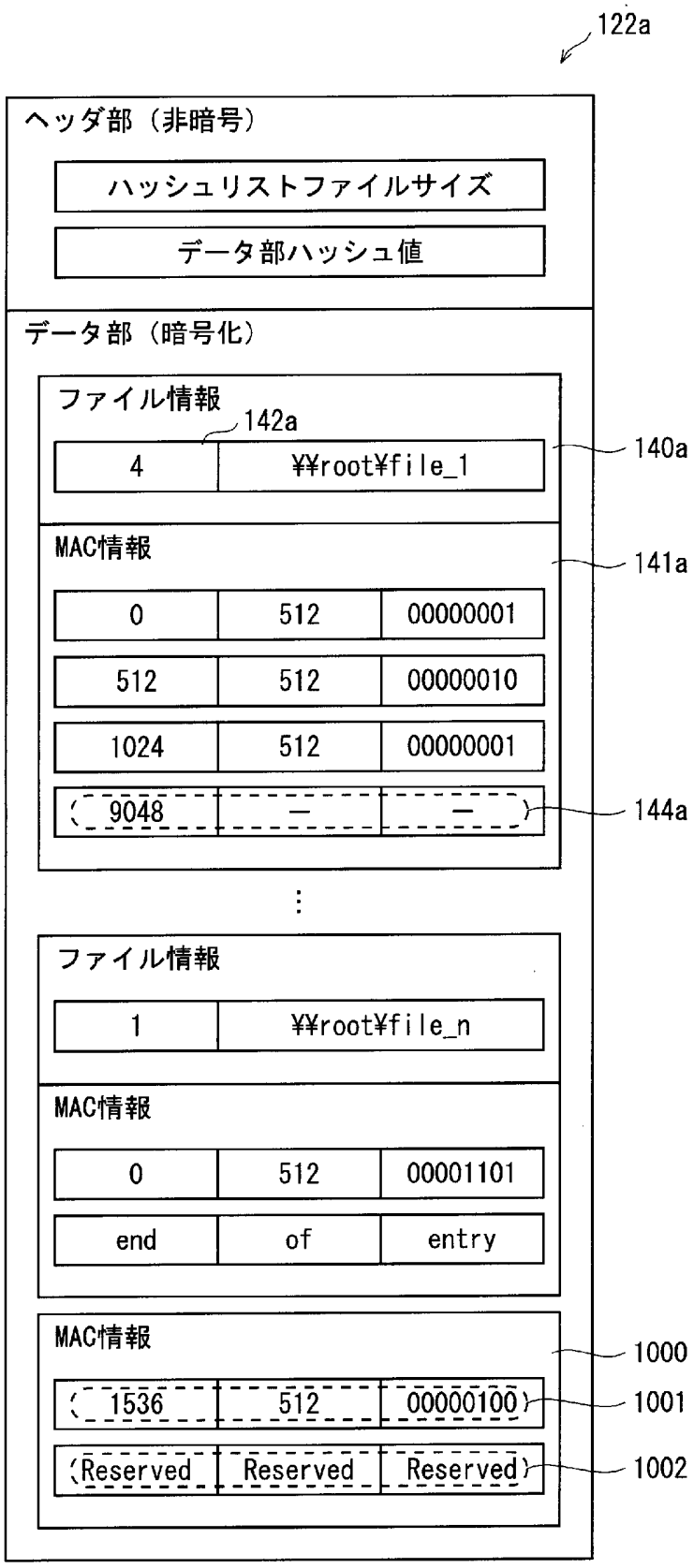
[図16]


b4
S450
取得したファイルから
検出対象のブロックを取得
S455
取得したブロックに対する
検出用ハッシュ値を算出
S460
検出ハッシュ値
＝ハッシュ値？
NO
b1
YES
b3
b5
S465
未読のハッシュ情報
が存在？
YES
b2
NO
S470
改竄されていない旨を
呼出元へ出力
リターン

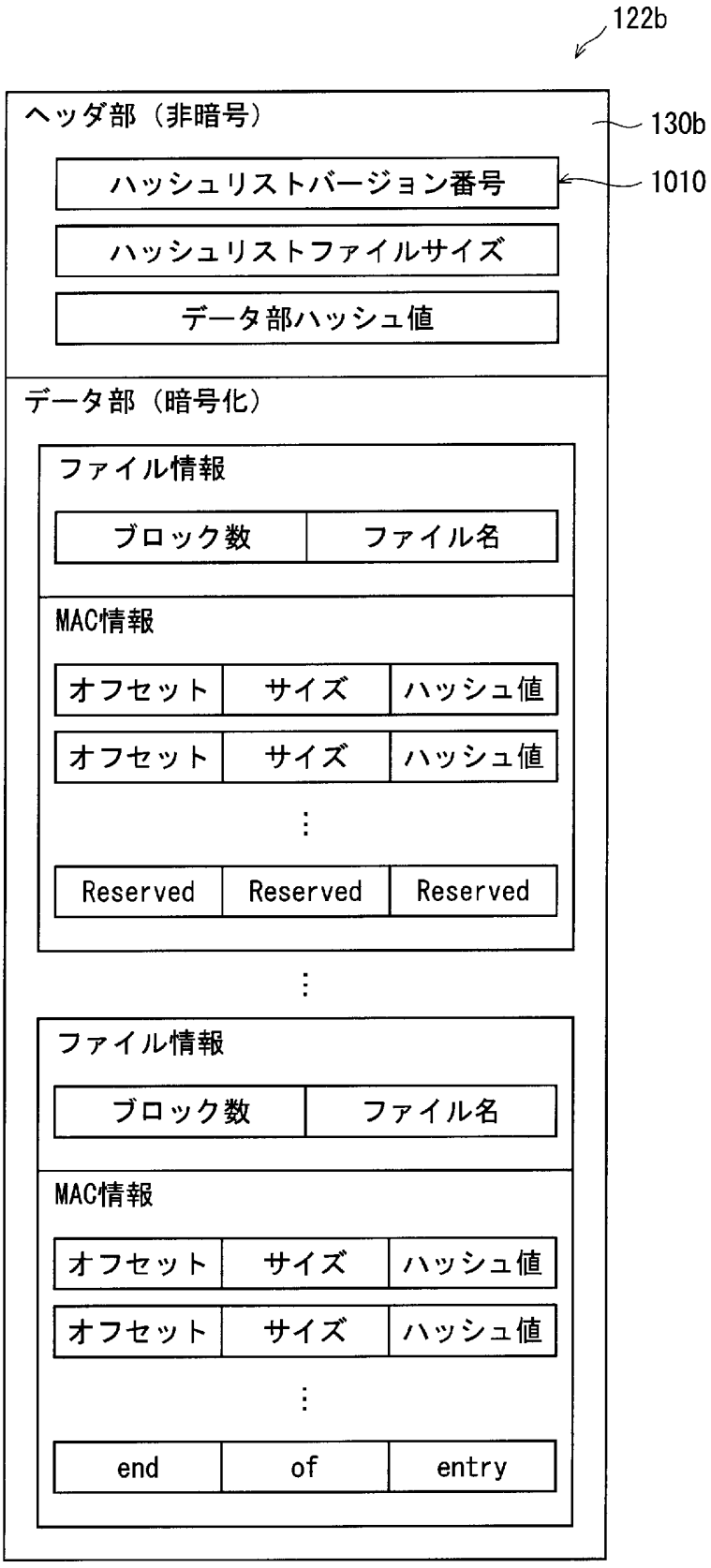
[図17]


マスタ鍵
部分鍵
改竄検出鍵の生成
改竄検出鍵
ハッシュリスト生成時
改竄検出時
検出対象ファイルの各ブロックのハッシュ値算出
ハッシュリストのデータ部の暗号化
ハッシュリストのデータ部ハッシュ値の算出
ハッシュリストのデータ部の改竄検出
ハッシュリストのデータ部の復号
検出対象ファイルの改竄検出

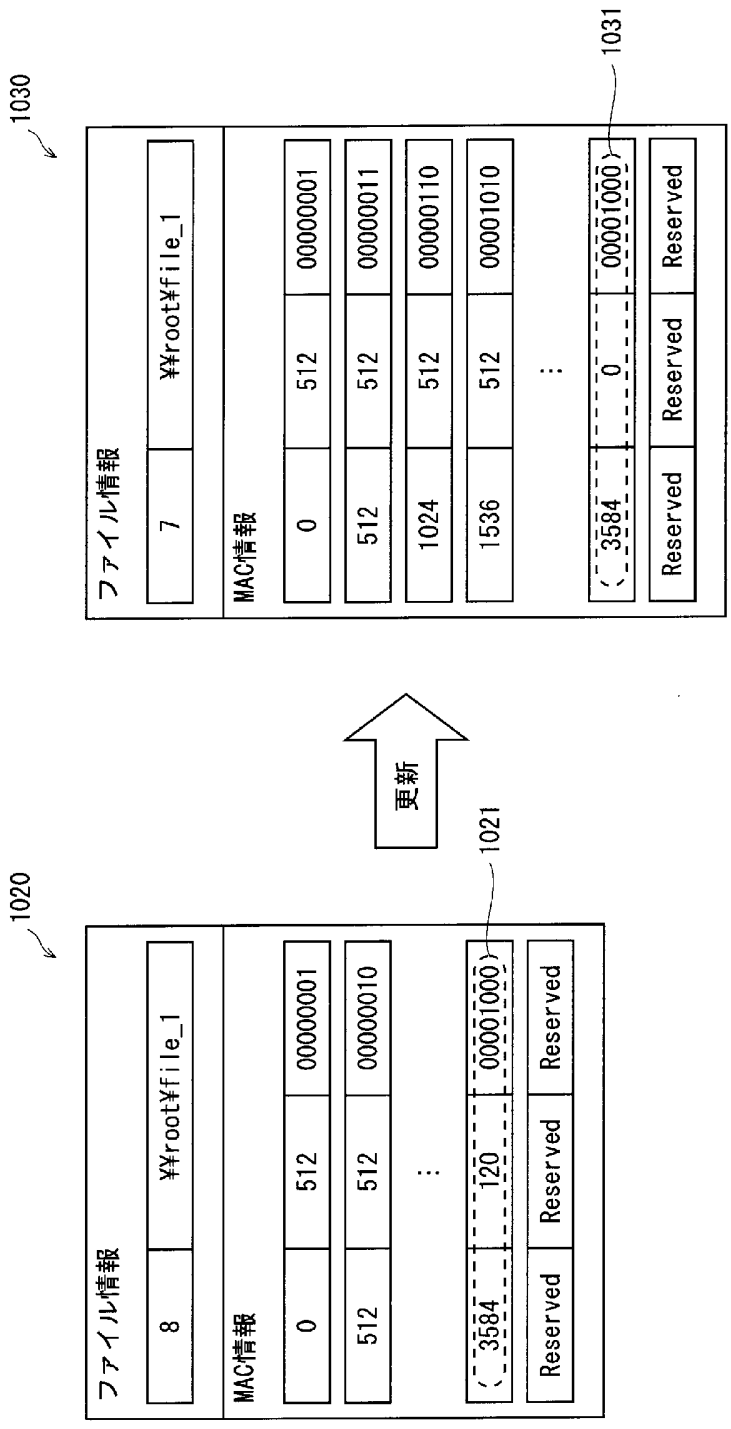
[図18]


122a
ヘッダ部（非暗号）
ハッシュリストファイルサイズ
データ部ハッシュ値
データ部（暗号化）
ファイル情報
142a
4
¥¥root¥file_1
140a
MAC情報
141a
0
512
00000001
512
512
00000010
1024
512
00000001
9048
—
—
144a
ファイル情報
1
¥¥root¥file_n
MAC情報
0
512
00001101
end
of
entry
MAC情報
1000
1536
512
00000100
1001
Reserved
Reserved
Reserved
1002

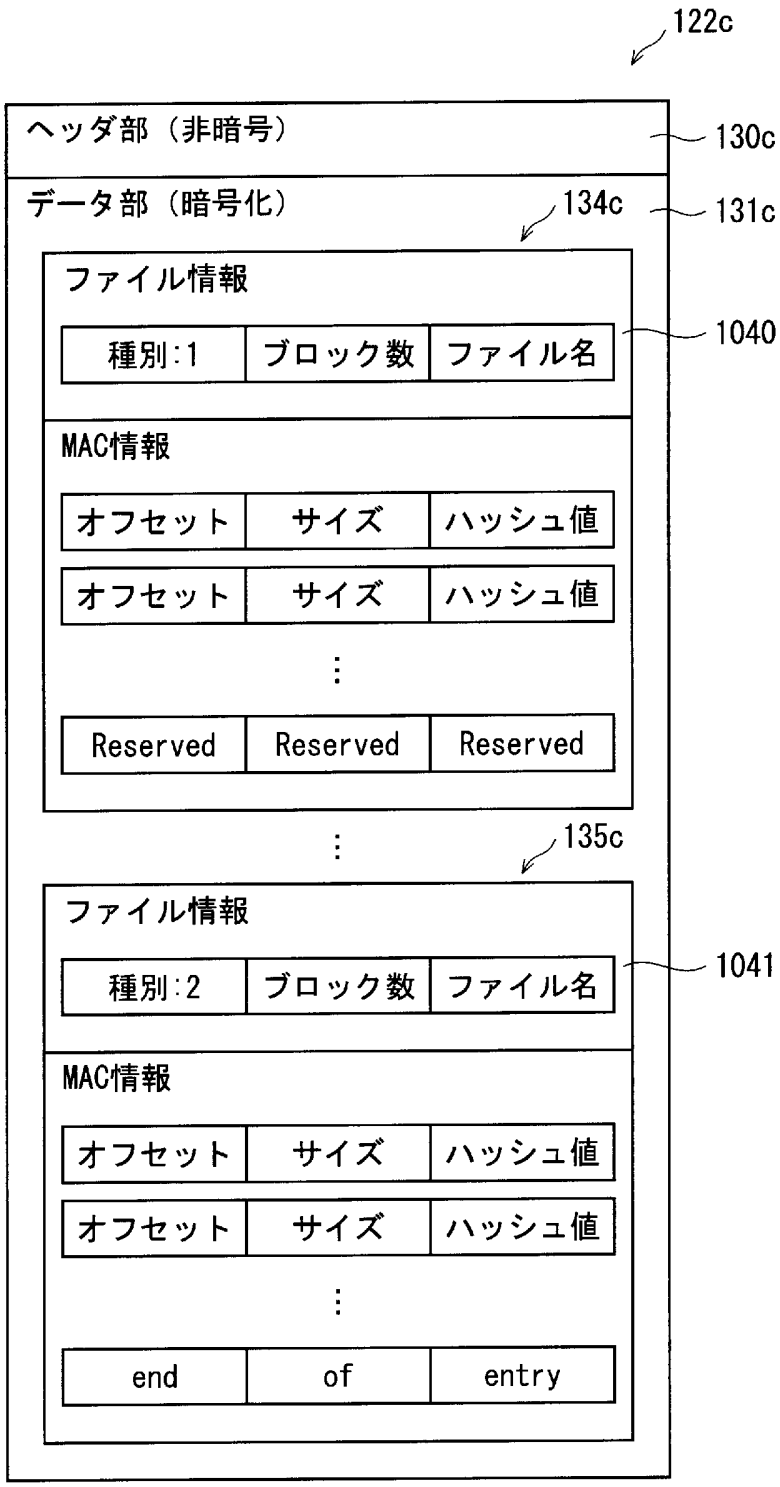
[図19]


122b
ヘッダ部（非暗号）
130b
ハッシュリストバージョン番号
1010
ハッシュリストファイルサイズ
データ部ハッシュ値
データ部（暗号化）
ファイル情報
ブロック数
ファイル名
MAC情報
オフセット
サイズ
ハッシュ値
オフセット
サイズ
ハッシュ値
Reserved
Reserved
Reserved
ファイル情報
ブロック数
ファイル名
MAC情報
オフセット
サイズ
ハッシュ値
オフセット
サイズ
ハッシュ値
end
of
entry

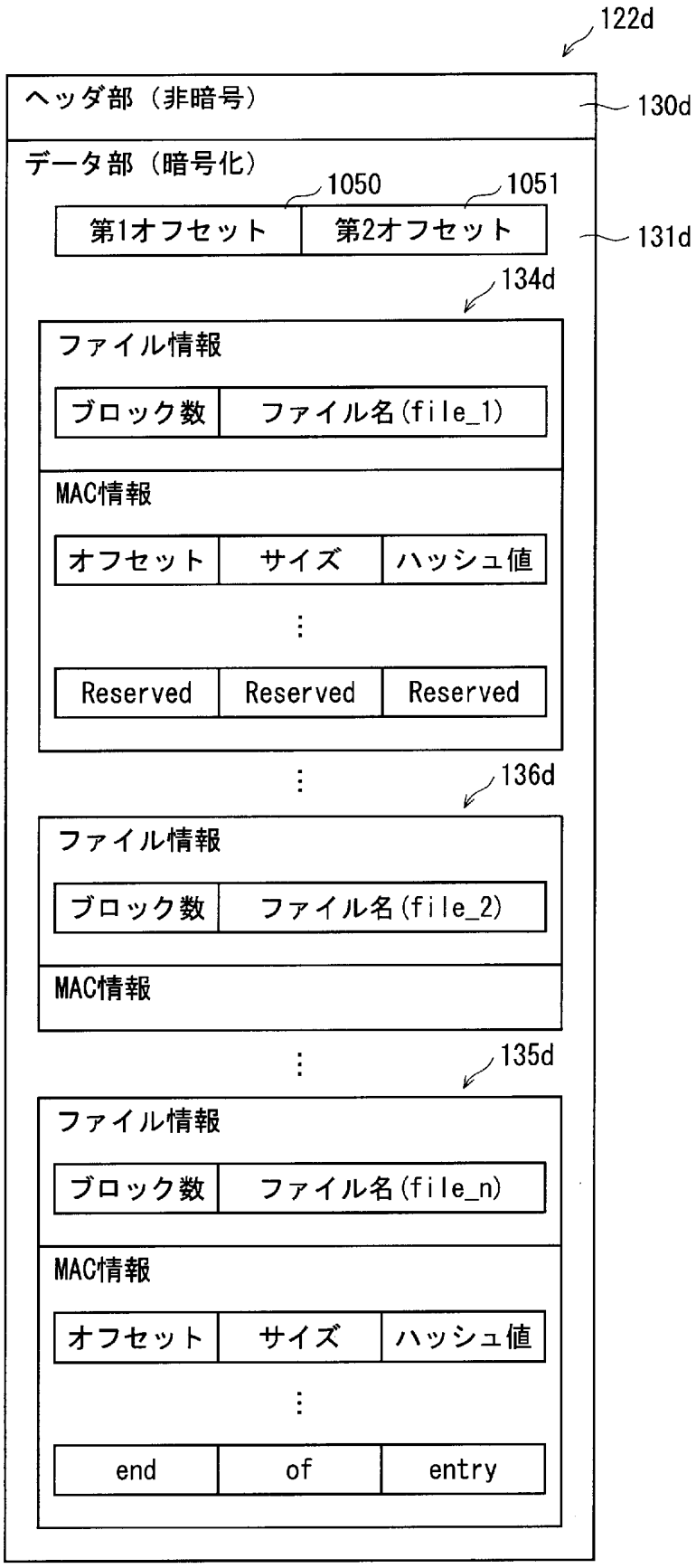
[図20]


1030
1031
ファイル情報
7
¥¥root¥file_1
MAC情報
0
512
00000001
512
512
00000011
1024
512
00000110
1536
512
00001010
3584
0
00001000
Reserved
Reserved
Reserved
更新
1020
1021
ファイル情報
8
¥¥root¥file_1
MAC情報
0
512
00000001
512
512
00000010
3584
120
00001000
Reserved
Reserved
Reserved

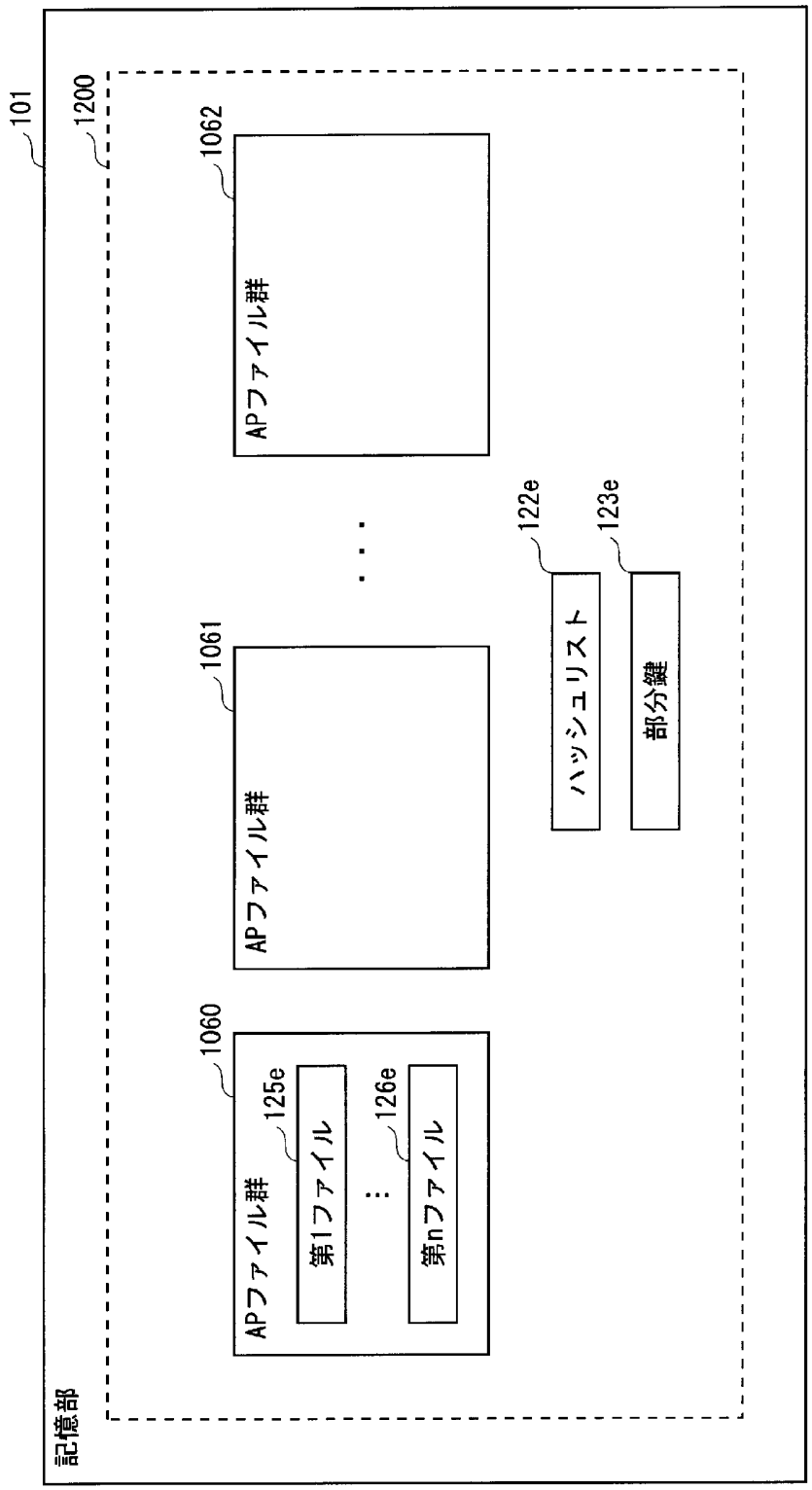
[図21]


122c
ヘッダ部（非暗号）
130c
データ部（暗号化）
131c
134c
ファイル情報
種別:1
ブロック数
ファイル名
1040
MAC情報
オフセット
サイズ
ハッシュ値
オフセット
サイズ
ハッシュ値
Reserved
Reserved
Reserved
135c
ファイル情報
種別:2
ブロック数
ファイル名
1041
MAC情報
オフセット
サイズ
ハッシュ値
オフセット
サイズ
ハッシュ値
end
of
entry

[図22]


122d
ヘッダ部（非暗号）
130d
データ部（暗号化）
1050
1051
第1オフセット
第2オフセット
131d
134d
ファイル情報
ブロック数
ファイル名(file_1)
MAC情報
オフセット
サイズ
ハッシュ値
Reserved
Reserved
Reserved
136d
ファイル情報
ブロック数
ファイル名(file_2)
MAC情報
135d
ファイル情報
ブロック数
ファイル名(file_n)
MAC情報
オフセット
サイズ
ハッシュ値
end
of
entry

[図23]


101
記憶部
1200
1060
APファイル群
125e
第1ファイル
126e
第nファイル
1061
APファイル群
1062
APファイル群
122e
ハッシュリスト
123e
部分鍵

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/310764

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01), ***G06F11/00***(2006.01), ***G06F12/00***(2006.01), ***G06F13/00***(2006.01), ***G06F21/22***(2006.01), ***H04L9/32***(2006.01)

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)
G06F21/24(2006.01), ***G06F11/00***(2006.01), ***G06F12/00***(2006.01), ***G06F13/00***(2006.01), ***G06F21/22***(2006.01), ***H04L9/32***(2006.01)

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 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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.
X Y	JP 2005-515534 A (Telefonaktiebolaget LM Ericsson), 26 May, 2005 (26.05.05), Par. Nos. [0016], [0019], [0030] to [0032], [0048], [0053] to [0054], [0060] & WO 2003/060673 A1 & US 2005/0091501 A1	1-8,11-18, 28-35 9-10,19-27
Y	JP 2002-16565 A (Toshiba Corp.), 18 January, 2002 (18.01.02), Par. No. [0039] (Family: none)	9-10,19-27

☐ 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	Date of mailing of the international search report
29 June, 2006 (29.06.06)	11 July, 2006 (11.07.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/310764

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature common to the inventions of claims 1, 17 relate to use of position information indicating a position to be updated upon update of an application file. This feature cannot be a special technical feature since it is disclosed in JP 2005-515534 A (Telefonaktiebolaget LM Ericsson) 26 May, 2005 (26.05.05). Accordingly, there is no technical relationship between claims 1 and 17 involving one or more of the same or corresponding special technical feature. Moreover, the inventions of claims 26-27 relate to a key generation.
(Continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee..

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

It is apparent that there is no technical relationship between claims 26-27 and claims 1, 17 involving special technical features.

Accordingly, this application includes at least three groups of inventions.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１０７６４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*G06F21/24(2006.01), G06F11/00(2006.01), G06F12/00(2006.01), G06F13/00(2006.01), G06F21/22(2006.01), H04L9/32(2006.01)*

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.　*G06F21/24(2006.01), G06F11/00(2006.01), G06F12/00(2006.01), G06F13/00(2006.01), G06F21/22(2006.01), H04L9/32(2006.01)*

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	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６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
X Y	JP 2005-515534 A （テレフォンアクチーボラゲット　エル　エム　エリクソン） 2005.05.26,【0016】,【0019】,【0030】－【0032】,【0048】,【0053】－【0054】,【0060】& WO 2003/060673 A1 & US 2005/0091501 A1	1-8,11-18,28-35 9-10,19-27
Y	JP 2002-16565 A （株式会社東芝） 2002.01.18, 【0039】（ファミリーなし）	9-10,19-27

☐　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 ２９．０６．２００６	国際調査報告の発送日 １１．０７．２００６
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　９０７１ 平井　誠 電話番号　０３－３５８１－１１０１　内線　３５４６

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１０７６４

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１，１７に共通する技術事項である、アプリケーションファイルの更新の際に更新する位置を示す位置情報を採用することは、JP 2005-515534 A （テレフォンアクチーボラゲット　エル　エム　エリクソン）　2005.05.26の記載からみて特別な技術的特徴とはいえない。したがって請求の範囲１，１７は一又は二以上の同一又は対応する特別な技術的特徴を含む技術的な関係にない。また、請求の範囲２６－２７は鍵生成に関するものであり、請求の範囲１，１７と明らかに特別な技術的特徴を含む技術的な関係にない。

したがって、この出願の発明の数は少なくとも３である。

１．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

２．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付を伴う異議申立てがなかった。