(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
2012 年 5 月 3 日(03.05.2012)

PCT

(10) 国際公開番号
WO 2012/056656 A1

(51) 国際特許分類:
G06F 21/22 (2006.01) *G06F 21/24* (2006.01)

(21) 国際出願番号: PCT/JP2011/005858

(22) 国際出願日: 2011 年 10 月 19 日(19.10.2011)

(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 2010-241986 2010 年 10 月 28 日(28.10.2010) 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): 海上 勇二 (UNAGAMI, Yuji). 布田 裕一 (FUTA, Yuichi). 松崎 なつめ (MATSUZAKI, Natsume). 静谷 啓樹 (SHIZUYA, Hiroki). 小泉 英介 (KOIZUMI, Eisuke). 長谷川 真吾 (HASEGAWA, Shingo).

(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, CL, 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, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, 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 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

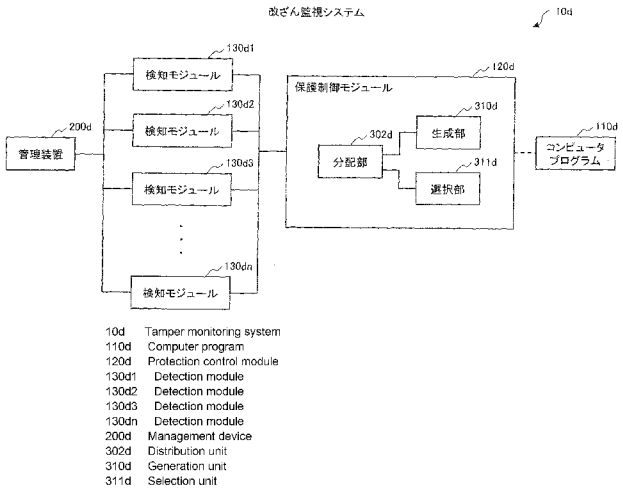
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: TAMPER MONITORING SYSTEM, PROTECTION CONTROL MODULE AND DETECTION MODULE

(54) 発明の名称 : 改ざん監視システム、保護制御モジュール及び検知モジュール

[図40]



(57) **Abstract**: In the present invention, tamper detection of a protection-control module can be performed even if some detection modules have been tampered with. A tamper monitoring system (10d) comprises a protection control module (120d), n detection modules and a management device (200d). The protection control module (120d) is provided with the following units that operate on the basis of a computer program: a generation unit (310d) that generates d sets of distribution data (d being less than n); a selection unit (311d) that selects d detection modules; and a distribution unit (302d) that distributes the generated d sets of distribution data to each of the d detection modules. The d detection modules determine whether the distribution data they received is correct, detect tampering with the protection control module and transmit determination results. The management device (200d), on the basis of the determination results, manages tampering with the protection control module (120d).

(57) 要約:

[続葉有]

WO 2012/056656 A1

一部の検知モジュールが改ざんされている場合も、保護制御モジュールの改ざん検出を行うことができる。改ざん監視システム１０ｄは、保護制御モジュール１２０ｄ、ｎ個の検知モジュール及び管理装置２００ｄを含む。保護制御モジュール１２０ｄは、コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成部３１０ｄ、ｄ個の検知モジュールを選択する選択部３１１ｄ及び生成したｄ個の前記分配データを各々ｄ個の検知モジュールへ分配する分配部３０２ｄを備える。ｄ個の各検知モジュールは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出し、判断結果を送信する。管理装置２００ｄは、判断結果を基にして、保護制御モジュール１２０ｄの改ざんを管理する。

明　細　書

発明の名称 ：

改ざん監視システム、保護制御モジュール及び検知モジュール

技術分野

[0001] 本発明は、機器内部で動作するモジュール等を監視する技術に関する。

背景技術

[0002] 近年、秘匿データを有しているアプリケーションプログラムが、悪意のある第三者（以下、「攻撃者」という）に解析されないようにするため、ソフトウェアによってアプリケーションプログラムを保護する技術が開発されつつある。

[0003] ソフトウェアによってアプリケーションプログラムを保護する技術として、例えば、ハッシュ値を用いた改ざん検証がある。また、アプリケーションプログラムを利用しないときには、アプリケーションプログラムを暗号化して保存しておき、利用するときにのみ、暗号化したアプリケーションプログラムを復号してメモリへロードする復号ロード機能等がある。

[0004] ところが、このような技術を利用しても、アプリケーションプログラムを保護するソフトウェア（以下、「保護制御モジュール」という）自体が攻撃者により改ざんされる可能性がある。保護制御モジュールが改ざんされると、アプリケーションプログラムが攻撃者の攻撃を受けることになる。このような攻撃に対抗するために、保護制御モジュールの改ざん検出を行う検知モジュールを用いて、保護制御モジュールの改ざん検出を行う。

[0005] 検知モジュールは、保護制御モジュールを構成するすべてのデータを読み込み、ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）値を計算し、予め記憶しているＭＡＣ値と比較することにより、保護制御モジュールの改ざん検出を行う。

先行技術文献

特許文献

[0006] 特許文献1：日本国特許第３０５６７３２号特許公報

特許文献2：ＷＯ２００８／０９９６８２国際公開公報

特許文献3：ＷＯ２００９／１１８８００国際公開公報

非特許文献

[0007] 非特許文献1：岡本龍明、山本博資、「現代暗号」、産業図書（１９９７年）

非特許文献2：ＩＴＵ－Ｔ Ｒｅｃｏｍｍｅｎｄａｔｉｏｎ Ｘ．５０９ （１９９７ Ｅ）： Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ － Ｏｐｅｎ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ － Ｔｈｅ Ｄｉｒｅｃｔｏｒｙ： Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ，１９９７

発明の概要

発明が解決しようとする課題

[0008] しかしながら、検知モジュールが改ざんされ、検知モジュールのセキュリティが劣化している場合、改ざんされた検知モジュールが、保護制御モジュールに含まれる鍵データや保護制御モジュールの機能自体を、不正利用する危険性がある。そうすると、当該検知モジュールによって、不正なアプリケーションがインストールされ、当該アプリケーションによって、ユーザの個人情報やコンテンツなどが漏えいする可能性がある。

[0009] 本発明は、上記の問題点に鑑みなされたものであって、複数の検知モジュールのうち一部の検知モジュールが改ざんされている場合であっても、保護制御モジュールの改ざん検出を行うことができる改ざん監視システム、保護制御モジュール、検知モジュール、制御方法及び制御用プログラムを記録している記録媒体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

[0010] 前記目的を達成するために、本発明は、コンピュータプログラムを保護する保護制御モジュールと、前記保護制御モジュールを監視するためのｎ個の検知モジュールと、管理装置とを含む改ざん監視システムであって、前記保

護制御モジュールは、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成手段と、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールを選択する選択手段と、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配手段とを備え、ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出し、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信し、前記管理装置は、前記検知モジュールのそれぞれから前記判断結果を受信し、受信した判断結果を基にして、前記保護制御モジュールの改ざんを管理することを特徴とする。

発明の効果

[0011] 本発明によれば、全ての検知モジュールに検知処理を実行させるのではなく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができる。

図面の簡単な説明

[0012] [図1]実施の形態２における検知システム１０の全体構成図である。

[図2]保護制御モジュール１２０の構成を示すブロック図である。

[図3]検知モジュール１３１の構成を示すブロック図である。

[図4]判断部２１０の構成を示すブロック図である。

[図5]検証基データ配布部２２０の構成を示すブロック図である。

[図6]機器１００のハードウェア構成図である。

[図7]機器１００のソフトウェア階層図である。

[図8]検知システム１０の全体の動作を示すフローチャートである。

[図9]初期設定処理を示すシーケンス図である。

[図10]初期設定処理における検証基データの生成処理の動作を示すフローチャートである。

[図11]データ分割を説明するための図である。

[図12]分割データ１の検証基データ６３０のデータ構成を示す図である。

[図13]分割データ２の検証基データ６５０のデータ構成を示す図である。

[図14]分割データ３の検証基データ６７０のデータ構成を示す図である。

[図15]検知処理の動作を示すシーケンス図である。図１６へ続く。

[図16]検知処理の動作を示すシーケンス図である。図１５から続く。

[図17]検知モジュールの選択のために用いる対応表３３０のデータ構造を示す。

[図18]検証基データの更新処理を示すシーケンス図である。

[図19]実施の形態３における初期設定処理の動作を示すシーケンス図である。

[図20]検証基データの生成処理の動作を示すフローチャートである。

[図21]データ分散を説明するための図である。

[図22]検証基データ６９０のデータ構成を示す図である。

[図23]検知処理の動作を示すシーケンス図である。図２４へ続く。

[図24]検知処理の動作を示すシーケンス図である。図２３から続く。

[図25]検知モジュールの選択のために用いる対応表３３０ａのデータ構造を示す。

[図26]実施の形態４における検知処理の動作を示すシーケンス図である。図２７へ続く。

[図27]検知処理の動作を示すシーケンス図である。図２８へ続く。

[図28]検知処理の動作を示すシーケンス図である。図２９へ続く。

[図29]検知処理の動作を示すシーケンス図である。図２８から続く。

[図30]検知モジュールの選択のために用いる対応表３３０ｂのデータ構造を示す。

[図31]実施の形態５における複数の復号サブプロセスから構成される復号処

理プロセスを説明するための図である。

[図32]検証基データ配布部２２０ａの構成を示すブロック図である。

[図33]検証基データ２４０のデータ構成を示す図である。

[図34]検証基データの生成処理の動作を示すフローチャートである。

[図35]検知処理の動作を示すシーケンス図である。図３６へ続く。

[図36]検知処理の動作を示すシーケンス図である。図３５から続く。

[図37]復号部分処理１の検証基データ２５０ａのデータ構成を示す図である。

[図38]復号部分処理２の検証基データ２５０ｂのデータ構成を示す図である。

[図39]復号部分処理３の検証基データ２５０ｃのデータ構成を示す図である。

[図40]実施の形態１における監視システム１０ｄの全体構成図である。

発明を実施するための形態

[0013] 本発明の一実施態様は、コンピュータプログラムを保護する保護制御モジュールと、前記保護制御モジュールを監視するためのｎ個の検知モジュールと、管理装置とを含む改ざん監視システムであって、前記保護制御モジュールは、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成手段と、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールを選択する選択手段と、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配手段とを備え、ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出し、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信し、前記管理装置は、前記検知モジュールのそれぞれから前記判断結果を受信し、受信した判断結果を基にして、前記保護制御モジュールの改ざんを管理することを特徴とする。

[0014] この態様によると、全ての検知モジュールに検知処理を実行させるのでは

なく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができる。

[0015] ここで、前記改ざん監視システムは、１台の情報処理装置を含み、前記情報処理装置が前記保護制御モジュールとｎ個の前記検知モジュールとを含み、前記コンピュータプログラムを記憶しており、前記情報処理装置と前記管理装置とは、ネットワークを介して接続されているとしてもよい。

[0016] この構成によると、１台の情報処理装置が前記保護制御モジュールとｎ個の前記検知モジュールとを含むので、情報処理装置の起動中、常に、各検知モジュールは、前記保護制御モジュールを監視することができる。

[0017] ここで、前記改ざん監視システムは、１台の情報処理装置及びｎ台の検知装置を含み、前記情報処理装置が前記保護制御モジュールを含み、前記コンピュータプログラムを記憶しており、ｎ台の前記検知装置が、それぞれ、１個の前記検知モジュールを含み、前記情報処理装置とｎ台の前記検知装置と前記管理装置とは、ネットワークを介して接続されているとしてもよい。

[0018] この構成によると、検知モジュールを含む検知装置と、保護制御モジュールを含む情報処理装置とは、ネットワークを介して、接続されている。このため、保護制御モジュールと検知モジュールとが同時に改ざんされる可能性が低くなる。

[0019] 本発明の別の実施態様は、コンピュータプログラムを保護する保護制御モジュールであって、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成手段と、当該保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択する選択手段と、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配手段とを備え、ｄ個の前記検知モジュール

のそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出するとしてもよい。

[0020] この態様によると、全ての検知モジュールに検知処理を実行させるのではなく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができる。

[0021] ここで、前記生成手段は、前記コンピュータプログラムを暗号化して生成した暗号化コンピュータプログラムを記憶している記憶手段と、前記暗号化コンピュータプログラムを復号してコンピュータプログラムを生成する復号手段と、生成された前記コンピュータプログラムを基にして、ｄ個の前記分配データを生成する分配データ生成手段とを含むとしてもよい。また、前記分配データ生成手段は、前記コンピュータプログラムを構成するデータを分割してｄ個の前記分配データを生成するとしてもよい。

[0022] これらの構成によると、保護制御モジュールの改ざんを検出するために、保護制御モジュール自体により秘匿されるデータを用いていない。このため、秘匿するデータが検知モジュールに漏洩することを防止することができる。

[0023] ここで、前記分配データ生成手段は、前記コンピュータプログラムを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成し、前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを復元することができるように、前記コンピュータプログラムを分散する秘密分散法であるとしてもよい。

[0024] この構成によると、ｄより小さいｋ個以上の検知モジュールによる監視結果を用いて、保護制御モジュールの改ざんを検出することができる。従って

、（ｄ－ｋ）個以下の検知モジュールが改ざんされている場合であっても、保護制御モジュールの改ざんを検出することができる。

[0025] ここで、前記生成手段は、前記コンピュータプログラムを暗号化して生成した暗号化コンピュータプログラムを記憶している記憶手段と、前記暗号化コンピュータプログラムに、復号処理を施す過程において、ｄ個の前記分配データを生成する復号手段とを含み、前記復号処理は、ｄ個の復号サブ処理から構成され、ｄ個の復号サブ処理を順次施すことにより、前記暗号化コンピュータプログラムの復号を行い、各復号サブ処理から出力される復号出力を前記分配データとするとしてもよい。

[0026] この構成によると、保護制御モジュールの改ざんを検出するために、保護制御モジュール自体により秘匿されるデータを用いていないので、秘匿するデータが検知モジュールに漏洩することを防止することができる。

[0027] ここで、前記選択手段は、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールの組合せと、当該組合せを識別する識別情報とを対応付けて含む対応表を保持し、前記組合せの選択に用いる選択情報を取得し、取得した選択情報に一致する識別情報に対応する組合せを前記対応表から取得し、取得し組合せに含まれる検知モジュールを選択するとしてもよい。

[0028] また、前記選択手段は、乱数を生成し、生成した乱数を前記選択情報とすることにより、前記選択情報を取得するとしてもよい。

[0029] また、前記選択手段は、前記分配手段によりｄ個の前記分配データを分配するごとに、前記選択情報を新たに生成するとしてもよい。

[0030] また、各検知モジュールは、乱数を生成し、他の全ての検知モジュールへ送信し、各検知モジュールは、受信した乱数及び自身が生成した乱数を用いて、選択情報を生成し、生成した前記選択情報を前記保護制御モジュールへ送信し、前記選択手段は、前記検知モジュールから前記選択情報を受信し、受信した前記選択情報を用いるとしてもよい。

[0031] また、保護制御モジュールの改ざんを管理する管理装置は、前記選択情報を生成し、生成した前記選択情報を前記保護制御モジュールへ送信し、前記

選択手段は、前記管理装置から前記選択情報を受信し、受信した前記選択情報を用いるとしてもよい。

[0032] これらの構成によると、保護制御モジュールが恣意的に検知モジュールを選択することができない。

[0033] ここで、前記コンピュータプログラムは、前記保護制御モジュールの保護の対象であるアプリケーションプログラム、又は、前記保護制御モジュールの動作手順を示すプログラムであるとしてもよい。

[0034] また、前記保護制御モジュールは、情報処理装置に含まれ、前記情報処理装置は、前記コンピュータプログラムを記憶しているとしてもよい。

[0035] 本発明の別の実施態様は、コンピュータプログラムを保護する保護制御モジュールを監視する検知モジュールであって、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成し、前記保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択し、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する保護制御モジュールから１個の前記分配データを受信する受信手段と、受信した前記分配データが正しいか否かを判断する検証手段と、正しいと判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する送信手段とを備え、前記受信手段は、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取り、前記検証手段は、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断し、前記送信手段は、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信することを特徴とする。

[0036] この態様によると、保護制御モジュールの改ざんを検出するために、保護制御モジュール自体により秘匿されるデータを用いていないので、秘匿するデータが検知モジュールに漏洩することを防止することができる。

[0037] ここで、前記検証手段は、自身の監視結果及び受信した監視結果を用いて、自身を含め、ｄ個の検知モジュールがそれぞれ受信した分配データが正し

いと決定したか否かを判断し、ｄ個の検知モジュールがそれぞれ受信した分配データが正しいと決定した場合に、前記保護制御モジュールが改ざんされていないと決定し、ｄ個の検知モジュールのうち、少なくとも１個の検知モジュールが受信した分配データが正しくないと決定した場合に、前記保護制御モジュールが改ざんされていると決定するとしてもよい。

[0038] この構成によると、全ての検知モジュールに検知処理を実行させるのではなく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができる。

[0039] ここで、前記保護制御モジュールは、前記コンピュータプログラムを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成し、前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを復元することができるように、前記コンピュータプログラムを分散する秘密分散法であり、前記検証手段は、自身の監視結果及び受信した監視結果を用いて、自身を含め、少なくともｋ個の検知モジュールがそれぞれ受信した分配データが正しいと決定したか否かを判断し、少なくともｋ個の検知モジュールがそれぞれ受信した分配データが正しいと決定した場合に、前記保護制御モジュールが改ざんされていないと決定し、（ｄ－ｋ＋１）個以上の検知モジュールがそれぞれ受信した分配データが正しくないと決定した場合に、前記保護制御モジュールが改ざんされていると決定するとしてもよい。

[0040] この構成によると、ｄより小さいｋ個以上の検知モジュールによる監視結果を用いて、保護制御モジュールの改ざんを検出することができる。従って、（ｄ－ｋ）個以下の検知モジュールが改ざんされている場合であっても、保護制御モジュールの改ざんを検出することができる。

[0041] ここで、ｎ個の前記検知モジュール及び前記保護制御モジュールは、情報処理装置に含まれ、前記情報処理装置は、前記コンピュータプログラムを記憶しているとしてもよい。

[0042] また、前記検知モジュールは、検知装置に含まれ、前記保護制御モジュールは、情報処理装置に含まれ、前記情報処理装置は、前記コンピュータプログラムを記憶しているとしてもよい。

[0043] 以下、図面に基づき本発明の実施の形態について説明する。

[0044] １．実施の形態１

（１）本発明に係る一の実施の形態としての改ざん監視システム１０ｄについて説明する。

[0045] 改ざん監視システム１０ｄは、図４０に示すように、保護制御モジュール１２０ｄ、ｎ個の検知モジュール１３０ｄ１、１３０ｄ２、１３０ｄ２、・・・、１３０ｄｎ及び管理装置２００ｄを含んでいる。

[0046] 保護制御モジュール１２０ｄは、コンピュータプログラム１１０ｄを保護する。

[0047] ｎ個の検知モジュール１３０ｄ１、１３０ｄ２、１３０ｄ２、・・・、１３０ｄｎは、保護制御モジュール１２０ｄを監視する。

[0048] 保護制御モジュール１２０ｄは、生成部３１０ｄ、選択部３１１ｄ及び分配部３０２ｄから構成される。

[0049] 生成部３１０ｄは、コンピュータプログラム１１０ｄを基にして、ｎより小さいｄ個の分配データを生成する。

[0050] 選択部３１１ｄは、ｎ個の検知モジュール１３０ｄ１、１３０ｄ２、１３０ｄ２、・・・、１３０ｄｎのうち、ｄ個の検知モジュールを選択する。

[0051] 分配部３０２ｄは、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する。

[0052] ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断し、当該保護制御モジュールの改ざんを検出し、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する。

[0053] 管理装置２００ｄは、前記検知モジュールのそれぞれから前記判断結果を受信し、受信した判断結果を基にして、保護制御モジュール１２０ｄの改ざんを管理する。

[0054] この構成によると、全ての検知モジュールに検知処理を実行させるのではなく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができる。

[0055] （２）次のように構成してもよい。

[0056] 改ざん監視システム１０ｄは、１台の情報処理装置（図示していない）を含む。前記情報処理装置が保護制御モジュール１２０ｄとｎ個の検知モジュール１３０ｄ１、１３０ｄ２、・・・、１３０ｄｎを含み、コンピュータプログラム１１０ｄを記憶している。

[0057] 前記情報処理装置と管理装置２００ｄとは、ネットワークを介して接続されている。

[0058] （３）次のように構成してもよい。

[0059] 改ざん監視システム１０ｄは、１台の情報処理装置（図示していない）及びｎ台の検知装置（図示していない）を含む。

[0060] 前記情報処理装置が保護制御モジュール１２０ｄを含み、コンピュータプログラム１１０ｄを記憶している。

[0061] ｎ台の前記検知装置が、それぞれ、１個の前記検知モジュールを含む。

[0062] 前記情報処理装置とｎ台の前記検知装置と管理装置２００ｄとは、ネットワークを介して接続されている。

[0063] （４）次のように構成してもよい。

[0064] （４－１）生成部３１０ｄは、記憶部と復号部と分配データ生成部とを含む。

[0065] 記憶部は、コンピュータプログラム１１０ｄを暗号化して生成した暗号化コンピュータプログラムを記憶している。

[0066] 復号部は、前記暗号化コンピュータプログラムを復号してコンピュータプログラムを生成する。

[0067] 分配データ生成部は、生成された前記コンピュータプログラムを基にして、ｄ個の前記分配データを生成する。

[0068] （４－２）分配データ生成部は、前記コンピュータプログラムを構成するデータを分割してｄ個の前記分配データを生成する。

[0069] （４－３）分配データ生成部は、前記コンピュータプログラムを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成する。ここで、前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを復元することができるように、前記コンピュータプログラムを分散する秘密分散法である。

[0070] （５）次のように構成してもよい。

[0071] 生成部３１０ｄは、記憶部及び復号部を含む。

[0072] 復号部は、コンピュータプログラム１１０ｄを暗号化して生成した暗号化コンピュータプログラムを記憶している。

[0073] 復号部は、前記暗号化コンピュータプログラムに、復号処理を施す過程において、ｄ個の前記分配データを生成する。ここで、前記復号処理は、ｄ個の復号サブ処理から構成され、ｄ個の復号サブ処理を順次施すことにより、前記暗号化コンピュータプログラムの復号を行い、各復号サブ処理から出力される復号出力を前記分配データとする。

[0074] （６）次のように構成してもよい。

[0075] （６－１）選択部３１１ｄは、対応表（図示していない）を保持する。この対応表は、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールの組合せと、当該組合せを識別する識別情報とを対応付けて含む。前記組合せの選択に用いる選択情報を取得し、取得した選択情報に一致する識別情報に対

応する組合せを前記対応表から取得し、取得し組合せに含まれる検知モジュールを選択する。

[0076] （６－２）選択部３１１ｄは、乱数を生成し、生成した乱数を前記選択情報とすることにより、前記選択情報を取得する。

[0077] （６－３）選択部３１１ｄは、分配部３０２ｄによりｄ個の前記分配データを分配するごとに、前記選択情報を新たに生成する。

[0078] （６－４）各検知モジュールは、乱数を生成し、他の全ての検知モジュールへ送信する。また、各検知モジュールは、受信した乱数及び自身が生成した乱数を用いて、選択情報を生成し、生成した前記選択情報を前記保護制御モジュールへ送信する。

[0079] 選択部３１１ｄは、前記検知モジュールから前記選択情報を受信し、受信した前記選択情報を用いる。

[0080] （６－５）管理装置２００ｄは、前記選択情報を生成し、生成した前記選択情報を保護制御モジュール１２０ｄへ送信する。

[0081] 選択部３１１ｄは、管理装置２００ｄから前記選択情報を受信し、受信した前記選択情報を用いる

（７）コンピュータプログラム１１０ｄは、保護制御モジュール１２０ｄの保護の対象であるアプリケーションプログラム、又は、保護制御モジュール１２０ｄの動作手順を示すプログラムであるとしてもよい。

[0082] （８）次のように構成してもよい。

[0083] （８－１）検知モジュール１３０ｄ１は、受信部、検証部及び送信部を備える。他の検知モジュールも同様である。

[0084] 検証部は、保護制御モジュール１２０ｄから１個の前記分配データを受信する。ここで、保護制御モジュール１２０ｄは、コンピュータプログラム１１０ｄを基にして、ｎより小さいｄ個の分配データを生成し、保護制御モジュール１２０ｄを監視するためのｎ個の検知モジュール１３０ｄ１、１３０ｄ２、・・・、１３０ｄｎのうち、ｄ個の検知モジュールを選択し、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュール

へ分配する。

[0085] 検証部は、受信した前記分配データが正しいか否かを判断する。

[0086] 送信部は、正しいと判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する。

[0087] 受信部は、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取る。

[0088] 検証部は、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断する。

[0089] 送信部は、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する。

[0090] （８－２）検証部は、自身の監視結果及び受信した監視結果を用いて、自身を含め、ｄ個の検知モジュールがそれぞれ受信した分配データが正しいと決定したか否かを判断する。ｄ個の検知モジュールによりそれぞれ受信した分配データが正しいと決定された場合に、保護制御モジュール１２０ｄが改ざんされていないと決定する。ｄ個の検知モジュールのうち、少なくとも１個の検知モジュールにより受信した分配データが正しくないと決定された場合に、保護制御モジュール１２０ｄが改ざんされていると決定する。

[0091] （８－３）保護制御モジュール１２０ｄは、コンピュータプログラム１１０ｄを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成する。ここで、前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを復元することができるように、前記コンピュータプログラムを分散する秘密分散法である。

[0092] 検証部は、（ａ）自身の監視結果及び受信した監視結果を用いて、自身を含め、少なくともｋ個の検知モジュールがそれぞれ受信した分配データが正しいと決定したか否かを判断する。（ｂ）少なくともｋ個の検知モジュールによりそれぞれ受信した分配データが正しいと決定された場合に、前記保護制御モジュールが改ざんされていないと決定する。（ｃ）（ｄ－ｋ＋１）個

以上の検知モジュールによりそれぞれ受信した分配データが正しくないと決定された場合に、前記保護制御モジュールが改ざんされていると決定する。

[0093] ２．実施の形態２

本発明に係る別の実施の形態としての情報処理装置及び管理装置から構成される検知システム１０について説明する。

[0094] ２．１　検知システム１０の構成

検知システム１０は、図１に示すように、情報処理装置としての機器１００及び管理装置２００から構成されている。機器１００及び管理装置２００は、ネットワーク２０を介して接続されている。

[0095] 機器１００は、ネットワーク２０を介した様々なサービスをユーザに提供する情報処理装置である。例えば、機器１００は、ネットワーク２０を介して、コンテンツ配信サーバ（図示していない）にアクセスすることにより、音楽や映像などのコンテンツを購入して再生する。また、金融機関のシステム（図示していない）にアクセスすることにより、ネットバンキング（預金の残高照会や口座振り込みなど）を利用する。

[0096] （１）機器１００の構成

機器１００は、後述するように、プロセッサ、メモリ及びその他のユニットを備えたコンピュータシステムである。メモリ上に記憶されている制御用のコンピュータプログラムに従って、プロセッサが動作することにより、機器１００は、その機能を達成する。

[0097] 図１に示すように、機器１００のメモリは、アプリケーションソフト（以下、「アプリ」という。）１１０、アプリ１１１、アプリ１１２、アプリ１１３、アプリ１１４、保護制御モジュール１２０、及び検知モジュール群１３０を記憶している。ここで、アプリ１１０、アプリ１１１、アプリ１１２、アプリ１１３、アプリ１１４、保護制御モジュール１２０及び検知モジュール群１３０内の各検知モジュールは、それぞれ、コンピュータプログラムである。これらのコンピュータプログラムは、それぞれ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。アプリ１１０、アプリ１１１、アプリ１１２、アプリ１１３、アプリ１１４、保護制御モジュール１２０及び検知モジュール群１３０内の各検知モジュールに従って、プロセッサが動作する。こうして、アプリ１１０、アプリ１１１、アプリ１１２、アプリ１１３、アプリ１１４、保護制御モジュール１２０及び検知モジュール群１３０内の各検知モジュールは、その機能を達成する。

[0098] このように、保護制御モジュール１２０を記憶しているメモリ及びプロセッサは、一つの保護制御回路を構成している。

[0099] アプリ１１０、１１１、１１２、１１３、１１４は、それぞれ、ネットワークを介して、機器１００を使用するユーザに、様々な機能を提供するためのソフトウェア、つまり、コンピュータプログラムである。例えば、アプリ１１０は、コンテンツ配信サーバ（不図示）から音楽コンテンツや映像コンテンツを購入するためのソフトウェアである。また、アプリ１１１は、その購入したコンテンツを再生するためのソフトウェアである。さらに、アプリ１１２は、金融機関のシステム（不図示）にアクセスし、残高確認や振り込みなどのネットバンキングを利用するためのソフトウェアである。

[0100] 各アプリは、コンテンツ配信サーバや金融機関のシステムと認証を行うための認証鍵など、秘匿データを有している。秘匿データは、悪意のある第三者（以下、「攻撃者」という。）によりアプリから抜き取られ、不正に利用されないようにするために、保護される必要があるデータである。

[0101] 保護制御モジュール１２０は、攻撃者により各アプリが解析され、認証鍵などの秘匿データが抜き取られないように各アプリを保護するための機能を制御するモジュールである。アプリを保護するための機能としては、復号ロード機能、改ざん検出機能、解析ツール検出機能などがある。復号ロード機能は、アプリを利用しないときには、当該アプリを暗号化して保存しておき、アプリを利用するときにのみ、暗号化アプリを復号してメモリへロードする機能である。また、改ざん検出機能は、アプリが改ざんされていないかをチェックする機能である。さらに、解析ツール検出機能は、デバッガなどの

解析ツールが動作しないかをチェックする機能である。

[0102] 保護制御モジュール１２０は、これらの機能の動作を制御し、各アプリが攻撃者によって解析されていないかなどをチェックする。攻撃者による攻撃を検出したときには、保護制御モジュール１２０は、攻撃が検出されたアプリの動作を停止する。次に、当該アプリが利用していたメモリ、特に秘匿データが記録されたメモリ領域のクリア（例えば、メモリ領域を「０」で埋める）などの処理を行う。こうして、秘匿データの漏洩を防止する。

[0103] 検知モジュール群１３０は、ｎ（ｎは、正整数）個の検知モジュールから構成される。一例として、検知モジュール群１３０は、図１に示すように、５つの検知モジュール１３１、検知モジュール１３２、検知モジュール１３３、検知モジュール１３４及び検知モジュール１３５から構成される。

[0104] ここで、検知モジュール１３１を記憶しているメモリ及びプロセッサは、一つの検知回路を構成している。また、検知モジュール１３２、検知モジュール１３３、検知モジュール１３４及び検知モジュール１３５の各検知モジュールについても、同様に、各検知モジュールを記憶しているメモリ及びプロセッサは、一つの検知回路を構成している。

[0105] 検知モジュール１３１、１３２、１３３、１３４及び１３５は、保護制御モジュール１２０が改ざんされているか否かを検証するために、保護制御モジュール１２０による暗号化アプリの復号処理の結果が正しいか否かを判断する。

[0106] 各検知モジュールは、保護制御モジュール１２０についての監視結果及び判断結果を、ネットワーク２０を介して、管理装置２００へ送信する。ここで、監視結果は、分割データが正しいか否かを示し、また、判断結果は、保護制御モジュール１２０が改ざんされているか否かを示す。

[0107] （２）管理装置２００の構成

管理装置２００は、検証基データを生成する。ここで、検証基データは、保護制御モジュール１２０が正しく動作しているか否かを検証するために必要なデータである。次に、生成した検証基データを機器１００へ配布する。

[0108] 管理装置２００は、図１に示すように、判断部２１０、検証基データ配布部２２０及び通信部２３０から構成される。通信部２３０は、ネットワーク２０を介して機器１００と通信を行う。なお、機器１００と管理装置２００との間のネットワークを介した通信には、通信データが暗号化されるなど、セキュリティの確保された通信路を用いてもよい。

[0109] 管理装置２００は、具体的には、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスクユニットなどを備えるコンピュータシステムである。ＣＰＵが、ＲＯＭまたはハードディスクユニットに記憶されているコンピュータプログラムに従って動作することにより、管理装置２００は、上記の機能を発揮する。

[0110] 判断部２１０は、機器１００内部のソフトウェア（アプリ１１０から１１４、保護制御モジュール１２０、検知モジュール群１３０）の状態（つまり、各ソフトウェアが改ざんされているか否か等の状態）に応じて、機器１００が実行すべき処理を決定し、検証基データ配布部２２０に各種指示を行う。詳細な構成は後述する。

[0111] 検証基データ配布部２２０は、機器１００内部のソフトウェア（保護制御モジュール１２０）が検知モジュールにより検知される際に、検知モジュールが検証に用いる検証基データを送信する。検証基データの詳細な構成は後述する。

[0112] 通信部２３０は、機器１００から受信した情報に応じて管理装置２００内部の各部に機器１００から受信した情報を出力する。また、管理装置２００内部の各部からの指示や情報を機器１００に送信する。具体的には、更新処理の際に、検証基データ配布部２２０からの指示や通知などを機器１００に送信したり、機器１００からの改ざん検出の監視結果などの情報を判断部２１０に出力したりする。

[0113] 続いて、各モジュールの詳細を順に説明する。

[0114] （３）保護制御モジュール１２０の詳細な構成

図２は、保護制御モジュール１２０の機能構成を示す機能ブロック図である。

[0115] 同図に示すように、保護制御モジュール１２０は、受信部３０１、送信部３０２、制御部３０３、復号ロード部３０４、改ざん検出部３０５、解析ツール検出部３０６、暗復号鍵保持部３０７、検証基データ保持部３０８、検証基データ生成部３０９、アプリ分割部３１０及び検知モジュール選択部３１１から構成される。

[0116] 受信部３０１は、各検知モジュールから、各種依頼などを受信する。

[0117] 送信部３０２は、各検知モジュールへ、各種依頼などを送信する。

[0118] 制御部３０３は、復号ロード部３０４、改ざん検出部３０５及び解析ツール検出部３０６を制御し、各アプリが攻撃者により攻撃されている場合に、それを検出する。

[0119] 復号ロード部３０４は、機器１００内部に保持されている暗号化されたアプリ（１１０から１１４）を実行するときに、暗号化されたアプリ（１１０から１１４）を暗復号鍵を用いて復号し、得られたアプリ（１１０から１１４）をメモリ上にロードする処理を行う。また、アプリ（１１０から１１４）実行中に、他のアプリへのコンテキストスイッチ(context switch)が発生したときに、暗復号鍵を用いてメモリ上のデータを暗号化し、再び元のアプリ（１１０から１１４）へコンテキストスイッチしたときに、暗号化したデータを復号する処理を行う。

[0120] なお、コンテキストスイッチとは、複数のプロセスが１つのＣＰＵを共有できるように、ＣＰＵの状態(コンテキスト)を保存したり復元したりする過程のことである。

[0121] 改ざん検出部３０５は、各アプリが改ざんされているかどうか改ざん検出処理を実行する。改ざん検出処理には、各アプリに付加されている改ざん検出用の証明書を用いる方法と、ＭＡＣ値を比較する方法とがある。

[0122] なお、証明書に関しては非特許文献２に詳しく説明されている。

[0123] 解析ツール検出部３０６は、デバッガなどの解析ツールがインストールされたり、動作したりしたときにそれを検出する。不正な攻撃者が各アプリを攻撃するために、解析ツールをインストールしたり、動作させることが想定

されるからである。検出方法としては、例えば、ファイル名を検索する方法や、デバッガが使用する特殊なレジスタが使用されているかを調べる方法や、デバッガが設定する割り込みを検出する方法などを用いる。

[0124] 暗復号鍵保持部３０７は、各アプリを暗復号するための暗復号鍵を保持する。

[0125] 検証基データ保持部３０８は、管理装置２００から受信した検証基データを保持する。検証基データの構成については、後述する。

[0126] 検証基データ生成部３０９は、検証基データ保持部３０８に保持している検証基データから検証基データを生成する。

[0127] アプリ分割部３１０は、復号ロード部３０４で復号したアプリ（１１０から１１４）のデータ、つまり、それぞれのアプリのコンピュータプログラムを構成するデータを分割する。

[0128] 検知モジュール選択部３１１は、検知処理時に検知を実行する検知モジュールを選択する。選択方法については、後述する。

[0129] （４）検知モジュールの詳細な構成

次に、検知モジュール１３１、１３２、１３３、１３４及び１３５の詳細について説明する。

[0130] 図３は、検知モジュール１３１の機能的な構成を示す機能ブロック図である。検知モジュール１３２、１３３、１３４及び１３５も、検知モジュール１３１と同様の構成を有しており、これらについての説明を省略する。

[0131] 同図に示すように、検知モジュール１３１は、受信部４０１、送信部４０２、制御部４０３、検証部４０４及び検証基データ保持部４０５から構成される。

[0132] 受信部４０１は、管理装置２００から、各種指示を受信する。また、他のモジュールへ依頼した処理の結果や、他の検知モジュールから保護制御モジュール１２０に対する監視結果を受信する。

[0133] 送信部４０２は、管理装置２００、保護制御モジュール１２０及び他の検知モジュールへ、各種処理結果などのデータを送信する。

[0134] 制御部４０３は、受信部４０１が受信した各種指示や通知に基づいて、検証部４０４を制御し、保護制御モジュール１２０の検証処理を行う。

[0135] 検証部４０４は、保護制御モジュール１２０が正常に動作しているか検証を行う。検証方法としては、保護制御モジュール１２０に対する検知では、検証基データ保持部４０５に保持している検証基データを用いて、保護制御モジュール１２０が正常に動作しているかを検証する。

[0136] 検証基データ保持部４０５は、保護制御モジュール１２０の復号ロード部３０４が正常に動作するか否かを検証するための検証基データを保持する。検証基データは、保護制御モジュール１２０から与えられたものである。

[0137] （５）判断部２１０の詳細な構成

図４は、判断部２１０の機能構成を示す機能ブロック図である。同図に示すように、判断部２１０は、受信部５０１、送信部５０２、指示生成部５０３及びモジュール選択部５０４から構成される。

[0138] 受信部５０１は、各検知モジュールから、監視結果や各種依頼などを受信し、指示生成部５０３へ送信する。さらに、検証基データ配布部２２０から処理が完了した通知を受信し、指示生成部５０３に送信する。

[0139] 送信部５０２は、指示生成部５０３で生成された指示を管理装置２００内の検証基データ配布部２２０へ送信する。

[0140] 指示生成部５０３は、保護制御モジュール１２０から検証基データの送付の依頼を受け取った場合には、送付の依頼に基づいて検証基データ配布部２２０に対して検証基データを配布する旨の指示を生成し、生成した指示を送信部５０２へ出力する。また、保護制御モジュール１２０の検知処理の実行時に、検知を実行する検知モジュールを選択するように、モジュール選択部５０４に対する検知モジュールの選択の指示を生成し、生成した指示をモジュール選択部５０４へ出力する。

[0141] 指示生成部５０３から検知モジュールの選択の指示を受け取ると、モジュール選択部５０４は、保護制御モジュール１２０の検知処理の実行時に、どの検知モジュールが検知を実行するかを決定する。モジュール選択部５０４

は、機器１００が保持するｎ個の検知モジュールから構成される検知モジュール群１３０から、ｄ（ｄは、ｎより小さい正の整数）個の検知モジュールを選択する。選択対象の検知モジュールを決定するために、検知モジュール１３１から開始して、検知モジュール１３２、１３３、１３４、１３５のように、順番に検知モジュールを選択する方法を用いてもよいし、複数の検知モジュールからランダムに１個又は複数個の検知モジュールを選択する方法を用いてもよい。次に、モジュール選択部５０４は、選択した検知モジュールを識別する検知モジュール識別子を、指示生成部５０３及び送信部５０２、通信部２３０及びネットワーク２０を介して、機器１００へ送信する。

[0142] （６）検証基データ配布部２２０の詳細な構成

図５は、検証基データ配布部２２０の機能構成を示す機能ブロック図である。

[0143] 同図に示すように、検証基データ配布部２２０は、受信部６０１、送信部６０２、制御部６０３、認証部６０４、証明書生成部６０５、署名秘密鍵保持部６０６、暗号鍵保持部６０７、データ分割部６０８、アプリ保持部６０９、検証基データ生成部６１０、保護制御モジュール保持部６１１及び検知モジュール保持部６１２から構成される。

[0144] 署名秘密鍵保持部６０６は、証明書生成部６０５により証明書を生成するときに利用する管理装置２００の署名秘密鍵（署名私有鍵）を保持している。

[0145] 暗号鍵保持部６０７は、保護制御モジュール１２０と共有している暗復号鍵を保持している。

[0146] アプリ保持部６０９は、機器１００にインストールされるアプリ１１０、１１１、１１２、１１３、１１４のデータ、つまり、それぞれのアプリを構成するコンピュータプログラムを記憶している。

[0147] 保護制御モジュール保持部６１１は、機器１００にインストールされる保護制御モジュール１２０を構成するコンピュータプログラムを保持している。

[0148] 検知モジュール保持部６１２は、機器１００にインストールされる検知モジュールを構成するコンピュータプログラムを保持する。

[0149] これらのコンピュータプログラムは、それぞれ、それぞれ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。

[0150] 受信部６０１は、各検知モジュールから保護制御モジュール１２０に対する監視結果を受信する。

[0151] 送信部６０２は、機器１００内部の各アプリ及び保護制御モジュール１２０の改ざん検証の依頼や検証に必要な検証基データなどを送信する。

[0152] 制御部６０３は、検証基データ配布部２２０の各構成要素を制御する。

[0153] 認証部６０４は、各検知モジュールや保護制御モジュール１２０と相互認証を行う。

[0154] 証明書生成部６０５は、アプリ保持部６０９に保持するアプリのデータに対し、データ分割部６０８を用いて分割し、保護制御モジュール保持部６１１に保持されている保護制御モジュール１２０を構成するコンピュータプログラムに含まれている復号ロード部３０４を用いてアプリを暗号化して暗号化アプリを求め、暗号化アプリと分割データから検証値を生成する。さらに、管理装置２００の署名秘密鍵（署名私有鍵）を用いて署名データを生成し、生成した署名データを含む証明書を生成する。

[0155] なお、署名方式に関しては非特許文献１の１７１ページから１８７ページに詳しく説明されている。

[0156] データ分割部６０８は、アプリ保持部６０９に記憶されているアプリ１１０、１１１、１１２、１１３、１１４のデータをそれぞれ分割して複数個の分割データを生成する。

[0157] 検証基データ生成部６１０は、アプリ保持部６０９に記憶されている各アプリのデータと、データ分割部６０８により生成された複数の分割データとから、検証基データを生成する。検証基データ生成部６１０は、生成した検証基データを機器１００へ送信する。検証基データの構成については後述す

る。

[0158] （７）機器１００のハードウェア構成

続いて、図６を用いて、機器１００のハードウェア構成について説明する。

[0159] 同図に示すように、機器１００は、ＣＰＵ（Central Processing Unit）１７１、例えば不揮発メモリであるＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory）１７２、ＲＡＭ（Random Access Memory）１７３、及びＮＩＣ（Network Interface Card）１７４等を含んで構成され、これらはバス１７５を介して相互に通信可能に接続されている。

[0160] ＥＥＰＲＯＭ１７２には、保護制御モジュール１２０を含む制御用の各種モジュール、検知モジュール１３１、１３２、１３３、１３４、１３５及びアプリ１１０、１１１、１１２、１１３、１１４などが格納されている。

[0161] ＥＥＰＲＯＭ１７２に格納されている保護制御モジュール１２０を含む制御用の各種モジュールをＣＰＵ１７１が実行することにより、制御用の各種モジュールの各機能部の制御が実現される。各機能部は、具体的には、コンピュータプログラムによって記述され実現される。

[0162] ＲＡＭ１７３は、ＣＰＵ１７１のワークエリアとして用いられる。ＲＡＭ１７３には各検知モジュール及び各アプリがロードされる。ＲＡＭ１７３に格納された各検知モジュール及び各アプリをＣＰＵ１７１が実行することにより、検知モジュール及び各アプリの機能が実現される。

[0163] ＮＩＣ１７４は、ネットワークに接続するための拡張カードである。

[0164] （８）ソフトウェア階層

続いて、図７を用いて、機器１００において動作するソフトウェア（コンピュータプログラム）のソフトウェア階層の構造について、説明する。

[0165] 機器１００においては、コンピュータプログラムとして、ブートローダ１９０、保護制御モジュール１２０、ＯＳ１８０及びアプリ１１０、１１１、１１２、１１３、１１４が動作する。ブートローダ１９０、保護制御モジュ

ール１２０、ＯＳ１８０及びアプリ１１０、１１１、１１２、１１３、１１４は、階層的に構成されている。

[0166] 図７に示すように、ブートローダ１９０及び保護制御モジュール１２０が最下位層に位置している。その上に、ＯＳ１８０が位置し、ＯＳ１８０の上に、アプリ１１０、１１１、１１２、１１３、１１４が位置している。

[0167] 同図に示すように、検知モジュール群１３０は、ＯＳ１８０の中に組み込まれている。各アプリはＯＳ１８０の配下で動作し、保護制御モジュール１２０は、ブートローダ１９０等とともにＯＳ１８０の管理外にある。

[0168] 機器１００の起動の際には、最初に、ブートローダ１９０が起動され、次に、保護制御モジュール１２０及びＯＳ１８０が起動される。ＯＳ１８０の起動中において、検知モジュール群１３０が起動される。次に、アプリ１１０、１１１、１１２、１１３、１１４が起動され、各アプリが実行される。

[0169] ２．２ 検知システム１０の動作概略

（１）全体の動作概要

検知システム１０の動作を、図８に示すフローチャートを用いて説明する。初めに、検知システム１０の大まかな処理を説明する。大まかな処理として、以下の２つの処理がある。

[0170] １つ目の処理は、ソフトウェア（保護制御モジュール１２０）を検証するために必要となる検証基データなどを埋め込む処理（初期設定処理）である。

[0171] ２つ目の処理は、機器１００内部のソフトウェア（保護制御モジュール１２０）が改ざんされていないかを検知する処理（検知処理）である。

[0172] 上記２つの処理の関係は、図８に示す通りである。

[0173] 検知システム１０では、機器１００が工場で製造される際に初期設定処理が行われ、保護制御モジュール１２０内へ検証基データが埋め込まれる（ステップＳ１００）。その後、機器１００が工場から出荷され、ユーザの利用に供される。

[0174] ユーザにより機器１００が利用される際には、機器１００内部では、保護

制御モジュール１２０が各アプリを攻撃者による攻撃から保護する。これと同時に、各検知モジュールは、保護制御モジュール１２０が攻撃されていないかをチェックする検知処理を行う（ステップＳ２００）。

[0175] 検知処理を行った結果、各検知モジュールによる保護制御モジュール１２０に対する監視結果を管理装置２００へ通知する。また、保護制御モジュール１２０が改ざんされたと判明した場合には、改ざんされた旨を機器１００が有する表示部に表示する。

[0176] 続いて、上記２つの処理について、その詳細を順に説明する。

[0177] （２）初期設定処理の動作

まず、初期設定処理について説明する。

[0178] 図９は、初期設定処理の検知システム１０の動作の流れを示すシーケンス図である。本シーケンス図において、検知モジュール１３１、１３２、１３３、１３４及び１３５の各々が個別に行う処理を、検知モジュール群１３０が行う処理としてまとめて記載している。

[0179] 保護制御モジュール１２０は、管理装置２００の保護制御モジュール保持部６１１に保持されており、検知モジュール１３１、１３２、１３３、１３４及び１３５は、管理装置２００の検知モジュール保持部６１２に保持されており、アプリ１１０、１１１、１１２、１１３及び１１４は、アプリ保持部６０９に保持されている。

[0180] 工場における機器１００の製造時に、管理装置２００は、機器１００に対して保護制御モジュール１２０、検知モジュール１３１、１３２、１３３、１３４及び１３５、並びに、アプリ１１０、１１１、１１２、１１３及び１１４を送信し、機器１００は、保護制御モジュール１２０、検知モジュール１３１、１３２、１３３、１３４及び１３５、並びに、アプリ１１０、１１１、１１２、１１３及び１１４を受信する（ステップＳ１００１）。機器１００は、機器１００のＥＥＰＲＯＭ１７２へ受信した各アプリ、保護制御モジュール１２０、各検知モジュールをインストール（書き込み）する（ステップＳ１００２）。これらの各アプリには、ソフトウェアが改ざんされてい

るかどうかを検証するための証明書（改ざん検出用証明書）が付加されている。上記ソフトウェア以外にも、機器１００の動作に必要なソフトウェアがインストールされる。

[0181] ソフトウェアのインストール（ステップＳ１００２）が終わると、機器１００は、機器１００の初期設定を行うソフトウェアや、正常に動作するかをテストするためのソフトウェアなどを実行することにより、初期化処理を行い（ステップＳ１００３）、保護制御モジュール１２０に対して初期化指示を出力する（ステップＳ１００４）。

[0182] 初期設定処理では、保護制御モジュール１２０の初期化処理が行われる。

[0183] 初期化指示を受け取ると（ステップＳ１００４）、保護制御モジュール１２０は、管理装置２００へ検証基データの送付を依頼する（ステップＳ１００５）。管理装置２００は、保護制御モジュール１２０から依頼を受信すると（ステップＳ１００５）、検証基データの生成処理を実行する（ステップＳ１００６）。検証基データの生成処理が完了すると、管理装置２００は、生成した検証基データを保護制御モジュール１２０へ送信する（ステップＳ１００７）。保護制御モジュール１２０は、管理装置２００から検証基データを受信し（ステップＳ１００７）、受信した検証基データを検証基データ保持部３０８へ記憶する（ステップＳ１００８）。

[0184] （３）検証基データの生成処理の動作

ここでは、図９のステップＳ１００６に示す検証基データの生成処理の詳細について、図１０に示すフローチャートを用いて説明する。

[0185] 管理装置２００の検証基データ生成部６１０は、アプリ保持部６０９に保持されている複数のアプリを読み出し、暗号鍵保持部６０７から暗復号鍵を読み出し、読み出した複数のアプリのそれぞれを、読み出した暗復号鍵を用いて、暗号化アルゴリズムにより暗号化して複数の暗号化アプリを生成する（ステップＳ１１０１）。ここで用いる暗号化アルゴリズムの一例は、ＡＥＳ（Advanced Encryption Standard）である。

[0186] 次に、データ分割部６０８は、アプリ保持部６０９に保持されている複数

のアプリを読み出し、読み出した複数のアプリのそれぞれを分割して、複数の分割データを生成する（ステップＳ１１０２）。ここにおけるアプリの分割方法としては、メモリ上にロードされるアプリのデータを一定サイズで分割してもよい。また、アプリのデータに対し法を取ったりしてもよい。例えば、１つのアプリのデータに対し、３つの法の値、例えば、

「７」、「１１」、「１７」で法を取ることで、１つのアプリのデータから３つの分割データを生成するとしてもよい。

[0187] 図１１はアプリのデータを分割する動作概要図である。この図に一例として示すように、データ分割部６０８は、アプリ１１０のデータを分割して、３個の分割データ１（１１０ａ）、分割データ２（１１０ｂ）及び分割データ３（１１０ｃ）を生成する。さらに具体的に説明すると、データ分割部６０８は、アプリ１１０、１１１、１１２、１１３及び１１４をそれぞれ３分割し、各アプリについて、３個の分割データ１、分割データ２及び分割データ３を生成する。

[0188] なお、アプリのデータを分割する方法として、中国人剰余定理を用いてアプリのデータが復元できるように、分割するとしてもよい。中国人剰余定理は非特許文献１の１５ページに記載されている。例えば、１つのアプリのデータが、１０進数による表現により、「１２００」であるとしたとき、このアプリのデータについて、３つの法の値、例えば、「７」、「１１」、「１７」で法を取ったとする。このとき、７×１１×１７＝１３０９であり、アプリのデータが「１３０９」より小さいため、中国人剰余定理からアプリの「７」、「１１」、「１７」で法を取った値から、アプリのデータ１２００を一意に求めることができる。なお、ここでは、１つのアプリのデータが、１０進数による表現により、「１２００」であるとしているが、これは、説明を簡略化するためであり、実際のアプリのデータが１０進数による表現により「１２００」であることはなく、アプリは、通常、もっと大きいサイズのコンピュータプログラムであることは言うまでもない。

[0189] ここでは、図１１に示すように、アプリのデータを３分割した例を用いて

説明する。データ分割部６０８は、複数のアプリ１１０、１１１、１１２、１１３及び１１４のデータをそれぞれ分割して分割データ１、分割データ２、分割データ３を生成する。一例として、図１１に示すように、データ分割部６０８は、アプリ１１０を分割して分割データ１（１１０ａ）、分割データ２（１１０ｂ）、分割データ３（１１０ｃ）を生成する。

[0190] データ分割部６０８による分割の終了後、証明書生成部６０５は、すべての分割データのそれぞれについて、つまり、分割データ毎に、暗号化したアプリと分割データの関係を示す検証値及び証明書（復号処理証明書）を生成する（ステップＳ１１０３）。

[0191] 次に、検証基データ生成部６１０は、すべての分割データのそれぞれについて、分割識別情報、判定情報、複数の検証値組及び証明書（復号処理証明書）を含む検証基データを生成する（ステップＳ１１０４）。なお、分割識別情報及び判定情報については、後述する。

[0192] （検証基データのデータ構成）

検証基データのデータ構成の一例を図１２から図１４を用いて説明する。

[0193] 図１２から図１４にそれぞれ示す検証基データ６３０、６５０及び６７０は、一例として、複数のアプリ１１０、１１１、１１２、１１３及び１１４のそれぞれを３分割した場合におけるものである。

[0194] 図１２に示す検証基データ６３０は、複数のアプリ１１０、１１１、１１２、１１３及び１１４それぞれから生成された分割データ１について生成されたものである。また、図１３に示す検証基データ６５０は、複数のアプリ１１０、１１１、１１２、１１３及び１１４それぞれから生成された分割データ２について生成されたものである。さらに、図１４に示す検証基データ６７０は、複数のアプリ１１０、１１１、１１２、１１３及び１１４それぞれから生成された分割データ３について生成されたものである。

[0195] 検証基データ６３０、６５０及び６７０は、図１２から図１４に示すように、それぞれ、分割識別情報、判定情報、複数の検証値組及び証明書から構成される。

[0196] 図１２に示す検証基データ６３０は、一例として、分割識別情報６３１、判定情報６３２、検証値組６３３ａ、６３３ｂ、６３３ｃ、６３３ｄ、６３３ｅ及び証明書６３４から構成されている。

[0197] 分割識別情報は、検証基データがアプリのどの分割データに対応するかを示す識別子である。言い換えると、検証基データが、アプリのデータを分割した際の、全ての分割データのうちのどの分割データに対応するかを示す情報である。

[0198] 一例として、分割識別情報は、分割数と分割データを識別する情報とを含む。

[0199] 例えば、アプリのデータを一定のサイズで分割する場合、例えば、アプリが３分割されたとき、分割データをそれぞれ、（３，１）、（３，２）及び（３，３）により示すことにする。ここで、（ａ，ｂ）は、アプリをａ個に分割したときの、ｂ番目の分割データを示すものとする。この場合に、図１２に示す分割識別情報６３１は、一例として、（３，１）であり、図１２に示す検証基データ６３０は、３分割された各アプリの１番目の分割データに対応している。また、図１３に示す分割識別情報６５１は、一例として、（３，２）であり、図１３に示す検証基データ６５０は、３分割された各アプリの２番目の分割データに対応している。さらに、図１４に示す分割識別情報６７１は、一例として、（３，３）であり、図１４に示す検証基データ６７０は、３分割された各アプリの３番目の分割データに対応している。

[0200] また、アプリのデータについて、複数の法を取ることにより分割データを生成する場合、例えば、アプリのデータについて法「７」、「１１」、「１７」を取ることによりアプリのデータを分割する場合に、分割識別情報は、分割数と法の値とを含むことにより、検証基データがアプリのどの分割データに対応するかを示す識別子であるとしてもよい。この場合に、図１２に示す分割識別情報６３１は、一例として、（３，７）となり、分割識別情報（３，７）は、分割数が「３」であり、複数のアプリのデータに対し法「７」を取ったことを示す。また、図１３に示す分割識別情報６５１は、一例とし

て、（３，１１）となり、分割識別情報（３，１１）は、分割数が「３」であり、アプリのデータに対し法「１１」を取ったことを示す。さらに、図１４に示す分割識別情報６７１は、一例として、（３，１７）となり、分割識別情報（３，１７）は、分割数が「３」であり、アプリのデータに対し法「１７」を取ったことを示す。ここで、分割識別情報（ａ，ｂ）は、アプリをａ個に分割したとき、法「ｂ」を用いることを示す。

[0201] ここで、分割識別情報には、分割数も含めているが、これに限定するものではなく分割したうちの何番目の分割データであるかを示した情報だけでもよいし、単に他の分割識別情報と区別できる情報であればよい。また、アプリのデータを一定サイズに分割することに限らず、それぞれの分割データのサイズは異なってもよいし、アプリのデータの一部を集めて分割データとしてもよい。

[0202] 判定情報は、分割データのすべてが検証されたかを判定するための情報である。

[0203] 判定情報は、一例として、分割数を含む。判定情報により示される個数分の異なる分割データの検証を行えば、全ての分割データが検証される。例えば、アプリのデータを一定のサイズで３分割する場合、判定情報には、分割数「３」と同じ値「３」が記載される。この場合には、３個の分割データの検証を行えば、全ての分割データが検証されたこととなる。

[0204] 一例として、図１２に示す判定情報６３２、図１３に示す判定情報６５２及び図１４に示す判定情報６７２は、それぞれ、「３」である。従って、この場合には、３個の分割データの検証を行えば、全ての分割データが検証されたこととなる。

[0205] また、アプリのデータについて、複数の法を取ることにより分割データを生成する場合には、判定情報は、複数の法を掛け合わせた値であるとしてもよい。例えば、アプリのデータについて、「７」、「１１」、「１７」のそれぞれで法を取る場合、判定情報には、「１３０９」と記載される。ここで、「１３０９」は、「７」、「１１」、「１７」を掛け合わせた値である。

これにより中国人剰余定理が成り立っていることを判定できる。また、中国人剰余定理が成り立つように分割すればよいので、復号が公開鍵暗号のＲＳＡ暗号の場合、判定情報は、ＲＳＡ暗号の公開鍵であるｎ（＝ｐ×ｑ）（ｐ、ｑは素数）の値より大きい値であればよいし、復号が共通鍵暗号のＡＥＳ暗号の場合、判定情報は、１２８ビットより大きい値であればよい。ＲＳＡ暗号に関しては非特許文献１の１１０ページから１１３ページに記載されている。

[0206] また、判定情報は、検証基データに記載されているとしているが、これに限ることなく、予め各検知モジュールが保持するとしてもよいし、検知モジュールのいずれかが保持しており、他の検知モジュールに送信するとしてもよい。

[0207] 検証値組の数は、アプリの数と同一である。例えば、検証基データ６３０に含まれている複数の検証値組は、それぞれ、アプリ１１０、１１１、１１２、１１３及び１１４に対応している。各検証値組は、アプリ識別情報、データ及び検証値を含む。

[0208] アプリ識別情報は、対応するアプリを識別する識別子である。

[0209] データは、対応するアプリの暗号化されたアプリである。

[0210] 検証値は、対応するアプリの分割データを検証するための値である。検証値は、対応する暗号化されたアプリのデータと生成した分割データとを結合して得られた結合体に、ハッシュ関数による演算を施して得たハッシュ値である。

[0211] （検証値）＝Ｈａｓｈ（暗号化アプリのデータ｜｜分割データ）

ここで、Ｈａｓｈ（ａ）は、ａに対してハッシュ関数による演算を施して得られたハッシュ値を示し、Ｘ｜｜Ｙは、Ｘ及びＹをこの順序で結合することを示す。

[0212] なお、検証値としてハッシュ関数による演算を施して得られたハッシュ値を使用しているが、これに限定するものではない。次のように、署名などを用いるとしてもよい。

[0213] （検証値）＝Ｓｉｇｎ（署名私有鍵、暗号化アプリのデータ｜｜分割データ）

ここで、Ｓｉｇｎ（ａ、ｂ）は、鍵ａを用いてｂに対して生成した署名データを示す。

[0214] また、ハッシュ値を計算する対象データは暗号化データと分割データとの結合体だけでなく、アプリを識別するアプリ識別情報やアプリの内容を示す情報（ＤＶＤやＢＤの再生アプリ、ネットバンキングのアプリなど）を含んでもよい。また、保護制御モジュール１２０の識別情報を含んでもよい。

[0215] 証明書は、復号処理証明書である。証明書は、検証基データに含まれる全ての検証値を結合して結合体を生成し、生成した結合体にハッシュ関数による演算を施してハッシュ値を計算し、計算したハッシュ値に対して、署名秘密鍵保持部６０６の署名秘密鍵を用いて生成した署名データである。

[0216] （証明書）＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値｜｜検証値｜｜・・・｜｜検証値））

図１２に示す検証基データ６３０の場合において、証明書６３４は、次のようにして算出される。

[0217] （証明書６３４）＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値Ａ｜｜検証値Ｂ｜｜検証値Ｃ｜｜検証値Ｄ｜｜検証値Ｅ））

図１３に示す検証基データ６５０及び図１４に示す検証基データ６７０の場合においても、各証明書は、上記と同様にして算出される。

[0218] （４）検知処理の動作

ここでは、図８のステップＳ２００に示す検知処理について、図１５及び図１６を用いて、説明する。図１５及び図１６は、検知処理を示すシーケンス図である。

[0219] 機器１００は、図８のステップＳ１００に示す初期設定処理を終えると工場から出荷され、ユーザの元へ送られる。ユーザが機器１００を使用し、各アプリを利用しているときには、機器１００内部では、保護制御モジュール１２０が復号ロード機能、改ざん検出機能、解析ツール検出機能などの機能

を制御し、各アプリを攻撃者による攻撃から保護する。ここでは、アプリ１１０の実行時に保護制御モジュール１２０の検証を行う場合を例に説明する。他のアプリ１１１、１１２、１１３、１１４の実行時に検証を行う場合も同様の動作であり、説明を省略する。

[0220] 保護制御モジュール１２０は、ＯＳ１８０からアプリ１１０を実行するコマンドを受信する（ステップＳ２０００）。このコマンドを受信すると、復号ロード部３０４は、暗号化されたアプリ１１０を復号する（ステップＳ２００１）。次に、アプリ分割部３１０は、復号して生成されたアプリ１１０を、検証基データ保持部３０８に保持している検証基データのそれぞれの分割識別情報に基づいて分割する（ステップＳ２００２）。分割識別情報に、３分割することが記載されていれば、アプリを３分割する。以下、アプリを３分割する場合について説明する。

[0221] 保護制御モジュール１２０の検知モジュール選択部３１１は、アプリ識別情報、分割データ及び検証基データの分配先の検知モジュールを選択する（ステップＳ２００３）。ここで、アプリ識別情報は、保護制御モジュール１２０がＯＳ１８０から受信したコマンドによる実行の対象であるアプリを識別する識別情報である。分割データは、アプリ分割部３１０による分割により生成された分割データである。また、検証基データは、検証基データ保持部３０８に保持されている検証基データのうち、生成された分割データに対応するものである。検証基データについては、図１２から図１４に一例を示している。

[0222] （４－１）検知モジュールの選択方法

図１７を用いて、検知モジュール選択部３１１による検知モジュールの選択方法を説明する。

[0223] 検知モジュール選択部３１１は、図１７に示す対応表３３０を保持している。

[0224] 検知モジュール選択部３１１は、検知モジュール選択部３１１が保持する対応表３３０を用いて、検知モジュール１３１、１３２、１３３、１３４、

１３５のうち、どの検知モジュールに分配するかを決定することにより、検知モジュールの選択を行う。

[0225] 検知モジュール選択部３１１が保持する対応表３３０には、検知モジュール１３１、１３２、１３３、１３４、１３５のうち、どの３つの検知モジュールを選択するかのすべての組合せのパターンが、Ｉｎｄｅｘに対応付けて、記述されている。

[0226] 図１７に示す対応表３３０は、Ｉｎｄｅｘと、検知モジュール識別子の組合せとの組を複数個含んでいる。Ｉｎｄｅｘは、対応する組合せを識別する識別子である。例えば、対応表３３０は、Ｉｎｄｅｘ３３１ａ「１」に対応して、検知モジュール１３１、１３２、１３３をそれぞれ識別する識別子「１３１」、「１３２」、「１３３」の組合せ３３２ａを含み、Ｉｎｄｅｘ３３１ｂ「２」に対応して、検知モジュール１３１、１３２、１３４をそれぞれ識別する識別子「１３１」、「１３２」、「１３４」の組合せ３３２ｂを含み、Ｉｎｄｅｘ３３１ｃ「３」に対応して、検知モジュール１３１、１３２、１３５をそれぞれ識別する識別子「１３１」、「１３２」、「１３５」の組合せ３３２ｃを含む。

[0227] ここで、各Ｉｎｄｅｘは、正の整数であり、Ｉｎｄｅｘ３３１ａ、３３１ｂ、３３１ｃ、・・・、は、「１」、「２」、「３」、・・・、「１０」である。これらの値は、「１」を初期値とし、その値に順に「１」を加算して得られたものである。

[0228] 検知モジュール選択部３１１は、乱数を生成し、生成した乱数を検知モジュールを選択するための選択情報とする。この乱数は、「１」から、対応表３３０に含まれる組の数までの整数の範囲からランダムに選択される。

[0229] 検知モジュール選択部３１１は、対応表３３０から、選択情報と同じ値を有するＩｎｄｅｘを決定し、対応表３３０から、決定したＩｎｄｅｘに対応する組合せを選択することにより、検知モジュールを選択する。例えば、検知モジュール選択部３１１は、選択情報が「１」である場合、対応表３３０から、Ｉｎｄｅｘ３３１ａ「１」に対応する組合せ３３２ａを選択する。組

合せ３３２ａは、識別子「１３１」、「１３２」及び「１３３」を含んでいるので、検知モジュール１３１、１３２、１３３が選択されたこととなる。

[0230] 以下、検知モジュール１３１、１３２、１３３の組合せを選択したものとして説明する。

[0231] 図１５へ戻り、検知処理の説明を続行する。

[0232] 保護制御モジュール１２０は、アプリ識別情報と、分割データと、分割データに対応する検証基データとを、選択した検知モジュールへ分配する。ここでは、一例として、検知モジュール１３１へアプリ識別情報「１１０」、アプリの分割データの１番目の情報（分割データ１（１１０ａ））、検証基データ６３０を送信し（ステップＳ２００４）、検知モジュール１３２へアプリ識別情報「１１０」、アプリの分割データの２番目の情報（分割データ２（１１０ｂ））、検証基データ６５０を送信し（ステップＳ２００５）、検知モジュール１３３へアプリ識別情報、アプリの分割データの３番目の情報（分割データ３（１１０ｃ））、検証基データ６７０を送信するものとする（ステップＳ２００６）。

[0233] 各検知モジュールは、保護制御モジュール１２０のアプリの復号処理の入力データ（つまり、暗号化アプリ）と分割データの対応が正しいか否かを受信した検証基データを用いて検証する（ステップＳ２００７）。具体的に、各検知モジュールは、検証基データ内のアプリ識別情報に対応する暗号化アプリのデータと、受信したアプリの分割データから検証値を生成する。そして、生成した検証値と受信した検証基データ内の検証値と比較し、両者が一致するか判断する。さらに、検証基データ内の証明書（復号処理証明書）の署名検証を行う。

[0234] 検証基データ内の証明書（復号処理証明書）の署名検証は、次のようにして行う。

[0235] Ｖｅｒｉｆｙ（署名公開鍵、証明書６３４、Ｈａｓｈ（検証値Ａ｜｜検証値Ｂ｜｜検証値Ｃ｜｜検証値Ｄ｜｜検証値Ｅ））

ここでは、一例として、図１２に示す検証基データ６３０を用いる場合を

示している。署名公開鍵は、管理装置２００の公開鍵であり、証明書６３４、検証値Ａ、検証値Ｂ、検証値Ｃ、検証値Ｄ及び検証値Ｅは、当該検知モジュールが受信した検証基データ６３０内に含まれているものである。また、Ｖｅｒｉｆｙ（ａ、ｂ、ｃ）は、公開鍵ａを用いて、データｃに対して、証明書ｂが正しいか否かを検証し、その検証結果を示す。検証結果は、検証が成功したか失敗したかを示す。

[0236] 各検知モジュールは、検証値が一致しない、又は、検証に失敗した場合には、保護制御モジュール１２０が改ざんされていると判定し（ステップＳ２００８でＹ）、管理装置２００の判断部２１０へ、分割データが改ざんされていることを示す監視結果を送信する（ステップＳ２００９）。各検知モジュールは、検証値が一致し、かつ、検証に成功した場合には、保護制御モジュール１２０が改ざんされていないと判定し（ステップＳ２００８でＮ）、分割データが改ざんされていないことを示す監視結果とともに、検証基データ内の分割識別情報を他の検知モジュールへ送信する（ステップＳ２０１０）。そして、各検知モジュールは、保護制御モジュール１２０から送信されたすべての分割データが正しいと検証されたか否かを確認する（ステップＳ２０１１）。

[0237] 以下、具体的に説明する。

[0238] 検知モジュール１３１は、分割識別情報６３１「（３、１）」を検知モジュール１３２及び検知モジュール１３３へ送信する。分割識別情報６３１「（３、１）」は、分割数が３であり、分割データがそのうちの１番目のデータであることを示した情報である。

[0239] 検知モジュール１３１は、検知モジュール１３２から分割識別情報６５１「（３、
２）」を受信し、検知モジュール１３３から分割識別情報６７１「（３、３）」を受信する。ここで、分割識別情報６５１「（３、２）」は、分割数が３であり、分割データがそのうちの２番目のデータであることを示した情報であり、分割識別情報６７１「（３、３）」は、分割数が３であり、分割デ

ータがそのうちの３番目のデータであることを示した情報である。検知モジュール１３１は、検証基データ６３０に含まれる判定情報６３２を参照することにより、アプリのデータが３分割されていることがわかる。また、検知モジュール１３１は、受信した分割識別情報６５１及び分割識別情報６７１の内容を確認することにより、２番目のデータと３番目のデータがそれぞれ検知モジュール１３２及び１３３により検証されたことを知ることができる。

[0240] よって、各検知モジュールは、保護制御モジュール１２０から送信されたすべての分割データがいずれかの検知モジュールにより検証されたことを確認することができる。

[0241] すべての分割データが正しいと検証されていない場合、又は、すべての分割データが１つの検知モジュールに送信されていた場合には、保護制御モジュール１２０が不正な動作を行ったとし、保護制御モジュール１２０が改ざんされていると判定し（ステップＳ２０１１でＹ）、判断部２１０へ、保護制御モジュール１２０が改ざんされていることを示す判断結果を送信する（ステップＳ２０１２）。

[0242] 保護制御モジュール１２０が改ざんされていない判定する場合（ステップＳ２０１１でＮ）、処理を終了する。この場合に、判断部２１０へ、保護制御モジュール１２０が改ざんされていないことを示す判断結果を送信してもよい。

[0243] （５）検証基データの更新処理の動作

検知システム１０では、機器１００に新たなアプリを追加してインストールする場合、保護制御モジュール１２０内の検証基データを更新する必要がある。保護制御モジュール１２０は、アプリが追加された場合、管理装置２００に検証基データの生成を依頼し、管理装置２００が生成した新しい検証基データを受信して保持する。

[0244] ここでは、図１８に示すシーケンス図を用いて、機器１００に新たなアプリ（「アプリ１１５」と記載する。）を追加してインストール場合を具体例

として用い、検証基データの更新処理の動作について説明する。

[0245] 機器１００に新たなアプリ１１５がダウンロードされると、保護制御モジュール１２０は、ＯＳ１８０からアプリ１１５を受信する（ステップＳ３００１）。保護制御モジュール１２０は、暗復号鍵保持部３０７に保持されている暗復号鍵を用いてアプリ１１５を暗号化する（ステップＳ３００２）。そして、保護制御モジュール１２０は、アプリ１１５を識別するアプリ識別情報と暗号化されたアプリ１１５と検証基データの送付依頼とを管理装置２００へ送信する（ステップＳ３００３）。

[0246] 管理装置２００は、アプリ識別情報と暗号化されたアプリ１１５と検証基データの送付依頼とを受信し（ステップＳ３００３）、受信した暗号化されたアプリ１１５を保護制御モジュール保持部６１１で保持している保護制御モジュール１２０の暗復号鍵で復号する。そして、上述したように、復号したアプリ１１５を含む新たな検証基データを生成する（ステップＳ３００４）。管理装置２００は、新たな検証基データを保護制御モジュール１２０へ送信する（ステップＳ３００５）。保護制御モジュール１２０は、新たな検証基データを受信し、受信した検証基データを検証基データ保持部３０８に記憶する（ステップＳ３００６）。

[0247] ２．３ 検知システム１０の効果

検知システム１０では、保護制御モジュール１２０による暗号化アプリの復号処理を検証するので、保護制御モジュール１２０が保持する暗復号鍵を用いることなく、保護制御モジュールが改ざんされているか否かを判定することができる。

[0248] また、各検知モジュールは、分割データを検証するので、各検知モジュールがアプリのすべてのデータを知ることなく検証することができる。

[0249] これにより、検知モジュールが改ざんされ不正動作をしたとしても、保護制御モジュール１２０の情報やアプリの情報が漏洩することがないので、システムの安全性を高めることができる。

[0250] また、本発明によれば、検知モジュール群１３０に含まれる全ての検知モ

ジュールを選択するのではなく、保護制御モジュール１２０は、検知モジュール群１３０の中から、選択した検知モジュールに、検知処理を実行させるので、保護制御モジュール１２０が選択をしなかった検知モジュールが不正動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュール１２０に対する検知処理には影響せず、保護制御モジュールが改ざんされているかを検証することができる。

[0251] ３．実施の形態３

本発明に係る別の実施の形態としての検知システム１０ａ（図示していない）について説明する。

[0252] 検知システム１０ａは、実施の形態２の検知システム１０と同様の構成を有している。ここでは、検知システム１０との相違点を中心として説明する。

[0253] ３．１　概要

検知システム１０では、保護制御モジュールによる検知動作の実行の指示先のｄ個の検知モジュールのうち１つでも攻撃されると、保護制御モジュールが改ざんされているかを検証することができない。

[0254] これに対して、検知システム１０ａでは、検知システム１０における分割データの生成に代えて、閾値秘密分散法（Threshold Secret Sharing Scheme）を用いて複数の分散データを生成し、生成した分散データの分配先であるいくつかの検知モジュールが攻撃されたとしても、ｄ個の検知モジュールのうち、ｋ（ｋは、正の整数であり、ｄより小さい。）個の検知モジュールが改ざんされていなければ、保護制御モジュールが改ざんされているかを検証できる。ここで、ｄを検知動作数と呼び、ｋを検知閾値と呼ぶ。

[0255] ここで用いる閾値秘密分散法は、次の通りである。

[0256] 管理装置２００のデータ分割部６０８は、ランダムに整数ａ１、ａ２、・・・、ａk-1 を選択する。整数ａ１、ａ２、・・・、ａk-1 をパラメタと呼び、パラメタ（ａ１、ａ２、・・・、ａk-1 ）と表す。また、素数ｒを選択

する。

[0257] こうして、データ分割部６０８は、図２３の式１に示すように、（ｋ－１）次多項式を設定する。式１において、ｓは、定数項であり、ｓは、各アプリのデータである。整数ａ１、ａ２、・・・、ａk-1 は、それぞれ、次数が１以上の項の係数である。

[0258] また、データ分割部６０８は、ｒ｜ｐ－１となるように、素数ｐを選択し、乗法群Ｚp*での位数がｒとなる要素ｇを定める。

[0259] 次に、図２０に示す式３により、ｃ０、ｃ１、・・・、ｃk-1 を計算する。

[0260] ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1 を検証値（ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1 ）と表す。

[0261] 管理装置２００は、検証値（ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1 ）を保護制御モジュール１２０へ出力する。

[0262] 保護制御モジュール１２０のアプリ分割部３１０は、図２３の式１に示す（ｋ－１）次多項式を用いて、式２に示すように、アプリ毎に、分散データｗｊ＝ｆ（ｊ）（ｊ＝１、２、・・・、ｄ）を生成する。保護制御モジュール１２０は、選択したｄ個の検知モジュールに、それぞれ、分散データｗｊ＝ｆ（ｊ）（ｊ＝１、２、・・・、ｄ）を送信する。また、ｄ個の検知モジュールに、それぞれ、検証値（ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1 ）を送信する。

[0263] 各検知モジュールは、図２３に示す式４が成立するか否かを判断することにより、送信された分散データｗｊが正しいか否かを検証する。式４が成立する場合には、分散データｗｊが正しく生成されたと判断する。式４が成立しない場合には、分散データｗｊが正しく生成されていないと判断する。

[0264] また、検知モジュールは、他の検知モジュールから検証結果を受け取り、受け取った検証結果及び自身の検証結果により、ｋ個以上の検知モジュールにおいて、式４による検証が成功したことを示す場合に、保護制御モジュール１２０は、改ざんされていないと決定する。一方、ｋ個未満の検知モジュ

ールにおいて、式４による検証が成功したことを示す場合に、保護制御モジュール１２０は、改ざんされていないと決定しない。

[0265] この秘密分散法は、検証可能閾値秘密分散法（verifiable secret sharing scheme)とも呼ばれ、ｄより小さいｋ個以上のどの分散データを用いても、元のデータ（ここでは、コンピュータプログラム）を復元することができるように、元のデータを分散する秘密分散法である

なお、秘密分散法及び閾値秘密分散法については、非特許文献１の２０９ページから２１９ページに詳しく説明されているので、ここでの説明は省略する。

[0266] ３．２ 動作

（１）初期設定処理の動作

初期設定処理について説明する。検知システム１０ａの初期設定処理は、図９に示す検知システム１０の初期設定処理と類似している。なお、ここでは、検知システム１０の初期設定処理との相違点を中心として、図１９に示すシーケンス図を用いて説明する。

[0267] 図１９に示すシーケンス図におけるステップＳ１００１～Ｓ１００５は、それぞれ、図９における対応するステップと同じであるので、説明を省略する。

[0268] ステップＳ１００５の次に、管理装置２００は、検証基データの生成処理を実行する（ステップＳ１００６ａ）。検証基データの生成処理の詳細については、後述する。検証基データの生成処理が完了すると、管理装置２００は、生成した検証基データ、パラメタ（ａ１、ａ２、・・・、ａk-1）及び素数ｒを保護制御モジュール１２０へ送信する（ステップＳ１００７ａ）。保護制御モジュール１２０は、管理装置２００から検証基データ、パラメタ（ａ１、ａ２、・・・、ａk-1）及び素数ｒを受信し（ステップＳ１００７ａ）、受信した検証基データ、パラメタ（ａ１、ａ２、・・・、ａk-1）及び素数ｒを検証基データ保持部３０８へ記憶する（ステップＳ１００８ａ）。

[0269] （２）検証基データの生成処理

検知システム１０ａの検証基データの生成処理の動作について、図２０に示すフローチャートを用いて説明する。ここで説明する検証基データの生成処理は、図１９に示すステップＳ１００６ａの詳細である。検知システム１０ａの検証基データの生成処理は、図１０に示す検知システム１０の検証基データの生成処理と類似している。ここでは、その相違点について説明する。

[0270] 図２０に示すフローチャートにおけるステップＳ１１０１は、図１０における対応するステップと同じであるので、説明を省略する。

[0271] 検証基データ配布部２２０のデータ分割部６０８は、アプリ毎に、図２３の式１に示す（ｋ－１）次多項式ｆ（ｘ）の各項の係数ａ１、ａ２、・・・、ａk-1 をランダムに選択する。各係数は、それぞれ整数である。また、素数ｒを選択する（ステップＳ１１０２ａ）。

[0272] 次に、データ分割部６０８は、アプリ毎に、ｒ｜ｐ－１となるように、素数ｐを選択し、乗法群Ｚp*での位数がｒとなる要素ｇを定め、図２０に示す式３により、ｃ０、ｃ１、・・・、ｃk-1 を計算する。また、データ分割部６０８は、アプリ毎に生成した検証値（ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1）を用いて、上述したように、複数のアプリについて生成した複数の検証値を結合して結合体を生成し、生成した結合体にハッシュ関数による演算を施し、得られたハッシュ値に、署名秘密鍵を用いてデジタル署名を施して、証明書を生成する。

[0273] （証明書）＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値｜｜検証値｜｜・・・｜｜検証値））

なお、検証値を結合する際に、各検証値は、ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1 をこの順序で結合したものとする（ステップＳ１１０３ａ）。

[0274] 次に、検証基データ生成部６１０は、１個の検証基データを生成する。検証基データは、図２２に示すように、分割識別情報、判定情報、複数の検証値組及び証明書（復号処理証明書）を含む。各検証値組は、アプリ識別情報

及び検証値を含む（ステップＳ１１０４ａ）。なお、分割識別情報及び判定情報については、後述する。

[0275] 図２１に、アプリのデータを分散する場合における動作概要図を示す。ここでは、アプリのデータに対し、閾値秘密分散法を用いて、４つの分散データを生成し、このうち、３つの分割データを用いて、元のアプリのデータが復元できるようにした例である。

[0276] 保護制御モジュール１２０のアプリ分割部３１０は、閾値秘密分散法を用いて、アプリ１１０、１１１、１１２、１１３及び１１４から、各アプリについて、各アプリのデータを分散して、一例として、４個の分散データ１、分散データ２、分散データ３及び分散データ４を生成する。

[0277] アプリ１１０から分散データを生成する場合について、具体的に説明すると、一例として図２１に示すように、アプリ分割部３１０は、閾値秘密分散法を用いて、アプリのデータ１１０「ｓ」を分散して、図２１に示す式２－１、式２－２、式２－３及び式２－４により、４個の分散データ１（１１０ｄ）「ｗ１ ＝ｆ（１）」、分散データ２（１１０ｅ）「ｗ２ ＝ｆ（２）」、分散データ３（１１０ｆ）「ｗ３ ＝ｆ（３）」及び分散データ４（１１０ｇ）「ｗ４ ＝ｆ（４）」を生成する。

[0278] 検知システム１０においては、生成された分割データの数と同数の検証基データが生成される。これに対して、検知システム１０ａにおいては、１個の検証基データが生成される。検証基データ生成部６１０により生成される検証基データの一例として、図２２に、検証基データ６９０を示す。

[0279] 検証基データ６９０は、図２２に示すように、分割識別情報６９１、判定情報６９２、複数の検証値組６９３ａ～６９３ｅ及び証明書６９４から構成されている。各検証値組は、アプリ識別情報及び検証値から構成されている。

[0280] ここで、分割識別情報６９１は、アプリ分割部３１０において生成される分散データの数ｄを示す。ここでは、一例として、分割識別情報６９１は、「４」である。

[0281] また、判定情報６９２は、検知閾値ｋである。ここでは、一例として、判定情報６９２は、「３」である。

[0282] アプリ識別情報は、対応するアプリを識別するための情報である。

[0283] 検証値は、上述した通りであり、（ｐ、ｇ、ｃ０、ｃ１、・・・、ｃk-1）である。

[0284] 証明書９６４は、上述した通りであり、複数の検証値を結合して得られた結合体にハッシュ関数による演算を施し、得られたハッシュ値に、署名秘密鍵を用いてデジタル署名を施して、生成した証明書である。

[0285] （３）検知処理の動作

検知システム１０ａの検知処理の動作について、図２３から図２４に示すシーケンス図を用いて説明する。

[0286] 図２２に示す検知システム１０ａの検知処理におけるステップＳ２１００及びＳ２１０１の動作は、検知システム１０の図１５に示すステップＳ２０００及びＳ２００１の動作と同様の動作であるため、説明を省略する。以下で、ステップＳ２１０２からの処理について説明する。

[0287] 保護制御モジュール１２０のアプリ分割部３１０は、検証基データ保持部３０８に保持しているパラメタ（ａ１、ａ２、・・・、ａk-1）及び素数ｒを用いて、図２３の式１に示す（ｋ－１）次多項式を設定する。式１において、ｓは、アプリ１１０のデータである。また、定数項ｓ以外の他の一次以上の項は、それぞれ、ａ１、ａ２、・・・、ａk-1 を係数とする。アプリ分割部３１０は、アプリ毎に、図２３の式２に示すように、ｄ個の分散データｗｊ（ｊ＝１、２、・・・、ｄ）を演算して生成する。

[0288] ここで、ｄは、検証基データ保持部３０８に保持している検証基データに含まれる分割識別情報により指定されている。また、ｋは、検証基データに含まれる判定情報により指定されている（ステップＳ２１０２）。

[0289] 一例として、ｄが「４」であり、ｋが「３」である場合には、アプリ分割部３１０により、４個の分散データが生成される。また、３個以上の分散データを用いた検証に成功すれば、保護制御モジュールの検証に成功する。

[0290] 保護制御モジュール１２０は、実施の形態２の検知モジュール選択部３１１に代えて、検知モジュール選択部３１１ａを含む。検知モジュール選択部３１１ａは、検知モジュール選択部３１１と類似した構成を有している。ここでは、相違点を中心として説明する。

[0291] 保護制御モジュール１２０の検知モジュール選択部３１１ａは、アプリ識別情報、分散データ及び検証基データの分配先の検知モジュールを選択する（ステップＳ２１０３）。ここで、アプリ識別情報は、保護制御モジュール１２０がＯＳ１８０から受信したコマンドによる実行の対象であるアプリを識別する識別情報である。分散データは、アプリ分割部３１０により生成された分散データである。また、検証基データは、検証基データ保持部３０８に保持されている検証基データである。検証基データについては、図２２に一例として検証基データ６９０を示している。

[0292] 図２５を用いて、検知モジュール選択部３１１ａによる検知モジュールの選択方法を説明する。

[0293] 検知モジュール選択部３１１ａは、図２５に示す対応表３３０ａを保持している。

[0294] 検知モジュール選択部３１１ａは、対応表３３０ａを用いて、検知モジュール１３１、１３２、１３３、１３４、１３５のうち、どの検知モジュールにアプリ識別情報、分散データ及び検証基データを分配するかを決定することにより、検知モジュールの選択を行う。

[0295] 図２５に示すように、検知モジュール選択部３１１ａが保持する対応表３３０ａには、検知モジュール１３１、１３２、１３３、１３４、１３５のうち、どの４つの検知モジュールを選択するかのすべての組合せのパターンが、Ｉｎｄｅｘに対応付けて、記述されている。

[0296] 図２４に示す対応表３３０ａは、図１７に示す対応表３３０と同様の構成を有している。対応表３３０ａは、Ｉｎｄｅｘと検知モジュール識別子の組合せとの組を複数個含んでいる。Ｉｎｄｅｘは、対応する組合せを識別する識別子である。例えば、対応表３３０ａは、Ｉｎｄｅｘ３３１ｄ「１」に対

応して、検知モジュール１３１、１３２、１３３、１３４をそれぞれ識別する識別子「１３１」、「１３２」、「１３３」、「１３４」の組合せ３３２ｄを含み、Ｉｎｄｅｘ３３１ｅ「2」に対応して、検知モジュール１３１、１３２、１３３、１３５をそれぞれ識別する識別子「１３１」、「１３３」、「１３４」、「１３５」の組合せ３３２ｅを含み、Ｉｎｄｅｘ３３１ｆ「３」に対応して、検知モジュール１３１、１３２、１３４、１３５をそれぞれ識別する識別子「１３１」、「１３２」、「１３４」、「１３５」の組合せ３３２ｆを含み、Ｉｎｄｅｘ３３１ｇ「４」に対応して、検知モジュール１３１、１３３、１３４、１３５をそれぞれ識別する識別子「１３１」、「１３３」、「１３４」、「１３５」の組合せ３３２ｇを含み、Ｉｎｄｅｘ３３１ｈ

「５」に対応して、検知モジュール１３２、１３３、１３４、１３５をそれぞれ識別する識別子「１３２」、「１３３」、「１３４」、「１３５」の組合せ３３２ｈを含む。

[0297] 検知モジュール選択部３１１ａは、対応表３３０ａから、選択情報と同じ値を有するＩｎｄｅｘを決定し、対応表３３０ａから、決定したＩｎｄｅｘに対応する組合せを選択することにより、検知モジュールを選択する。例えば、検知モジュール選択部３１１ａは、選択情報が「１」である場合、対応表３３０ａから、Ｉｎｄｅｘ３３１ｄ「1」に対応する組合せ３３２ｄを選択する。組合せ３３２ｄは、識別子「１３１」、「１３２」、「１３３」及び「１３４」を含んでいるので、検知モジュール１３１、１３２、１３３及び１３４が選択されたこととなる。 以下、検知モジュール１３１、１３２、１３３及び１３４の組合せを選択したものとして説明する。

[0298] 保護制御モジュール１２０は、アプリ識別情報と、分散データと、検証基データとを、選択した検知モジュールへ分配する。ここでは、検知モジュール１３１へアプリ識別情報、アプリの１番目の分散データ（分散データ１（１１０ｄ））及び検証基データを送信し（ステップＳ２１０４）、検知モジュール１３２へアプリ識別情報、アプリの２番目の分散データ（分散データ

２（１１０ｅ））及び検証基データを送信し（ステップＳ２１０５）、検知モジュール１３３へアプリ識別情報、アプリの３番目の分散データ（分散データ３（１１０ｆ））及び検証基データを送信し（ステップＳ２１０６）、検知モジュール１３４へアプリ識別情報、アプリの４番目の分散データ（分散データ４（１１０ｇ））及び検証基データを送信する（ステップＳ２１０７）。

[0299] 検知モジュール１３１、１３２、１３３及び１３４の各検証部４０４は、図２３に示す式４が成立するか否かを判断する。また、各検証部４０４は、検証基データに含まれている証明書の署名検証を行う（ステップＳ２１０８）。

[0300] 各検知モジュールは、式４が成立しない、又は、検証に失敗した場合には、保護制御モジュール１２０が改ざんされていると判定し（ステップＳ２０１９でＹ）、管理装置２００の判断部２１０へ、分散データが正しくないことを示す監視結果を送信する（ステップＳ２１１０）。各検知モジュールは、式４が成立し、かつ、検証に成功した場合には、分散データが正しいと決定し（ステップＳ２１０９でＮ）、分散データが正しいことを示す監視結果と、当該検知モジュールの識別子とを他の検知モジュールへ送信する（ステップＳ２１１１）。次に、各検知モジュールは、他の検知モジュールから受け取った監視結果及び自身の監視結果により、ｋ個以上の検知モジュールにおいて、式４による検証が成功したか否かを判断し（ステップＳ２１１２）、ｋ個以上の検知モジュールにおいて、式４による検証が成功したと判断する場合（ステップＳ２１１２でＮ）、保護制御モジュール１２０が改ざんされていないと決定し、処理を終了する。ｋ個以上の検知モジュールにおいて、式４による検証が成功したと判断しない場合（ステップＳ２１１２でＹ）、保護制御モジュール１２０が改ざんされたことを示す判断結果を管理装置２００の判断部２１０へ送信する（ステップＳ２１１３）。

[0301] 検証部４０４は、分散データの配布先のｄ個の検知モジュールのうち、自身の検知モジュールを含め、閾値であるｋ個以上の検知モジュールにより、

分散データが正しいことを示す監視結果を受け取った場合、保護制御モジュール１２０は改ざんされていないと判断する。この場合に、ｋ個未満の検知モジュールが、不正動作を行って、分散データが正しいにもかかわらず、分散データが改ざんされているとする監視結果を検証部４０４へ送信した場合においても、ｋ個以上の検知モジュールが、分散データが正しいと決定しているので、検証部４０４は、保護制御モジュール１２０は正常であると判断する。

[0302] 検証部４０４は、分散データの配布先のｄ個の検知モジュールのうち、（ｄ－ｋ＋１）個以上の検知モジュールにより、分散データが正しくないことを示す監視結果を受け取った場合、保護制御モジュール１２０は改ざんされていると判断する。

[0303] なお、管理装置２００の判断部２１０が上記の判断を行うとしてもよい。

[0304] 判断部２１０は、分散データの配布先のｄ個の検知モジュールのうち、閾値であるｋ個以上の検知モジュールにより、分散データが正しいことを示す監視結果を受け取った場合、保護制御モジュール１２０は改ざんされていないと判断する。この場合に、ｋ個未満の検知モジュールが、不正動作を行って、分散データが正しいにもかかわらず、分散データが改ざんされているとする監視結果を判断部２１０へ送信した場合においても、ｋ個以上の検知モジュールが、分散データが正しいと決定しているので、判断部２１０は、保護制御モジュール１２０は正常であると判断する。

[0305] また、判断部２１０は、分散データの配布先のｄ個の検知モジュールのうち、（ｄ－ｋ＋１）個以上の検知モジュールにより、分散データが正しくないことを示す監視結果を受け取った場合、保護制御モジュール１２０は改ざんされていると判断する。

[0306] ３．３　検知システム１０ａの効果

検知システム１０によると、ｄより小さいｋ個以上の検知モジュールによる監視結果を用いて、保護制御モジュールの改ざんを検出することができる。従って、（ｄ－ｋ）個以下の検知モジュールが改ざんされている場合であ

っても、保護制御モジュールの改ざんを検出することができる。

[0307] このように、検知システム１０ａによると、分散データの分配先の先の検知モジュールが不正動作を行ったとしても、保護制御モジュールが正常動作を行ったかの判断ができ、システムの安全性を維持することができる。

[0308] また、復号したアプリのデータの分散に閾値秘密分散法を用いることで、システムの安全性を理論的に評価することができる。

[0309] ４．実施の形態４

本発明に係る別の実施の形態としての検知システム１０ｂについて説明する。

[0310] 検知システム１０ｂは、実施の形態２の検知システム１０と同様の構成を有している。ここでは、検知システム１０との相違点を中心として説明する。

[0311] ４．１ 概要

検知システム１０では、保護制御モジュールが分割データの分配先の検知モジュールを選択している。しかし、保護制御モジュールが不正動作を行い、さらに、どの検知モジュールが不正動作を行うかを知っている場合、不正動作を行う検知モジュールに分割データを分配することにより、保護制御モジュールの不正動作を検出できないようにすることができる。そこで、検知システム１０ｂでは、検知モジュールが分割データの分配先の検知モジュールを決定することにより、保護制御モジュールが分配先の検知モジュールを恣意的に選択できないようにする。

[0312] ４．２ 動作

（１）検知処理の動作

ここでは、検知システム１０ｂにおける検知処理の動作について、図２６から図２９に示すシーケンス図を用いて説明する。検知システム１０ｂにおけるステップＳ２２００からステップＳ２２０２までの動作は、検知システム１０における図１５に示すステップＳ２０００からステップＳ２００２の動作と同様であるため、説明を省略する。以下で、ステップＳ２２０３から

の処理について説明する。

[0313] 保護制御モジュール１２０は、各検知モジュールへ検知処理の実行を通知する（ステップＳ２２０３）。

[0314] 保護制御モジュール１２０からの通知を受信後、各検知モジュールの検証部４０４は、乱数を生成する（ステップＳ２２０４）。送信部４０２は、生成した乱数を、他の全ての検知モジュールへ送信する（ステップＳ２２０５）。各検知モジュールは、他の全ての検知モジュールから乱数を受信し（ステップＳ２２０５）、検証部４０４は、受信した全ての乱数及び自ら生成した乱数を合計して合計値を算出し、算出した合計値を用いて、検証部４０４が保持する対応表３３０ｂ（後述する）のどのＩｎｄｅｘを選択するか示す選択情報を計算する（ステップＳ２２０６）。

[0315] 検証部４０４は、一例として図３０に示す対応表３３０ｂを保持している。対応表３３０ｂは、保護制御モジュール１２０の検知モジュール選択部３１１で保持している対応表３３０と同じものである。

[0316] 各検知モジュールは、対応表３３０ｂからＩｎｄｅｘの最大値を取得する。対応表３３０ｂにおいては、「１０」がＩｎｄｅｘの最大値である。次に、算出した合計値に対し、取得した最大値で法をとった値を選択情報として計算する。

[0317] 選択情報＝　（ｒ１　＋ｒ２　＋・・・＋ｒｎ）　ｍｏｄ　（Ｉｎｄｅｘの最大値）

ここで、ｒ１、ｒ２、・・・、ｒｎは、それぞれ、ｎ個の検知モジュールにより生成された乱数である。また、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0318] 例えば、すべての乱数の合計値が「２１」である場合、「１０」で法をとった値は

「１」となるので、選択情報は、「１」である。また、すべての乱数の合計値が「３０」である場合、「１０」で法をとった値は「０」となるので、選択情報は、「１０」である。

[0319] 各検知モジュールは、選択情報を保護制御モジュール１２０へ送信する（ステップＳ２２０７）。

[0320] 保護制御モジュール１２０は、受信した選択情報のいずれか一つに基づいて、図１７に示す対応表３３０から、当該選択情報に等しいＩｎｄｅｘを選択し、選択したＩｎｄｅｘに対応する検知モジュール識別子の組を選択する（ステップＳ２２０８）。

[0321] これ以降のステップＳ２２０９からステップＳ２２１７の動作は、実施の形態２における図１５～図１６に示すステップＳ２００４からステップＳ２０１２までの動作と同様の動作であるため、説明を省略する。

[0322] ４．３　検知システム１０ｂの効果

検知システム１０ｂにより、検知モジュールが連携して、分割データを分配する検知モジュールを検知モジュールが決定するので、保護制御モジュールは、分割データを分配する検知モジュールを恣意的に選択できない。また、検知モジュールのすべてが不正動作を行わない限り、検知モジュールの選択先を決定できない。これにより、保護制御モジュールが不正動作を行い、分割データを分配する検知モジュールを恣意的に選択することを防止し、システムの安全性を向上することができる。

[0323] ５．実施の形態５

本発明に係る別の実施の形態としての検知システム１０ｃについて説明する。

[0324] 検知システム１０ｃは、実施の形態２の検知システム１０と同様の構成を有している。ここでは、検知システム１０との相違点を中心として説明する。

[0325] ５．１　概要

検知システム１０ｃでは、保護制御モジュール１２０において、複数の復号サブプロセスから構成される復号処理のプロセスを経ることにより、暗号化アプリが復号される。このとき、各復号サブプロセスの入出力対応を検証することにより、保護制御モジュール１２０が改ざんされているかを判断す

る。

[0326] 図３１は、保護制御モジュール１２０における複数の復号サブプロセスから構成される復号処理３５０の概要を示す図である。検知システム１０ｃでは、一例として、復号処理３５０のプロセスは、復号部分処理１（３５１）、復号部分処理２（３５２）、及び復号部分処理３（３５３）の３個の復号サブプロセスから構成される。なお、４個以上の復号部分処理の復号サブプロセスから構成されるとしてもよい。

[0327] ここで、複数個の復号サブプロセスから構成される復号処理の例は、ＤＥＳ（Data Encryption Standard）及びＡＥＳ（Advanced Encryption Standard）である。

[0328] 復号部分処理１（３５１）は、暗号化アプリのデータ３５５を入力データとして受け取り、復号して中間値１（３５６）を生成し、中間値１（３５６）を出力データとして復号部分処理２（３５２）へ出力する。復号部分処理２（３５２）は、中間値１（３５６）を入力データとして受け取り、復号して中間値２（３５７）を生成し、中間値２（３５７）を出力データとして復号部分処理３（３５３）へ出力する。復号部分処理３（３５３）は、中間値２（３５７）を入力データとして受け取り、復号してアプリのデータ（３５８）を生成し、アプリのデータ（３５８）を出力データとして出力する。

[0329] 各検知モジュールは、復号部分処理ごとに生成された検証データを用いて、各復号部分処理の入出力の対応を検証する。なお、安全性の観点から、１つの検知モジュールが３個の復号部分処理についてすべて検証するのではなく、３個の検知モジュールが、それぞれ異なる復号部分処理を検証することが望ましい。一般的に、復号処理は、複数の復号部分処理から構成され、各復号部分処理の入出力の対応を、復号部分処理の数と同数の検知モジュールが、それぞれ異なる復号部分処理について検証することが望ましい。なお、復号部分処理の数より多い数の検知モジュールが、復号部分処理について検証するとしてもよい。この場合には、複数の検知モジュールが一つの復号部

分処理について検証を行うこととなる。

[0330] ５．２　構成

検知システム１０ｃの管理装置２００は、検知システム１０の管理装置２００が備える検証基データ配布部２２０に代えて、検証基データ配布部２２０ａを有する。検証基データ配布部２２０ａは、検知システム１０の管理装置２００が備える検証基データ配布部２２０と類似する構成を有している。ここでは、相違点を中心として説明する。

[0331] （１）検証基データ配布部２２０ａの構成

図３２は、検知システム１０ｃにおける検証基データ配布部２２０ａの機能構成を示す機能ブロック図である。検知システム１０における検証基データ配布部２２０と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。

[0332] 検知システム１０における検証基データ配布部２２０と比較すると、検証基データ配布部２２０ａは、データ分割部６０８を備えていない。また、検証基データ配布部２２０には存在しないソフトウェア実行部６２１を備える。

[0333] ソフトウェア実行部６２１は、保護制御モジュール保持部６１１に保持されている保護制御モジュールを用いて暗号化アプリを復号し、復号処理プロセスを構成する複数のサブ復号プロセスにおいて、中間値１、中間値２及び復号されたアプリのデータを取得する。

[0334] （検証基データのデータ構造）

また、検知システム１０ｃでは、検証基データ配布部２２０ａが生成する検証基データの構成が検知システム１０の検証基データの構成と異なる。

[0335] 図３３は、検知システム１０ｃにおける検証基データの一例としての、検証基データ２４０のデータ構成図である。

[0336] 検証基データ２４０は、図３３に示すように、復号部分処理１に関するデータ２４１ａ、復号部分処理２に関するデータ２４１ｂ及び復号部分処理３に関するデータ２４１ｃを含む。この検証基データは、保護制御モジュール

１２０の検証基データ保持部３０８に保持される。

[0337] （ａ）復号部分処理１に関するデータ２４１ａは、図３３に示すように、判定情報２４２ａ、複数の検証値組２４３ａ～２４７ａ、証明書２４８ａ及び復号部分識別子２４９ａから構成されている。

[0338] 判定情報２４２ａは、復号部分処理のすべてが検証されたかを判定するための情報であり、復号サブプロセスの数が記載される。例えば、復号処理プロセスが３個の復号サブプロセスから構成されている場合、「３」と記載されている。

[0339] 複数の検証値組２４３ａ～２４７ａの数は、アプリの数と同一であり、複数の検証値組２４３ａ～２４７ａは、それぞれ、アプリ１１０、１１１、１１２、１１３及び１１４に対応している。各検証値組は、アプリ識別情報、データ及び検証値を含む。

[0340] 検証値組に含まれるアプリ識別情報は、対応するアプリを識別する識別子である。

[0341] 検証値組に含まれるデータは、対応する暗号化アプリのデータである。

[0342] 検証値組に含まれる検証値は、暗号化アプリのデータ３５５と復号部分処理１（３５１）の出力データである中間値１（３５６）とから生成した復号検証値である。検証値は、保護制御モジュール１２０が正常動作した際のそれぞれの復号部分処理１（３５１）の入力データと出力データとを結合して得られた結合体に対して、ハッシュ関数による演算を施して得られたハッシュ値である。

[0343] 検証値＝Ｈａｓｈ（復号部分処理１（３５１）の入力データ｜｜復号部分処理１（３５１）の出力データ）

ここでは、検証値としてハッシュ値を使用したが、これに限定するものではなく、次に示すように、署名などを用いてもよい。

[0344] 検証値＝Ｓｉｇｎ（署名秘密鍵、（復号部分処理１（３５１）の入力データ｜｜復号部分処理１（３５１）の出力データ））

証明書２４８ａは、復号処理証明書である。復号処理証明書は、復号部分

処理１に関するデータ２４１ａに含まれる全ての検証値を結合し、これらの複数の検証値を結合して得られた結合体にハッシュ関数による演算を施してハッシュ値を計算し、計算したハッシュ値に対して、署名秘密鍵保持部６０６の署名秘密鍵を用いて、デジタル署名アルゴリズムを施して、生成した署名である。

[0345] 証明書２４８ａ＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値｜｜検証値｜｜、・・・、検証値｜｜検証値））

復号部分識別子２４９ａは、復号部分処理１（３５１）を識別する識別子である。一例として、復号部分識別子２４９ａは、「００１」である。

[0346] （ｂ）復号部分処理２に関するデータ２４１ｂは、図３３に示すように、判定情報２４２ｂ、複数の検証値組２４３ｂ～２４７ｂ、証明書２４８ｂ及び復号部分識別子２４９ｂから構成されている。

[0347] 判定情報２４２ｂは、復号部分処理のすべてが検証されたかを判定するための情報であり、復号サブプロセスの数が記載される。例えば、復号処理プロセスが３個の復号サブプロセスから構成されている場合、「３」と記載されている。

[0348] 複数の検証値組２４３ｂ～２４７ｂの数は、アプリの数と同一であり、複数の検証値組は２４３ｂ～２４７ｂ、それぞれ、アプリ１１０、１１１、１１２、１１３及び１１４に対応している。各検証値組は、アプリ識別情報、データ及び検証値を含む。

[0349] 検証値組に含まれるアプリ識別情報は、対応するアプリを識別する識別子である。

[0350] 検証値組に含まれるデータは、対応する暗号化アプリから生成された中間値１である。

[0351] 検証値組に含まれる検証値は、中間値１（３５６）と復号部分処理２（３５２）の出力データである中間値２（３５７）とから生成した復号検証値である。中間値１（３５６）及び中間値２（３５７）は、ソフトウェア実行部６２１が、アプリの復号処理を実行することにより取得される。検証値は、

保護制御モジュール１２０が正常動作した際のそれぞれの復号部分処理２（３５２）の入力データと出力データとを結合して得られた結合体に対して、ハッシュ関数による演算を施して得られたハッシュ値である。

[0352] 検証値＝Ｈａｓｈ（復号部分処理２（３５２）の入力データ｜｜復号部分処理２（３５２）の出力データ）

ここでは、検証値としてハッシュ値を使用したが、これに限定するものではなく、次に示すように、署名などを用いてもよい。

[0353] 検証値＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（復号部分処理２（３５２）の入力データ｜｜復号部分処理２（３５２）の出力データ））

証明書２４８ａは、復号処理証明書である。復号処理証明書は、復号部分処理２に関するデータ２４１ｂに含まれる全ての検証値を結合し、これらの複数の検証値を結合して得られた結合体にハッシュ関数による演算を施してハッシュ値を計算し、計算したハッシュ値に対して、署名秘密鍵保持部６０６の署名秘密鍵を用いて、デジタル署名アルゴリズムを施して、署名である。

[0354] 証明書２４８ｂ＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値｜｜検証値｜｜、・・・、検証値｜｜検証値））

復号部分識別子２４９ｂは、復号部分処理２（３５２）を識別する識別子である。一例として、復号部分識別子２４９ｂは、「００２」である。

[0355] （ｃ）復号部分処理３に関するデータ２４１ｃは、図３３に示すように、判定情報２４２ｃ、複数の検証値組２４３ｃ～２４７ｃ、証明書２４８ｃ及び復号部分識別子２４９ｃから構成されている。

[0356] 判定情報２４２ｃは、復号部分処理のすべてが検証されたかを判定するための情報であり、復号サブプロセスの数が記載される。例えば、復号処理プロセスが３個の復号サブプロセスから構成されている場合、「３」と記載されている。

[0357] 複数の検証値組２４３ｃ～２４７ｃの数は、アプリの数と同一であり、複数の検証値組２４３ｃ～２４７ｃは、それぞれ、アプリ１１０、１１１、１

１２、１１３及び１１４に対応している。各検証値組は、アプリ識別情報、データ及び検証値を含む。

[0358] 検証値組に含まれるアプリ識別情報は、対応するアプリを識別する識別子である。

[0359] 検証値組に含まれるデータは、対応する暗号化アプリのデータから生成された中間値２（３５７）である。

[0360] 検証値組に含まれる検証値は、中間値２（３５７）とアプリのデータ（３５８）とから生成した復号検証値である。ここで、アプリのデータ（３５８）は、復号部分処理３（３５３）の出力データである。復号したアプリのデータ（３５８）は、ソフトウェア実行部６２１が、アプリの復号処理を実行することにより取得される。検証値は、保護制御モジュール１２０が正常動作した際のそれぞれの復号部分処理３（３５３）の入力データと出力データとを結合して得られた結合体に対して、ハッシュ関数による演算を施して得られたハッシュ値である。

[0361] 検証値＝Ｈａｓｈ（復号部分処理３（３５３）の入力データ｜｜復号部分処理３（３５３）の出力データ）

ここでは、検証値としてハッシュ値を使用したが、これに限定するものではなく、次に示すように、署名などを用いてもよい。

[0362] 検証値＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（復号部分処理３（３５３）の入力データ｜｜復号部分処理３（３５３）の出力データ））

証明書２４８ｃは、復号処理証明書である。復号処理証明書は、復号部分処理３に関するデータ２４１ｃに含まれる全ての検証値を結合し、これらの複数の検証値を結合して得られた結合体にハッシュ関数による演算を施してハッシュ値を計算し、計算したハッシュ値に対して、署名秘密鍵保持部６０６の署名秘密鍵を用いて、デジタル署名アルゴリズムを施して、生成した署名である。

[0363] 証明書２４８ｃ＝Ｓｉｇｎ（署名秘密鍵、Ｈａｓｈ（検証値｜｜検証値｜｜、・・・、検証値｜｜検証値））

復号部分識別子２４９ｃは、復号部分処理３（３５３）を識別する識別子である。一例として、復号部分識別子２４９ｃは、「００３」である。

[0364] ５．３　動作

（１）検証基データの生成処理の動作

検知システム１０ｃにおける検証基データの生成処理を図３４に示すフローチャートを用いて説明する。

[0365] 検証基データの生成では、ソフトウェア実行部６２１は、機器１００にインストールされる複数のアプリであって、アプリ保持部６０９に保持している複数のアプリを保護制御モジュール１２０の暗復号鍵で暗号化する（ステップＳ１２０１）。ソフトウェア実行部６２１は、保護制御モジュール１２０の復号処理を実行し、複数の暗号化アプリを復号して、復号部分処理１（３５１）、復号部分処理２（３５２）及び復号部分処理３（３５３）の出力データである中間値１（３５６）、中間値２（３５７）及び復号したアプリのデータ（３５８）を取得する（Ｓ１２０２）。

[0366] 次に、証明書生成部６０５は、アプリ毎に、暗号化アプリのデータ（３５５）及び中間値１（３５６）の組、中間値１（３５６）及び中間値２（３５７）の組、並びに、中間値２（３５７）及び復号したアプリのデータ（３５８）の組のそれぞれに対し、検証値を生成し、各復号部分処理に関して、複数の検証値から、署名秘密鍵保持部６０６に保持されている署名秘密鍵を用いて、証明書を生成する（ステップＳ１２０３）。

[0367] 最後に、検証基データ生成部６１０は、復号部分処理１に関するデータ（２４１ａ）、復号部分処理２に関するデータ（２４１ｂ）、及び復号部分処理３に関するデータ（２４１ｃ）を含む検証基データ２４０を生成する（ステップＳ１２０４）。

[0368] （２）検知処理の動作

図３５及び図３６は、検知システム１０ｃにおける検知処理の動作を示すシーケンス図である。

[0369] ここでは、具体例として、機器１００がアプリ１１０を実行する場合にお

いて、保護制御モジュール１２０が検知処理を行うときについて説明する。

[0370] 保護制御モジュール１２０の検証基データ生成部３０９は、アプリ１１０を実行するコマンドを受信すると（ステップＳ２３００）、検証基データ保持部３０８に保持されている検証基データ２４０（図３３）から、復号部分処理１に関するデータ２４１ａ、復号部分処理２に関するデータ２４１ｂ及び復号部分処理３に関するデータ２４１ｃを分離して抽出し、復号部分処理１に関するデータ２４１ａを復号部分処理１の検証基データ２５０ａ（図３７に示す）とし、復号部分処理２に関するデータ２４１ｂを復号部分処理２の検証基データ２５０ｂ（図３８に示す）とし、復号部分処理３に関するデータ２４１ｃを復号部分処理３の検証基データ２５０ｃ（図３９に示す）として生成する（ステップＳ２３０１）。

[0371] 図３７に示す復号部分処理１の検証基データ２５０ａは、図３３の検証基データ２４０の復号部分処理１に関するデータ２４１ａと同じであり、図３８に示す復号部分処理２の検証基データ２５０ｂは、図３３の検証基データ２４０の復号部分処理２に関するデータ２４１ｂと同じであり、図３９に示す復号部分処理３の検証基データ２５０ｃは、図３３の検証基データ２４０の復号部分処理３に関するデータ２４１ｃと同じである。

[0372] 検証基データ２５０ａ、２５０ｂ及び２５０ｃの生成後、保護制御モジュール１２０は、暗号化されたアプリ１１０を復号する（ステップＳ２３０２）。

[0373] 保護制御モジュール１２０は、検知モジュール選択部３１１が保持する対応表３３０を用いて、検知モジュール１３１、１３２、１３３、１３４、１３５のうち、どの検知モジュールに検証基データを送信するかを決定する（ステップＳ２３０３）。ここでは、検知モジュール１３１、１３２、１３３を選択したとする。

[0374] 保護制御モジュール１２０は、選択した検知モジュール１３１へ、アプリ１１０を識別するアプリ識別情報と中間値１（３５６）と復号部分処理１の検証基データ２５０ａとを送信する（ステップＳ２３０４）。

[0375] また、保護制御モジュール１２０は、選択した検知モジュール１３２へ、アプリ１１０を識別するアプリ識別情報と中間値２（３５７）と復号部分処理２の検証基データ２５０ｂとを送信する（ステップＳ２３０５）。

[0376] さらに、保護制御モジュール１２０は、選択した検知モジュール１３３へ、アプリ１１０を識別するアプリ識別情報と復号したアプリのデータ（３５８）と復号部分処理３の検証基データ２５０ｃとを送信する（ステップＳ２３０６）。

[0377] 各検知モジュールは、受信した検証基データを用いて、復号部分処理の入出力対応が正しいか否かを検証する（ステップＳ２３０７）。具体的に、各検知モジュールは、受信した検証基データ内のデータと、受信した中間値またはアプリのデータから検証値を生成する。そして、生成した検証値と検証データ内の検証値と比較し、両者が一致するか判断する。さらに、復号処理証明書の署名検証を行う。

[0378] 各検知モジュールは、検証値が一致しない、または、署名検証に失敗した場合には、中間値又はアプリのデータが正しくないと判定し（ステップＳ２３０８でＹ）、判断部２１０へ中間値又はアプリのデータが正しくないことを示す監視結果を送信する（ステップＳ２３０９）。各検知モジュールは、検証値が一致し、かつ、署名検証に成功した場合には、保護制御モジュール１２０が改ざんされていないと判定し（ステップＳ２３０８でＮ）、各復号部分処理を検証した旨の通知及び検証基データ内の復号部分識別子を他の全ての検知モジュールへ送信する（ステップＳ２３１０）。一例として、検知モジュール１３１は、復号部分処理１を検証した旨の通知及び復号部分処理１（３５１）を識別する復号部分識別子「００１」を送信する。そして、各検知モジュールは、保護制御モジュール１２０のすべての復号部分処理が検証されたか否かを確認する（ステップＳ２３１１）。具体的には、各検知モジュールは、自身に割り当てられた復号部分処理を除く他の全ての復号部分処理を識別する復号部分識別子を受け取ったか否かを判断する。各検知モジュールは、自身に割り当てられた復号部分処理を除く他の全ての復号部分処

理を識別する復号部分識別子を受け取ったと判断する場合には、保護制御モジュール１２０が改ざんされていないと判定し（ステップＳ２３１１でＮ）、処理を終了する。

[0379] 各検知モジュールは、自身に割り当てられた復号部分処理を除く他の全ての復号部分処理を識別する復号部分識別子を受け取っていないと判断する場合には、すべての復号部分処理が検証されていない、又は、全ての復号部分処理についての出力データ（中間値１（３５６）、中間値２（３５７）及びアプリのデータ（３５７））並びに検証基データ２５０ａ、２５０ｂ及び２５０ｃが、１個の検知モジュールに送信されている可能性があり、保護制御モジュール１２０が不正動作を行ったものとして、保護制御モジュール１２０が改ざんされていると判定し（ステップＳ２３１１でＹ）、判断部２１０へ保護制御モジュール１２０が改ざんされていることを示す判断結果を送信する（ステップＳ２３１２）。

[0380] ５．４　検知システム１０ｃの効果

検知システム１０ｃでは、保護制御モジュール１２０が実行する復号処理のプロセスは、複数のサブプロセスである復号部分処理から構成され、復号部分処理ごとに入出力データの対応関係が検証される。そのため、仮に検知モジュールが不正動作をしたとしても、保護制御モジュール１２０が実行する復号処理の全体が漏洩するのを防止することができる。さらに、保護制御モジュール１２０による復号処理の全体のうち、どの部分が改ざんされたかを知ることができる。

[0381] また、保護制御モジュール１２０が選択をしなかった検知モジュールが不正動作をしたとしても保護制御モジュール１２０に対する検知処理には影響せず、保護制御モジュールが改ざんされているかを検証することができる。

[0382] ６．その他の変形例

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。

[0383] （１）上記各実施の形態では、検知処理後に相互監視処理を行うとしてもよい。相互監視処理に関しては、特許文献３に詳しく説明されているので、ここでの説明は省略する。

[0384] （２）上記変形例（１）では、検知処理後に、相互監視を実行し、保護制御モジュール１２０が正常であると判断できた場合は、相互監視の結果、発見した不正動作を行う検知モジュールを、保護制御モジュール１２０が無効化するとしてもよい。また、正常な検知モジュールを用いて、無効化処理を行うとしてもよい。無効化処理に関しては、特許文献３に詳しく説明されているので、ここでの説明は省略する。

[0385] （３）上記実施の形態４では、ｎ個の全ての検知モジュールが連携して、全ての検知モジュールが送信した乱数を合計して合計値を算出し、算出した合計値を用いて、選択すべき検知モジュールの組を決定するための選択情報を計算しているが、これには限定されない。

[0386] 一部の検知モジュールが連携し、これらの検知モジュールにより生成した乱数から選択情報を計算してもよい。

[0387] 具体的には、ｎ個の検知モジュールのうちの一部の検知モジュール（ここでは、ｍ個の検知モジュールとする。ｍは、ｎより小さい整数である。）がそれぞれ、乱数ｒ１、ｒ２、・・・、ｒｍを生成する。生成されたｍ個の乱数ｒ１、ｒ２、・・・、ｒｍを合計して合計値を算出し、算出した合計値について、Ｉｎｄｅｘの最大値による法を取り、得られた値を選択情報として計算する。

[0388] 選択情報＝ （ｒ１ ＋ｒ２ ＋・・・＋ｒｍ） ｍｏｄ Ｉｎｄｅｘの最大値

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0389] （４）上記実施の形態４では、全ての検知モジュールが連携して、全ての検知モジュールが送信した乱数から選択情報を計算しているが、これには限定されない。

[0390] 全ての検知モジュール及び保護制御モジュール１２０が連携し、それぞれが送信した乱数から選択情報を計算するとしてもよい。

[0391] 具体的には、ｎ個の全ての検知モジュールがそれぞれ乱数ｒ１、ｒ２、・・・、ｒｎを生成し、保護制御モジュールが乱数Ｒを生成し、生成された（ｎ＋１）個の乱数Ｒ、ｒ１、ｒ２、・・・、ｒｎを合計して合計値を算出し、算出した合計値を用いて、選択すべき検知モジュールの組を決定するための選択情報を計算してもよい。

[0392] 選択情報＝　（Ｒ＋ｒ１＋ｒ２＋・・・＋ｒｎ）　ｍｏｄ　（Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0393] また、ｎ個の検知モジュールのうちのｍ個の検知モジュールがそれぞれ乱数ｒ１、ｒ２、・・・、ｒｍを生成し、保護制御モジュールが乱数Ｒを生成し、生成された（ｍ＋１）個の乱数Ｒ、ｒ１、ｒ２、・・・、ｒｍを合計して合計値を算出し、算出した合計値を用いて、選択すべき検知モジュールの組を決定するための選択情報を計算してもよい。

[0394] 選択情報＝　（Ｒ＋ｒ１＋ｒ２＋・・・＋ｒｍ）　ｍｏｄ　（Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0395] （５）上記実施の形態４では、全ての検知モジュールが連携して、全ての検知モジュールが送信した乱数から選択情報を計算しているが、これには限定されない。

[0396] 保護制御モジュール１２０と各検知モジュールが共有する秘密のアルゴリズムを用いて、選択情報を決定するとしてもよい。

[0397] 例えば、保護制御モジュール１２０は、１個の乱数Ｒを生成し、生成した乱数Ｒに、保護制御モジュール１２０が秘密に保持している鍵Ｋを用いて、鍵付きハッシュ関数ＫｅｙｅｄＨａｓｈによる演算を施して、ハッシュ値Ｈ

を算出する。

[0398] Ｈ＝ＫｅｙｅｄＨａｓｈ（Ｋ、Ｒ）

ここで、ＫｅｙｅｄＨａｓｈ（Ａ、Ｂ）は、鍵Ａを用いて、値Ｂに鍵付きハッシュ関数による演算を施して、得られたハッシュ値を示す。

[0399] また、ｎ個の全ての検知モジュールも同様にして、それぞれ、１個の乱数ｒｉを生成し、生成した乱数に、検知モジュールが秘密に保持している鍵ｋｉを用いて、鍵付きハッシュ関数ＫｅｙｅｄＨａｓｈによる演算を施して、ハッシュ値ｈｉを算出する。

[0400] ｈｉ＝ＫｅｙｅｄＨａｓｈ（ｋｉ、ｒｉ）　（ｉ＝１、２、・・・、ｎ）

こうして、（ｎ＋１）個のハッシュ値Ｈ、ｈ１、ｈ２、・・・、ｈｎが算出される。

[0401] 次に、算出された（ｎ＋１）個の乱数を合計して合計値を算出し、算出した合計値について、Ｉｎｄｅｘの最大値による法を取り、得られた値を選択情報として計算する。

[0402] 選択情報＝（Ｈ＋ｈ１＋ｈ２＋・・・＋ｈｎ）ｍｏｄ（Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0403] なお、ｎ個の全ての検知モジュールではなく、ｎ個の検知モジュールのうちのｍ個の検知モジュールを用いて、選択情報を計算してもよい。

[0404] 選択情報＝（Ｈ＋ｈ１＋ｈ２＋・・・＋ｈｍ）ｍｏｄ（Ｉｎｄｅｘの最大値）

（６）上記実施の形態４では、すべての検知モジュールが連携して、すべての検知モジュールが送信した乱数から選択情報を計算しているが、これには、限定されない。

[0405] 機器１００のＩＤを用いて、選択情報を生成するとしてもよい。機器１００のＩＤとは、例えば、機器１００の製造番号である。

[0406] 例えば、次のようにして選択情報を計算してもよい。

[0407] 選択情報 ＝ （機器１００の製造番号） ｍｏｄ （Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0408] これにより、攻撃者が一台の攻撃の対象機器を解析することで、解析した対象機器がどのＩｎｄｅｘを選択しているかを知ったとしても、他の機器は、その対象機器が有するＩＤとは、別のＩＤを有しているので、他の機器により用いられる選択情報は、対象機器により用いられる選択情報と異なり、対象機器の解析で知った選択情報を、他の機器において用いることはできない。こうして、他の機器への攻撃を防止することができる。

[0409] （７）上記実施の形態４では、すべての検知モジュールが連携して、すべての検知モジュールが送信した乱数から選択情報を計算しているが、これには限定されない。

[0410] 機器１００の時刻情報を用いて、選択情報を計算するとしてもよい。ここで、機器１００の時刻情報は、一例として、年月日時分秒から構成される。

[0411] 例えば、次のようにして選択情報を計算してもよい。

[0412] 選択情報 ＝ （年月日時分秒） ｍｏｄ （Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0413] また、次のようにして選択情報を計算してもよい。

[0414] 選択情報 ＝ Ｈａｓｈ（年月日時分秒） ｍｏｄ （Ｉｎｄｅｘの最大値）

ここで、選択情報が「０」となる場合には、Ｉｎｄｅｘの最大値を選択情報とする。

[0415] （８）上記実施の形態４では、全ての検知モジュールが連携して、全ての検知モジュールが送信した乱数から選択情報を計算しているが、これには、限定されない。

[0416] 管理装置２００がＩｎｄｅｘを指定するとしてもよい。保護制御モジュール１２０はステップＳ２２０３で検知の実行を検知モジュールに通知しているが、検知モジュールへの通知に代えて、検知の実行を管理装置２００へ通知する。管理装置２００の判断部２１０は、保護制御モジュール１２０から検知実行の通知を受信すると、指示生成部５０３は、モジュール選択部５０４へモジュールを選択するように指示する。モジュール選択部５０４は、対応表からＩｎｄｅｘを選択し、選択したＩｎｄｅｘを指示生成部５０３へ送信する。指示生成部５０３は、モジュール選択部５０４から受信したＩｎｄｅｘを、送信部５０２を介して、保護制御モジュール１２０へ送信する。

[0417] 保護制御モジュール１２０は、Ｉｎｄｅｘを受け取り、受け取ったＩｎｄｅｘに対応する検知モジュール識別子の組を選択する。

[0418] （９）上記実施の形態４では、ステップＳ２２０８において、保護制御モジュール１２０は各検知モジュールからＩｎｄｅｘを受信し、Ｉｎｄｅｘに基づき検知モジュールを選択する。このとき、保護制御モジュール１２０が複数の検知モジュールから受信した全てのＩｎｄｅｘが完全に一致しない場合、言い換えると、一つでも異なるＩｎｄｅｘが存在する場合、いずれかの検知モジュールが不正動作を行っていると判断し、保護制御モジュール１２０が判断部２１０へ通知するとしてもよい。

[0419] （１０）上記実施の形態４では、ステップＳ２２０９からＳ２２１１において、保護制御モジュール１２０は、選択情報に基づいて選択した検知モジュールへ検証基データを送信する。

[0420] このとき、保護制御モジュール１２０が、選択情報に基づいて選択した検知モジュールへ検証基データを送信しなかった場合に、検知モジュールは、保護制御モジュール１２０が改ざんされていると判断し、判断部２１０に通知するとしてもよい。ここで、検知モジュールは、選択情報を知っているので、検知モジュールが対応表３３０を保持しているようにしておけば、検知モジュールは、選択情報に基づいて選択された検知モジュールを知ることができる。従って、当該検知モジュールが選択されている場合に、当該検知モ

ジュールが、検証基データを受信しなかったとき、保護制御モジュール１２０が、選択情報に基づいて選択した検知モジュールへ検証基データを送信しなかったことを知ることができる。

[0421] また、選択情報に基づいて選択した検知モジュールとは異なる検知モジュールに送信した場合に、保護制御モジュール１２０が改ざんされていると判断してもよい。ここで、検知モジュールは、選択情報を知っているので、検知モジュールが対応表３３０を保持しているようにしておけば、検知モジュールは、選択情報に基づいて選択された検知モジュールを知ることができる。従って、当該検知モジュールが選択されていない場合に、当該検知モジュールが、検証基データを受信したとき、保護制御モジュール１２０が、選択情報に基づいて選択した検知モジュールへ検証基データを送信しなかったことを知ることができる。

[0422] また、検知モジュールは、ステップＳ２２０７で選択情報を送信後、一定時間内に保護制御モジュール１２０からアプリ識別情報、分割データ及び検証基データを受信しなかった場合に、保護制御モジュール１２０が改ざんされていると判断してもよい。

[0423] （１１）上記各実施の形態と、上記変形例（１）を組み合わせて実施するとしてもよい。上記変形例（１）では、相互監視処理を実行するため、検知処理後に各検知モジュールが

不正動作を行っているか否かの判定ができる。一方、上記実施の形態では、相互監視処理を実行しないため、機器１００の処理を軽くすることができる。相互監視処理を実行するかの切り替えは、定期的に切り替えてもよいし、アプリによって異なるとしてもよいし、管理装置２００から切り替えの指示をするとしてもよいし、機器１００内部の処理の状況を鑑みて切り替えるとしてもよい。また、相互監視処理を実行する場合には、ステップＳ２００３ですべての検知モジュールを選択するとしてもよい。

[0424] （１２）上記の各モジュールは、具体的には、それぞれ個別のコンピュータプログラムであってもよいし、オペレーティングシステムに組み込まれる

モジュールであってもよいし、オペレーティングシステムから呼ばれるドライバプログラムであってもよいし、アプリケーションプログラムであってもよい。

[0425] （１３）上記の実施の形態２～５においては、情報処理装置である機器１００内において、複数の検知モジュール及び保護制御モジュールが動作するとしているが、これには限定されない。

[0426] 機器１００内において、保護対象のコンピュータプログラムと、前記コンピュータプログラムを保護する保護制御モジュールとが動作し、機器１００とは別の１台の検知装置において、複数の検知モジュールが動作し、これらの複数の検知モジュールが機器１００内の保護制御モジュールを監視するとしてもよい。ここで、機器１００と前記検知装置とは、ネットワークを介して接続されている。

[0427] ここで、検知装置は、１台に限定されない。複数台の検知装置が機器１００とネットワークを介して接続されているとしてもよい。検知装置の台数は、検知モジュールの数に等しい。各検知装置において、１個の検知モジュールが動作する。１台の検知装置の検知モジュールが機器１００内の保護制御モジュールを監視する。この結果、複数台の検知装置において動作する複数の検知モジュールが機器１００内の保護制御モジュールを監視することとなる。

[0428] （１４）上記の実施の形態２～５においては、情報処理装置である機器１００内において、アプリから複数の分割データを生成し、閾値秘密分散法によりアプリから複数の分散データを生成し、又は、暗号化アプリを復号する復号プロセスは、複数の復号サブプロセスから構成され、各復号サブプロセスにおける入力データ及び出力データを用いるとしている。しかし、これには限定されない。

[0429] 保護制御モジュールは、コンピュータプログラムであるので、保護制御モジュールから複数の分割データを生成してもよい。また、閾値秘密分散法により保護制御モジュールから複数の分散データを生成してもよい。また、保

護制御モジュールを暗号化し、暗号化保護制御モジュールを復号する復号プロセスは、複数の復号サブプロセスから構成され、各復号サブプロセスにおける入力データ及び出力データを用いるとしてもよい。

[0430] これらの場合に、検知モジュールは、保護制御モジュールから生成された複数の分割データを用いて、保護制御モジュールの改ざんを検出する。また、検知モジュールは、保護制御モジュールから生成された複数の分散データを用いて、保護制御モジュールの改ざんを検出する。また、暗号化された保護制御モジュールを復号する復号プロセスにおいて、各復号サブプロセスにおける入力データ及び出力データを用いて、保護制御モジュールの改ざんを検出する。

[0431] （１５）実施の形態２と実施の形態３とを組合せてもよい。この場合において、検証可能秘密分散法ではなく、しきい値ｋ、分配数ｄの（ｋ，ｄ）秘密分散法を用いて、分割データを生成する。検証基データの検証値は分割データのハッシュ値を用いる。

[0432] （１６）情報処理装置としての機器１００は、具体的には、パーソナルコンピュータ、ＢＤ再生装置、ＤＶＤ再生装置、ＢＤ記録装置、ＤＶＤ記録装置、デジタル放送受信再生装置、デジタル放送記録装置、携帯電話機などである。

[0433] （１７）次のようにしてもよい。

[0434] 本発明の一態様の情報処理装置は、アプリケーションを保護する機能を有する保護制御モジュールと、ｎ個の検知モジュールとを含む情報処理装置であって、前記保護制御モジュールは、暗号化された前記アプリケーションが入力データとして入力され、前記入力データを復号し、復号結果を出力データとして出力する復号手段と、前記出力データを少なくともｄ（ｄ≧２）個の分割データを分割する分割手段と、ｎ個の前記検知モジュールのうちｄ個の検知モジュールを選択する選択手段と、分割されたｄ個の分割データを、前記選択手段で選択した前記ｄ個の検知モジュールに分配する分配手段と、前記d個の検知モジュールのそれぞれは、分割された分割データ、前記入力デ

ータと前記復号手段が正常動作を行った場合に期待される分割データの値とに基づいて生成された検証データ、及び、入力データを用いて、分配された分割データが正しいか否かを判断する検証手段を備えることを特徴とする。

[0435] 本発明によれば、各検知モジュールは、保護制御モジュール自体のデータを用いた検証を行わず、保護制御モジュールが実行するアプリケーションの復号処理を検証するので、各検知モジュールに対して、保護制御モジュールが有する秘匿データが漏洩するのを防止することができる。

[0436] また、本発明によれば、検知を実行しないｎ－ｄ個の検知モジュールが攻撃されたとしても保護制御モジュールに対する検知処理に影響せず、保護制御モジュールが改ざんされているかを検証することができる。

[0437] ここで、前記分割手段は、前記ｄ個の分割データのうち、ｋ個の分割データを用いるとはじめて前記出力データを復元できるように、前記ｄ個の分割データを生成してもよい。

[0438] この構成によると、前記ｄ個の検知モジュールのうちのｋ個の検知モジュールが保持する分割データから出力データが復元できるため、前記出力データが入力データから正しく復号されたことを確認することができる。

[0439] ここで、前記選択手段は、所定の情報に基づいて、所定の情報と検知モジュールの識別情報との対応表から検知モジュールを選択してもよい。

[0440] この構成によると、保護制御モジュールは対応表を用いて検知モジュールを選択することができる。

[0441] ここで、前記所定の情報は、前記分配手段で分配するごとに毎回変更されるとしてもよい。

[0442] この構成によると、所定の情報は分配するごとに毎回変更することができる。これにより、保護制御モジュールが選択する検知モジュールを毎回変更することで、恣意的に分割データの送信先を決定できない。

[0443] ここで、前記所定の情報は、前記複数の検知モジュールが保持する部分情報を用いて生成されるとしてもよい。

[0444] この構成によると、保護制御モジュールが選択する検知モジュールを検知

モジュールが決定することで、保護制御モジュールが恣意的に決定できない。

[0445] ここで、前記検知モジュールのそれぞれは、乱数を生成し、他の検知モジュールへ送信する送信手段を備え、前記保持する部分情報は、前記検知モジュールが生成した乱数であるとしてもよい。

[0446] この構成によると、保護制御モジュールが選択する検知モジュールを検知モジュールが乱数を用いて決定することで、保護制御モジュールが恣意的に決定できない。

[0447] ここで、前記情報処理装置は、管理装置と接続し、前記所定の情報は前記管理装置から受信するとしてもよい。

[0448] この構成によると、保護制御モジュールが選択する検知モジュールを管理装置が決定することで、保護制御モジュールが恣意的に決定できない。

[0449] また、本発明の別の態様の情報処理装置は、アプリケーションを保護する機能を有する保護制御モジュールと、ｎ個の検知モジュールとを含む情報処理装置であって、前記保護制御モジュールは、暗号化された前記アプリケーションプログラムに対し、ｄ個の処理工程から成る復号処理を実行する復号手段と、ｎ個の前記検知モジュールのうちｄ個の検知モジュールを選択する選択手段と、前記ｄ個の処理工程それぞれの出力データであるｄ個の被検証データを、前記ｄ個の検知モジュールへ分配する分配手段とを備え、前記複数の検知モジュールのそれぞれは、分配された被検証データ、前記被検証データに対応する処理工程への入力データ、及び、前記入力データと前記復号手段が正常動作を行った場合に期待される出力データとに基づいて生成された検証データを用いて、前記被検証データが正しいか否かを判断する検証手段を備えることを特徴とする。

[0450] この構成によると、各検知モジュールは、保護制御モジュール自体のデータを用いた検証を行わず、保護制御モジュールが実行するアプリケーションの復号処理を検証するので、各検知モジュールに対して、保護制御モジュールが有する秘匿データが漏洩するのを防止することができる。

[0451] また、本発明によれば、複数の検知モジュールが、それぞれ異なる処理工程についての検証を行うので、各検知モジュールに対して、アプリケーションのデータが漏洩するのを防止することができる。

[0452] また、本発明によれば、復号処理のうち、どの処理工程が改ざんされているかを検知することもできる。

[0453] （１８）次のように構成してもよい。

[0454] （ａ）本発明の別の態様は、コンピュータプログラムを保護する保護制御回路と、前記保護制御回路を監視するためのｎ個の検知回路と、管理装置とを含む改ざん監視システムである。

[0455] 前記保護制御回路は、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成回路と、ｎ個の前記検知回路のうち、ｄ個の検知回路を選択する選択回路と、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知回路へ分配する分配回路とを備える。

[0456] ｄ個の前記検知回路のそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御回路の改ざんを検出し、前記保護制御回路が改ざんされているか否かを示す判断結果を送信する。

[0457] 前記管理装置は、前記検知回路のそれぞれから前記判断結果を受信し、受信した判断結果を基にして、前記保護制御回路の改ざんを管理する。

[0458] 前記検知回路は、前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成し、前記保護制御回路を監視するためのｎ個の検知回路のうち、ｄ個の検知回路を選択し、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知回路へ分配する保護制御回路から１個の前記分配データを受信する受信回路と、受信した前記分配データが正しいか否かを判断する検証回路と、正しいと判断した場合に、他の検知回路へ前記分配データが正しいことを示す監視結果を送信する送信回路とを備える。前記受信回路は、他の検知回路から受信した分配データが正しいことを示す監視結果を受け取り、前記検証回路は、自身の監視結果及び受信した監視結果を用いて、前記保護制御回路が改ざんされているか否かを判断し、前記送信

回路は、前記保護制御回路が改ざんされているか否かを示す判断結果を送信する。

[0459] （ｂ）本発明の別の態様は、保護対象コンピュータプログラムを保護する保護制御モジュールと、前記保護制御モジュールを監視するためのｎ個の検知モジュールと、管理装置とを含む改ざん監視システムである。

[0460] 前記保護制御モジュールは、複数のコンピュータ命令が組み合わされて構成される制御用コンピュータプログラムを記憶しているメモリ部と、前記メモリ部に記憶されている前記制御用コンピュータプログラムから１個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備える。前記制御用コンピュータプログラムは、コンピュータに、前記保護対象コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成ステップと、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールを選択する選択ステップと、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配ステップとを実行させる。

[0461] ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出し、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する。

[0462] 前記管理装置は、前記検知モジュールのそれぞれから前記判断結果を受信し、受信した判断結果を基にして、前記保護制御モジュールの改ざんを管理する

前記検知モジュールは、複数のコンピュータ命令が組み合わされて構成される制御用コンピュータプログラムを記憶しているメモリ部と、前記メモリ部に記憶されている前記制御用コンピュータプログラムから１個ずつコンピュータ命令を読み出し、解読し、その解読結果に応じて動作するプロセッサとを備える。前記制御用コンピュータプログラムは、コンピュータに、前記保護制御モジュールから１個の前記分配データを受信する受信ステップと、受信した前記分配データが正しいか否かを判断する検証ステップと、正しい

と判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する送信ステップとを実行させる。前記受信ステップは、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取り、前記検証ステップは、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断し、前記送信ステップは、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する。

[0463] （１９）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。

[0464] （２０）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。

[0465] 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よいし、一部又は全てを含むように１チップ化されてもよい。

[0466] 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・プロセッサを利用してもよい。

[0467] 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。

[0468] （２１）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。

[0469] （２２）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。

[0470] 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。

[0471] 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。

[0472] 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。

[0473] 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。

[0474] （２３）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

[0475] 本発明にかかる改ざん監視システム、保護制御モジュール及び検知モジュールは、全ての検知モジュールに検知処理を実行させるのではなく、保護制御モジュールにより選択された検知モジュールに、検知処理を実行させる。このため、保護制御モジュールにより選択されなかった検知モジュールが改ざんされ、不正に動作をしたとしても、選択された検知モジュールが改ざんされていなければ、改ざん監視システムの全体として、保護制御モジュールに対する改ざん検知処理には影響しない。こうして、保護制御モジュールが改ざんされているかを検証することができるという効果を有し、機器内部で動作するモジュール等を監視する技術として有用である。

符号の説明

[0476] １０、１０ａ、１０ｂ、１０ｃ　検知システム

１０ｄ　監視システム

１００　機器

１１０、１１１、１１２、１１３、１１４　アプリ

１２０、１２０ｄ　保護制御モジュール

１３０　検知モジュール群

１３１、１３２、１３３、１３４、１３５　検知モジュール

１３０ｄ１、１３０ｄ２、・・・、１３０ｄｎ　検知モジュール

１７１　ＣＰＵ

１７２　ＥＥＰＲＯＭ

１７３　ＲＡＭ

１７４　ＮＩＣ

１８０　ＯＳ

１９０　ブートローダ

２００、２００ｄ　管理装置

２１０　判断部

２２０、２２０ａ　検証基データ配布部

２３０　通信部

３０１　受信部

３０２　送信部

３０２ｄ　分配部

３０３　制御部

３０４　復号ロード部

３０５　改ざん検出部

３０６　解析ツール検出部

３０７　暗復号鍵保持部

３０８　検証基データ保持部

３０９　検証基データ生成部

３１０　アプリ分割部

３１０ｄ　生成部

３１１、３１１ａ　検知モジュール選択部

３１１ｄ　生成部

４０１　受信部

４０２　送信部

４０３　制御部

４０４　検証部

４０５　検証基データ保持部

５０１　受信部

５０２　送信部

５０３　指示生成部

５０４　モジュール選択部

６０１　受信部

６０２　送信部

６０３　制御部

６０４　認証部

６０５　証明書生成部

６０６　署名秘密鍵保持部

６０７　暗号鍵保持部

６０８　データ分割部

６０９　アプリ保持部

６１０　検証基データ生成部

６１１　保護制御モジュール保持部

６１２　検知モジュール保持部

６２１　ソフトウェア実行部

請求の範囲

[請求項1] コンピュータプログラムを保護する保護制御モジュールと、前記保護制御モジュールを監視するためのｎ個の検知モジュールと、管理装置とを含む改ざん監視システムであって、

前記保護制御モジュールは、

前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成手段と、

ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールを選択する選択手段と、

生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配手段とを備え、

ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出し、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信し、

前記管理装置は、前記検知モジュールのそれぞれから前記判断結果を受信し、受信した判断結果を基にして、前記保護制御モジュールの改ざんを管理する

ことを特徴とする改ざん監視システム。

[請求項2] 前記改ざん監視システムは、１台の情報処理装置を含み、

前記情報処理装置が前記保護制御モジュールとｎ個の前記検知モジュールとを含み、前記コンピュータプログラムを記憶しており、

前記情報処理装置と前記管理装置とは、ネットワークを介して接続されている

ことを特徴とする請求項１に記載の監視システム。

[請求項3] 前記改ざん監視システムは、１台の情報処理装置及びｎ台の検知装置を含み、

前記情報処理装置が前記保護制御モジュールを含み、前記コンピュ

ータプログラムを記憶しており、

ｎ台の前記検知装置が、それぞれ、１個の前記検知モジュールを含み、

前記情報処理装置とｎ台の前記検知装置と前記管理装置とは、ネットワークを介して接続されている

ことを特徴とする請求項１に記載の監視システム。

［請求項4］ コンピュータプログラムを保護する保護制御モジュールであって、

前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成手段と、

当該保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択する選択手段と、

生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配手段とを備え、

ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出する

ことを特徴とする保護制御モジュール。

［請求項5］ 前記生成手段は、

前記コンピュータプログラムを暗号化して生成した暗号化コンピュータプログラムを記憶している記憶手段と、

前記暗号化コンピュータプログラムを復号してコンピュータプログラムを生成する復号手段と、

生成された前記コンピュータプログラムを基にして、ｄ個の前記分配データを生成する分配データ生成手段と

を含むことを特徴とする請求項４に記載の保護制御モジュール。

［請求項6］ 前記分配データ生成手段は、前記コンピュータプログラムを構成するデータを分割してｄ個の前記分配データを生成する

ことを特徴とする請求項５に記載の保護制御モジュール。

[請求項7] 前記分配データ生成手段は、前記コンピュータプログラムを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成し、

前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを復元することができるように、前記コンピュータプログラムを分散する秘密分散法である

ことを特徴とする請求項５に記載の保護制御モジュール。

[請求項8] 前記生成手段は、

前記コンピュータプログラムを暗号化して生成した暗号化コンピュータプログラムを記憶している記憶手段と、

前記暗号化コンピュータプログラムに、復号処理を施す過程において、ｄ個の前記分配データを生成する復号手段とを含み、

前記復号処理は、ｄ個の復号サブ処理から構成され、ｄ個の復号サブ処理を順次施すことにより、前記暗号化コンピュータプログラムの復号を行い、

各復号サブ処理から出力される復号出力を前記分配データとする

とを特徴とする請求項４に記載の保護制御モジュール。

[請求項9] 前記選択手段は、ｎ個の前記検知モジュールのうち、ｄ個の検知モジュールの組合せと、当該組合せを識別する識別情報とを対応付けて含む対応表を保持し、前記組合せの選択に用いる選択情報を取得し、取得した選択情報に一致する識別情報に対応する組合せを前記対応表から取得し、取得し組合せに含まれる検知モジュールを選択する

ことを特徴とする請求項４に記載の保護制御モジュール。

[請求項10] 前記選択手段は、乱数を生成し、生成した乱数を前記選択情報とすることにより、前記選択情報を取得する

ことを特徴とする請求項９に記載の保護制御モジュール。

[請求項11] 前記選択手段は、前記分配手段によりｄ個の前記分配データを分配

するごとに、前記選択情報を新たに生成する

ことを特徴とする請求項９に記載の保護制御モジュール。

[請求項12] 各検知モジュールは、乱数を生成し、他の全ての検知モジュールへ送信し、

各検知モジュールは、受信した乱数及び自身が生成した乱数を用いて、選択情報を生成し、生成した前記選択情報を前記保護制御モジュールへ送信し、

前記選択手段は、前記検知モジュールから前記選択情報を受信し、受信した前記選択情報を用いる

ことを特徴とする請求項９に記載の保護制御モジュール。

[請求項13] 保護制御モジュールの改ざんを管理する管理装置は、前記選択情報を生成し、生成した前記選択情報を前記保護制御モジュールへ送信し、

前記選択手段は、前記管理装置から前記選択情報を受信し、受信した前記選択情報を用いる

ことを特徴とする請求項９に記載の保護制御モジュール。

[請求項14] 前記コンピュータプログラムは、前記保護制御モジュールの保護の対象であるアプリケーションプログラム、又は、前記保護制御モジュールの動作手順を示すプログラムである

ことを特徴とする請求項４に記載の保護制御モジュール。

[請求項15] 前記保護制御モジュールは、情報処理装置に含まれ、

前記情報処理装置は、前記コンピュータプログラムを記憶している

ことを特徴とする請求項４に記載の保護制御モジュール。

[請求項16] コンピュータプログラムを保護する保護制御モジュールを監視する検知モジュールであって、

前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成し、前記保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択し、生成したｄ個

の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する保護制御モジュールから１個の前記分配データを受信する受信手段と、

受信した前記分配データが正しいか否かを判断する検証手段と、

正しいと判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する送信手段とを備え、

前記受信手段は、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取り、

前記検証手段は、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断し、

前記送信手段は、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する

ことを特徴とする検知モジュール。

［請求項17］ 前記検証手段は、

自身の監視結果及び受信した監視結果を用いて、自身を含め、ｄ個の検知モジュールがそれぞれ受信した分配データが正しいと決定したか否かを判断し、

ｄ個の検知モジュールがそれぞれ受信した分配データが正しいと決定した場合に、前記保護制御モジュールが改ざんされていないと決定し、

ｄ個の検知モジュールのうち、少なくとも１個の検知モジュールが受信した分配データが正しくないと決定した場合に、前記保護制御モジュールが改ざんされていると決定する

ことを特徴とする請求項１６に記載の検知モジュール。

［請求項18］ 前記保護制御モジュールは、前記コンピュータプログラムを構成するデータから、検証可能閾値秘密分散法を用いて、ｄ個の前記分配データを生成し、前記検証可能閾値秘密分散法は、ｄより小さいｋ個以上のどの分配データを用いても、元の前記コンピュータプログラムを

復元することができるように、前記コンピュータプログラムを分散する秘密分散法であり、

前記検証手段は、

自身の監視結果及び受信した監視結果を用いて、自身を含め、少なくともｋ個の検知モジュールがそれぞれ受信した分配データが正しいと決定したか否かを判断し、

少なくともｋ個の検知モジュールがそれぞれ受信した分配データが正しいと決定した場合に、前記保護制御モジュールが改ざんされていないと決定し、

（ｄ－ｋ＋１）個以上の検知モジュールがそれぞれ受信した分配データが正しくないと決定した場合に、前記保護制御モジュールが改ざんされていると決定する

ことを特徴とする請求項１６に記載の検知モジュール。

[請求項19] ｎ個の前記検知モジュール及び前記保護制御モジュールは、情報処理装置に含まれ、前記情報処理装置は、前記コンピュータプログラムを記憶している

ことを特徴とする請求項１６に記載の検知モジュール。

[請求項20] 前記検知モジュールは、検知装置に含まれ、

前記保護制御モジュールは、情報処理装置に含まれ、前記情報処理装置は、前記コンピュータプログラムを記憶している

ことを特徴とする請求項１６に記載の検知モジュール。

[請求項21] コンピュータプログラムを保護する保護制御モジュールを制御するための制御方法であって、

前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成ステップと、

当該保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択する選択ステップと、

生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記

検知モジュールへ分配する分配ステップとを含み、

ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出する

ことを特徴とする制御方法。

[請求項22] 保護対象コンピュータプログラムを保護する保護制御モジュールを制御するための制御用プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

コンピュータに、

前記保護対象コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成する生成ステップと、

当該保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択する選択ステップと、

生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する分配ステップとを実行させ、

ｄ個の前記検知モジュールのそれぞれは、受信した前記分配データが正しいか否かを判断して、当該保護制御モジュールの改ざんを検出する

制御用プログラムを記録している記録媒体。

[請求項23] コンピュータプログラムを保護する保護制御モジュールを監視する検知モジュールを制御する制御方法であって、

前記コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成し、前記保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択し、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する保護制御モジュールから１個の前記分配データを受信する受信ステップと、

受信した前記分配データが正しいか否かを判断する検証ステップと

、

正しいと判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する送信ステップとを備え、

前記受信ステップは、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取り、

前記検証ステップは、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断し、

前記送信ステップは、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する

ことを特徴とする制御方法。

[請求項24] 保護対象コンピュータプログラムを保護する保護制御モジュールを監視する検知モジュールを制御する制御用プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

コンピュータに、

前記保護対象コンピュータプログラムを基にして、ｎより小さいｄ個の分配データを生成し、前記保護制御モジュールを監視するためのｎ個の検知モジュールのうち、ｄ個の検知モジュールを選択し、生成したｄ個の前記分配データを、それぞれ、選択したｄ個の前記検知モジュールへ分配する保護制御モジュールから１個の前記分配データを受信する受信ステップと、

受信した前記分配データが正しいか否かを判断する検証ステップと

、

正しいと判断した場合に、他の検知モジュールへ前記分配データが正しいことを示す監視結果を送信する送信ステップとを実行させ、

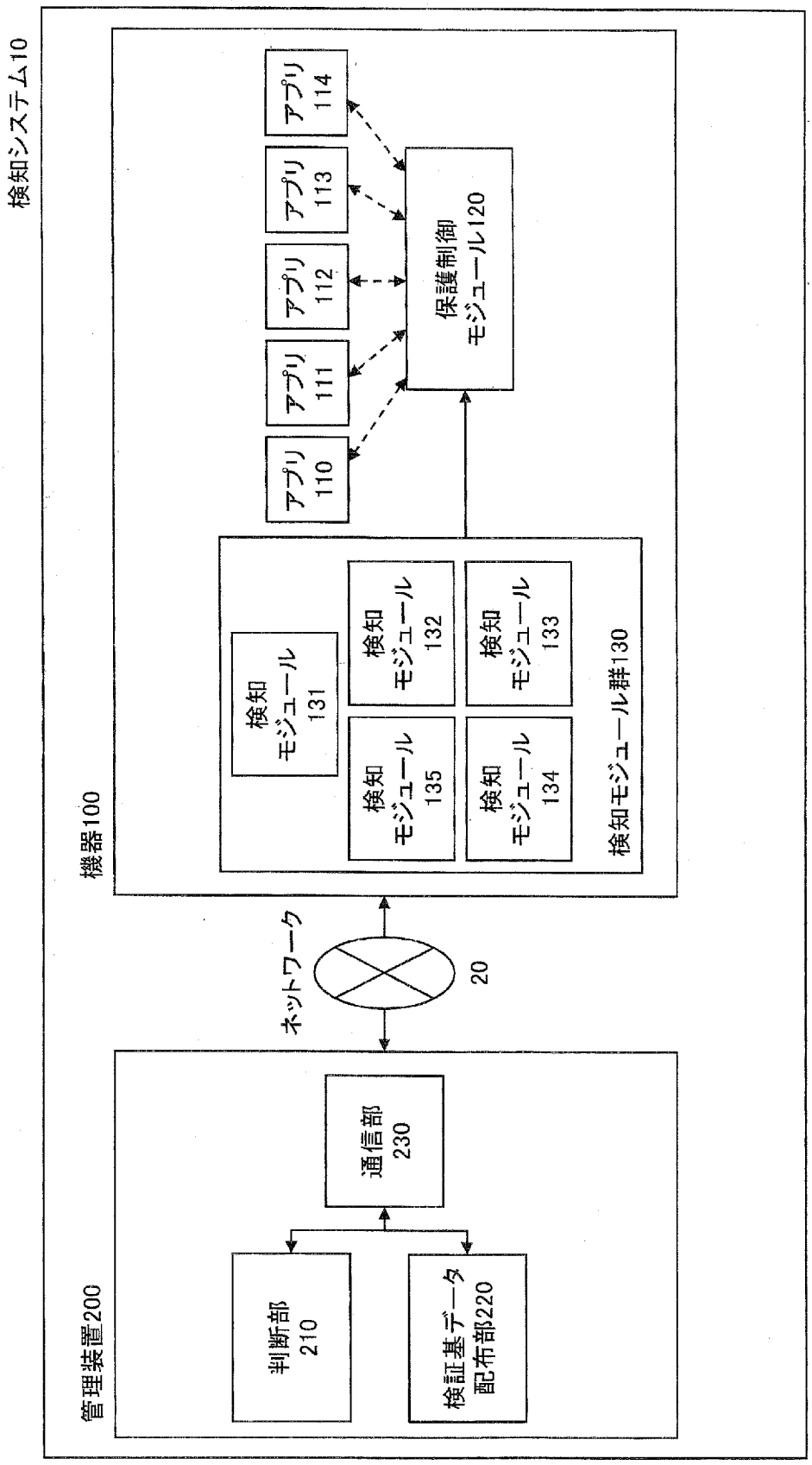
前記受信ステップは、他の検知モジュールから受信した分配データが正しいことを示す監視結果を受け取り、

前記検証ステップは、自身の監視結果及び受信した監視結果を用いて、前記保護制御モジュールが改ざんされているか否かを判断し、

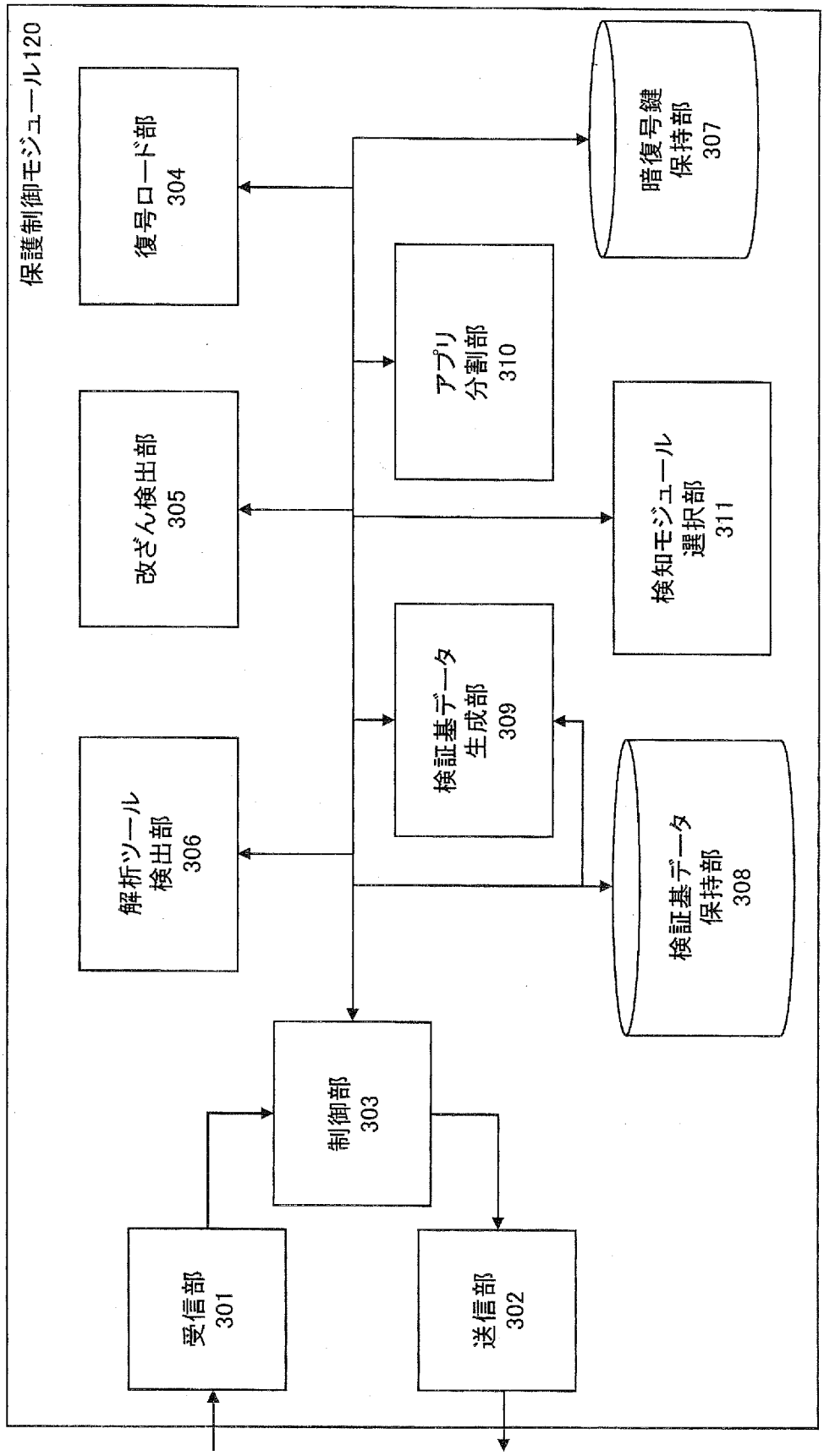
前記送信ステップは、前記保護制御モジュールが改ざんされているか否かを示す判断結果を送信する

制御用プログラムを記録している記録媒体。

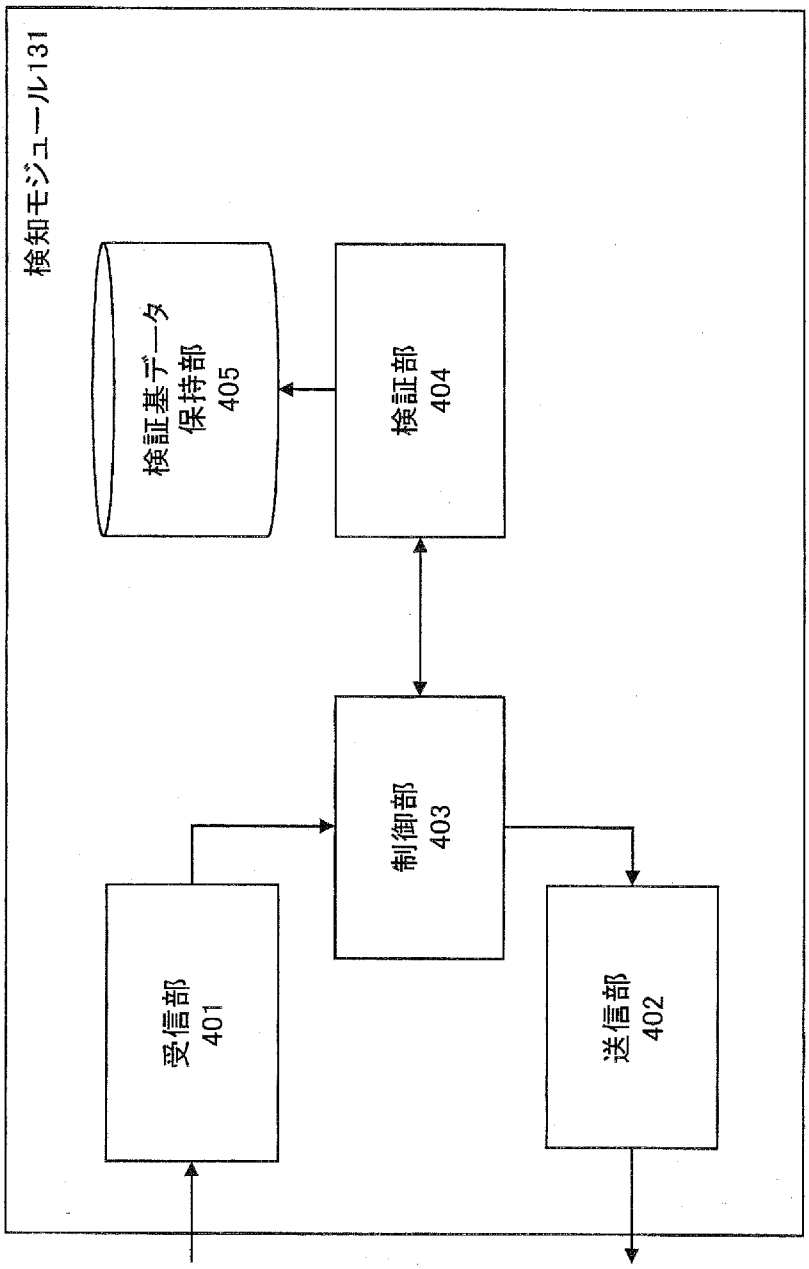
[図1]


検知システム10
機器100
アプリ 110
アプリ 111
アプリ 112
アプリ 113
アプリ 114
保護制御 モジュール120
検知モジュール群130
検知 モジュール 131
検知 モジュール 132
検知 モジュール 133
検知 モジュール 134
検知 モジュール 135
ネットワーク
20
管理装置200
通信部 230
判断部 210
検証基データ 配布部220

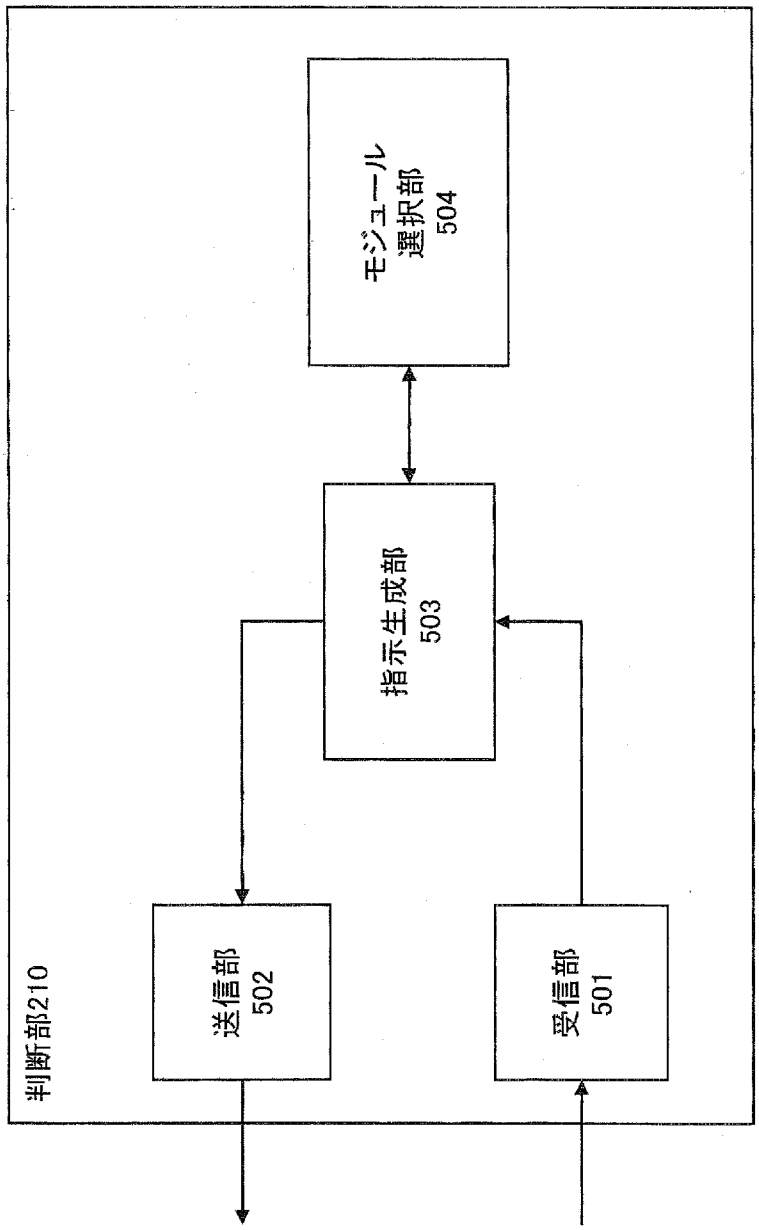
[図2]


保護制御モジュール120
復号ロード部
304
暗復号鍵
保持部
307
アプリ
分割部
310
改ざん検出部
305
検知モジュール
選択部
311
検証基データ
生成部
309
解析ツール
検出部
306
検証基データ
保持部
308
制御部
303
受信部
301
送信部
302

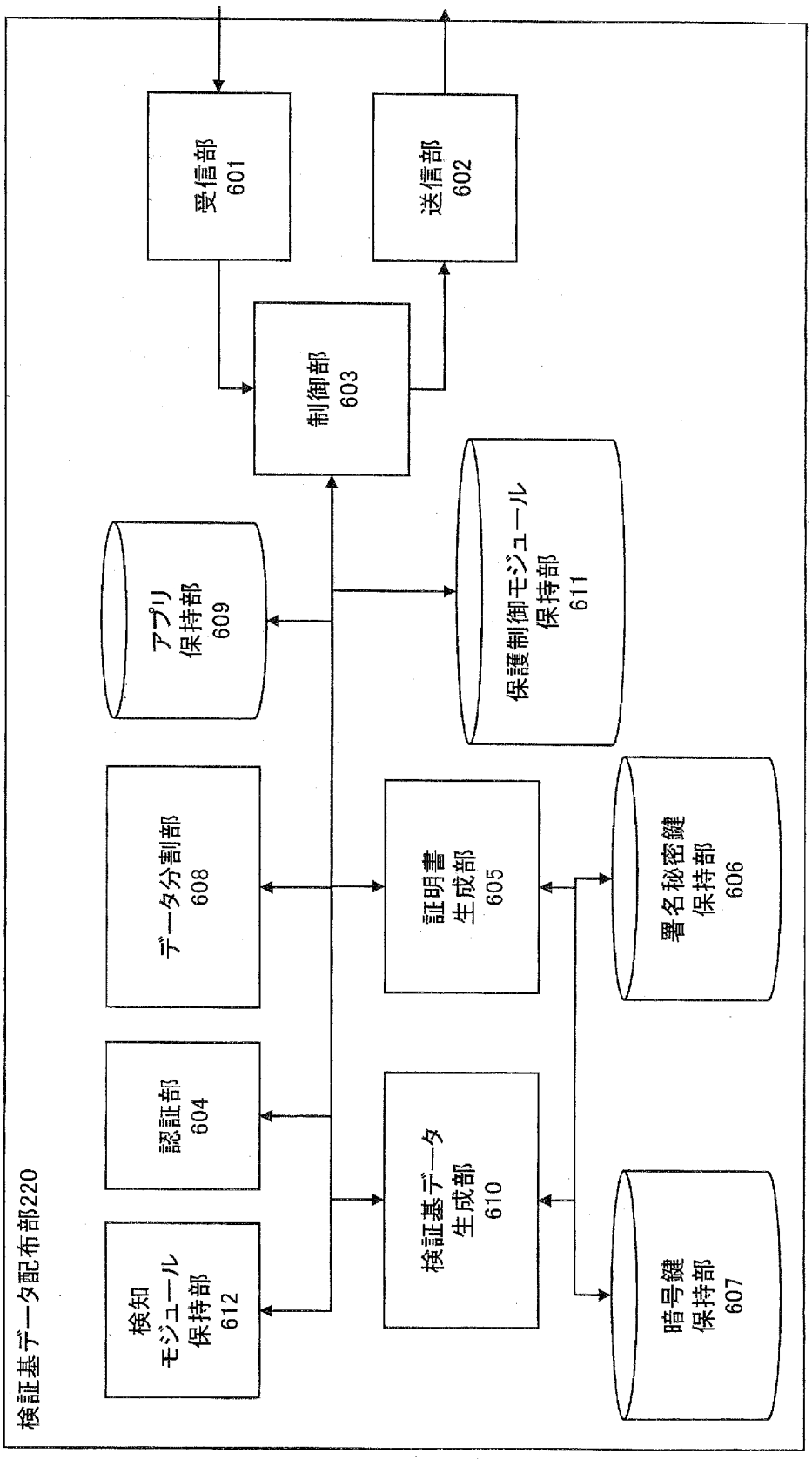
[図3]



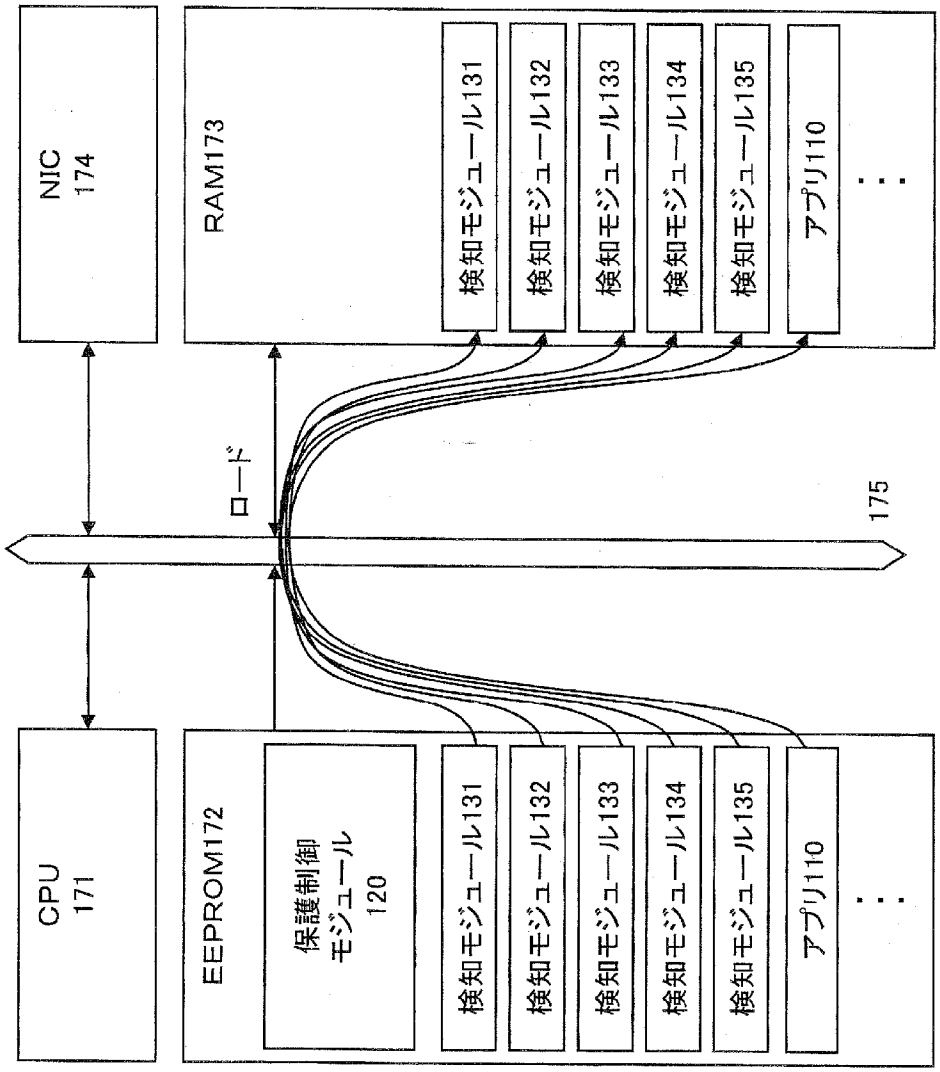
[図4]



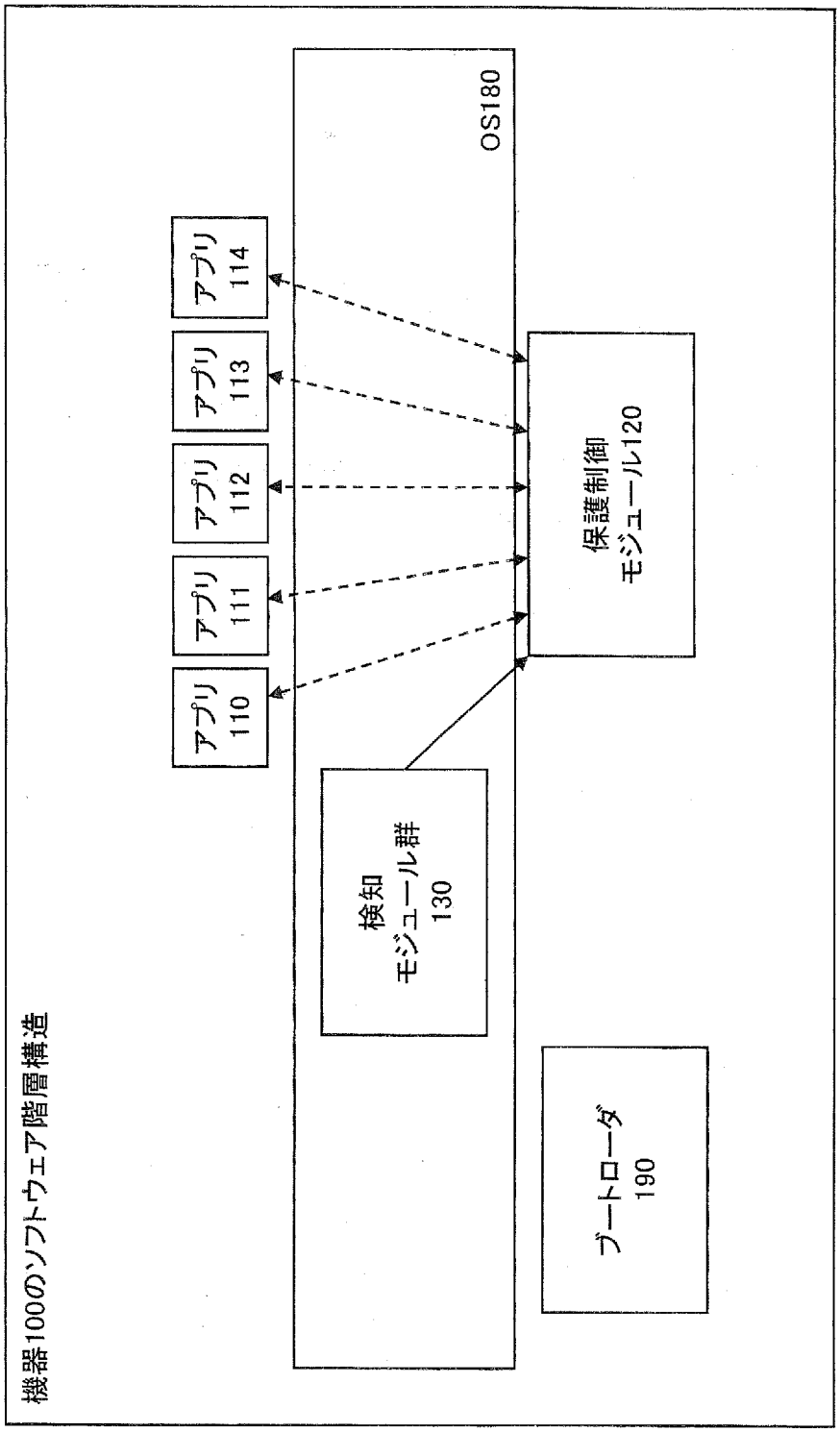
[図5]


検証基データ配布部220
受信部 601
送信部 602
制御部 603
アプリ保持部 609
保護制御モジュール保持部 611
データ分割部 608
証明書生成部 605
署名秘密鍵保持部 606
認証部 604
検証基データ生成部 610
検知モジュール保持部 612
暗号鍵保持部 607

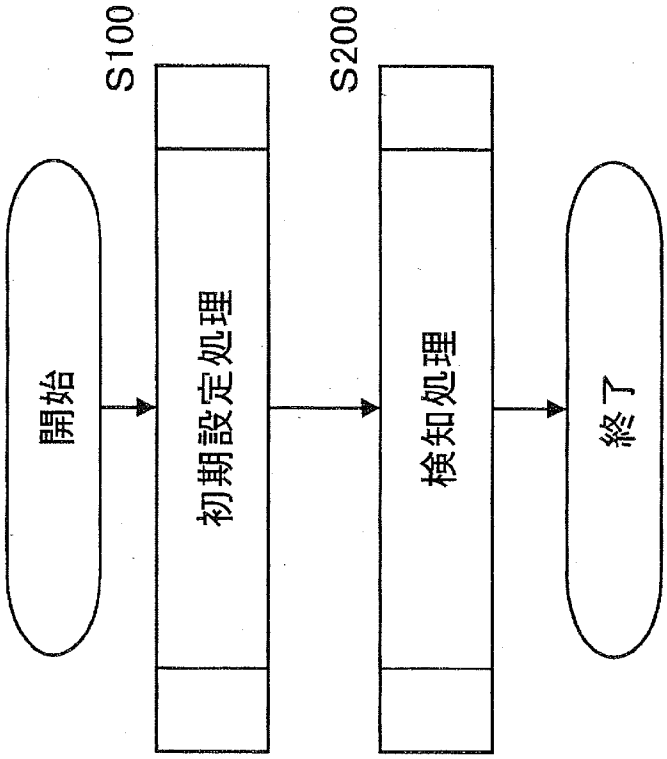
[図6]


NIC
174
RAM173
検知モジュール131
検知モジュール132
検知モジュール133
検知モジュール134
検知モジュール135
アプリ110
ロード
175
CPU
171
EEPROM172
保護制御
モジュール
120
検知モジュール131
検知モジュール132
検知モジュール133
検知モジュール134
検知モジュール135
アプリ110

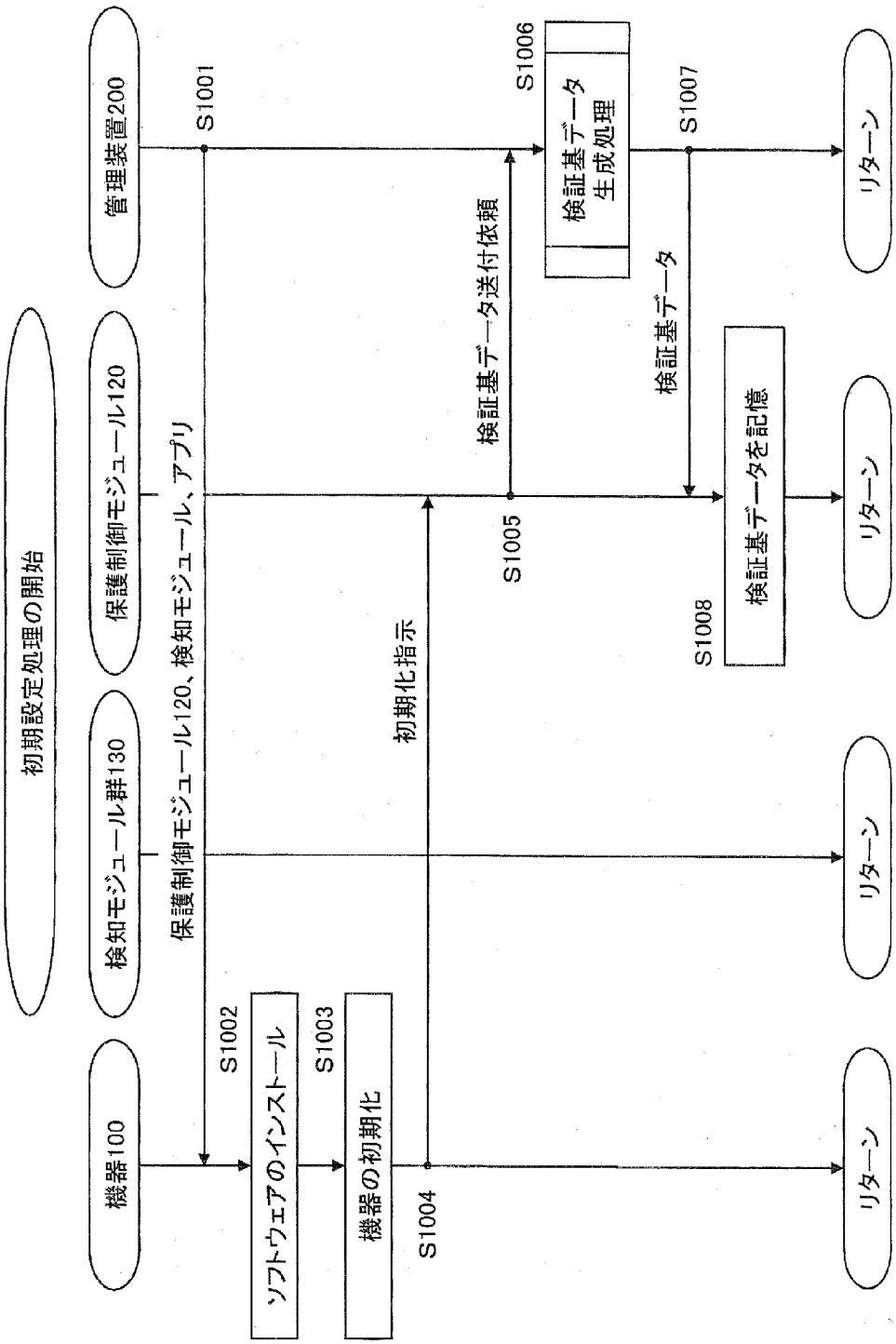
[図7]


機器100のソフトウェア階層構造
OS180
アプリ
110
アプリ
111
アプリ
112
アプリ
113
アプリ
114
保護制御
モジュール120
検知
モジュール群
130
ブートローダ
190

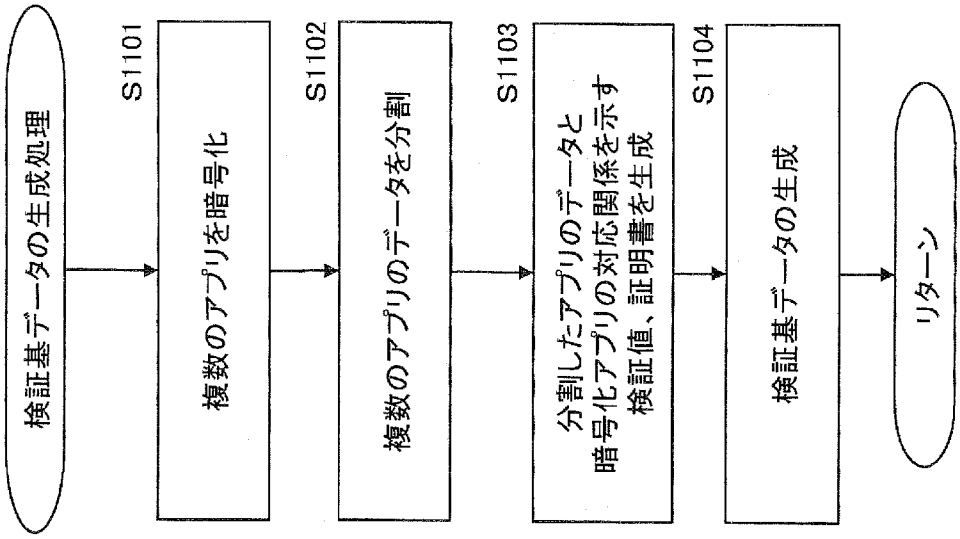
[図8]



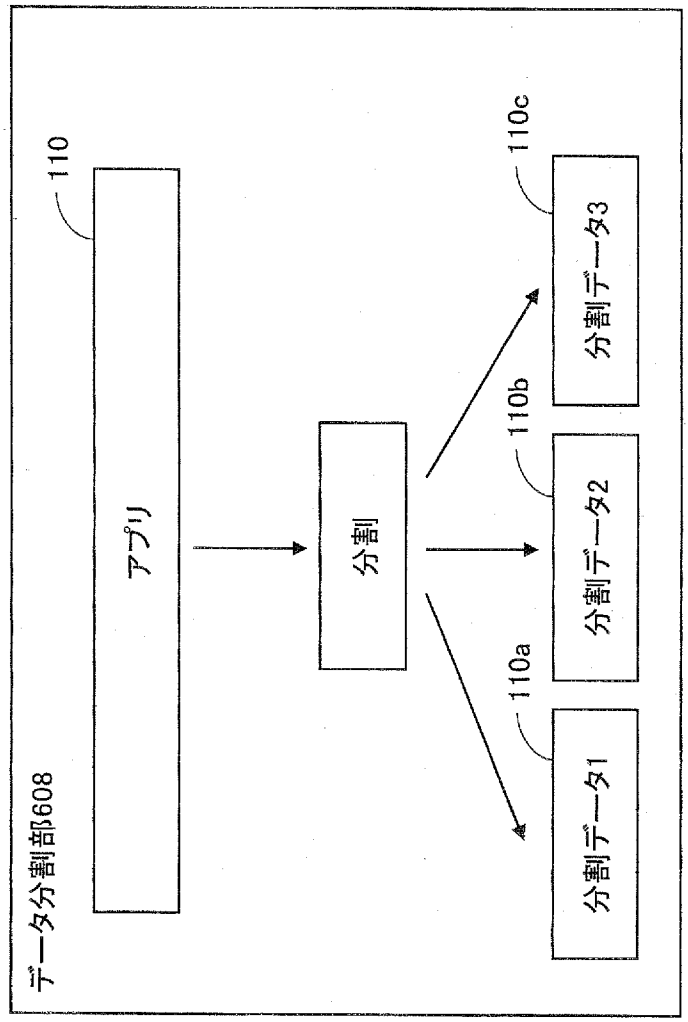
[図9]


初期設定処理の開始
機器100
検知モジュール群130
保護制御モジュール120
管理装置200
保護制御モジュール120、検知モジュール、アプリ
S1001
S1002
ソフトウェアのインストール
S1003
機器の初期化
S1004
初期化指示
検証基データ送付依頼
S1005
S1006
検証基データ生成処理
検証基データ
S1007
S1008
検証基データを記憶
リターン
リターン
リターン
リターン

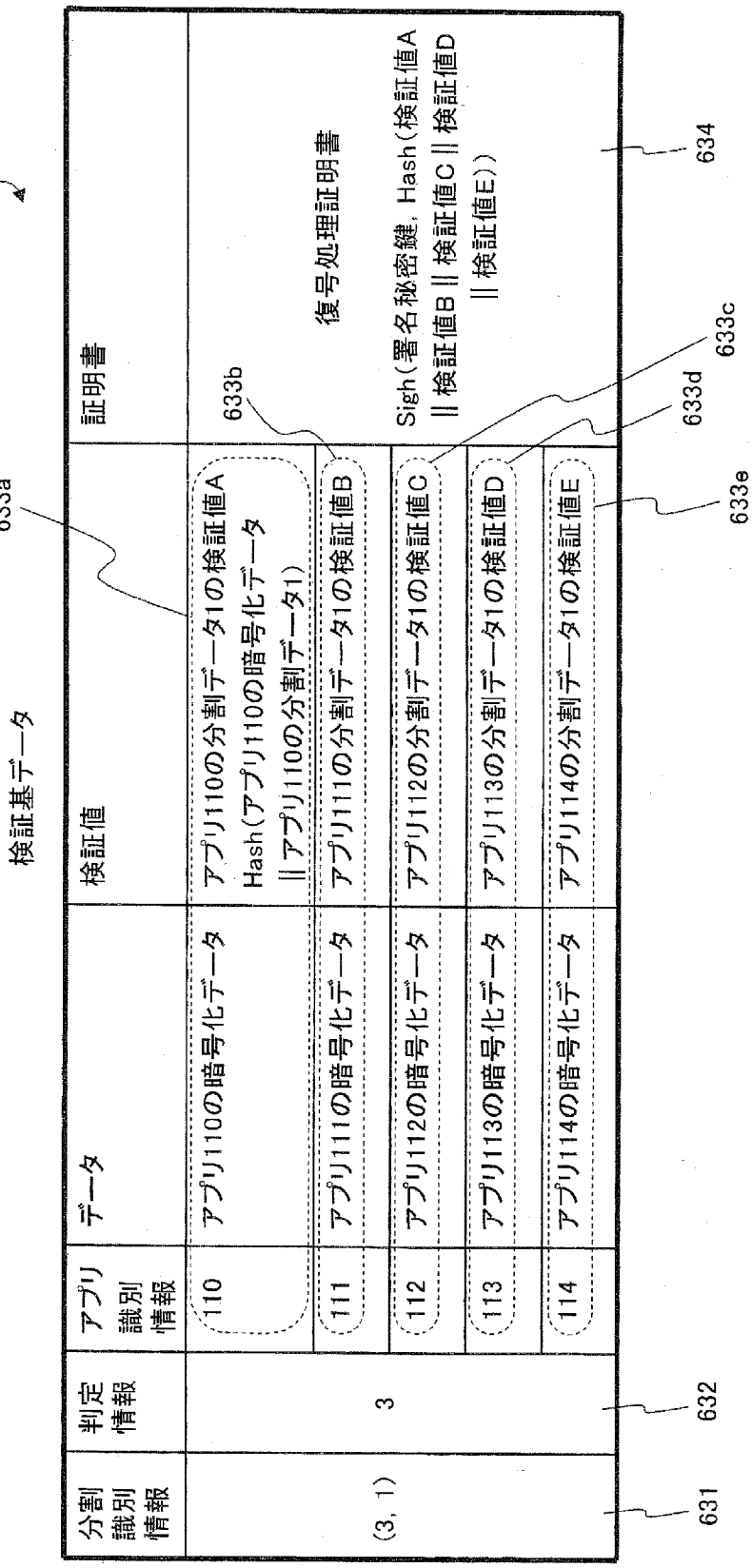
[図10]


検証基データの生成処理
S1101
複数のアプリを暗号化
S1102
複数のアプリのデータを分割
S1103
分割したアプリのデータと
暗号化アプリの対応関係を示す
検証値、証明書を生成
S1104
検証基データの生成
リターン

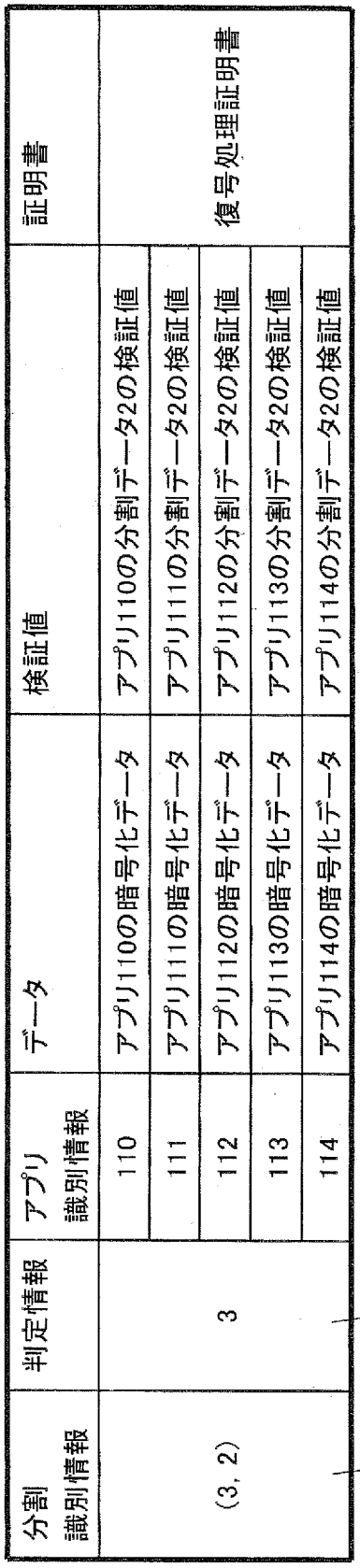
[図11]



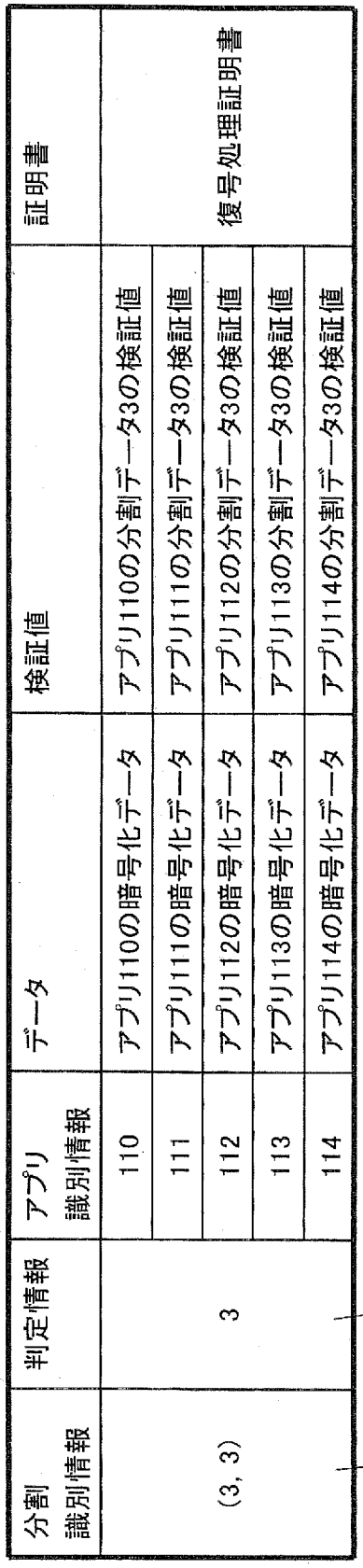
[図12]


630
検証基データ
633a
633b
633c
633d
633e
634
632
631
分割識別情報
判定情報
アプリ識別情報
データ
検証値
証明書
(3, 1)
3
110
111
112
113
114
アプリ110の暗号化データ
アプリ111の暗号化データ
アプリ112の暗号化データ
アプリ113の暗号化データ
アプリ114の暗号化データ
アプリ110の分割データ1の検証値A
Hash(アプリ110の暗号化データ
|| アプリ110の分割データ1)
アプリ111の分割データ1の検証値B
アプリ112の分割データ1の検証値C
アプリ113の分割データ1の検証値D
アプリ114の分割データ1の検証値E
復号処理証明書
Sigh(署名秘密鍵, Hash(検証値A
|| 検証値B || 検証値C || 検証値D
|| 検証値E))

[図13]

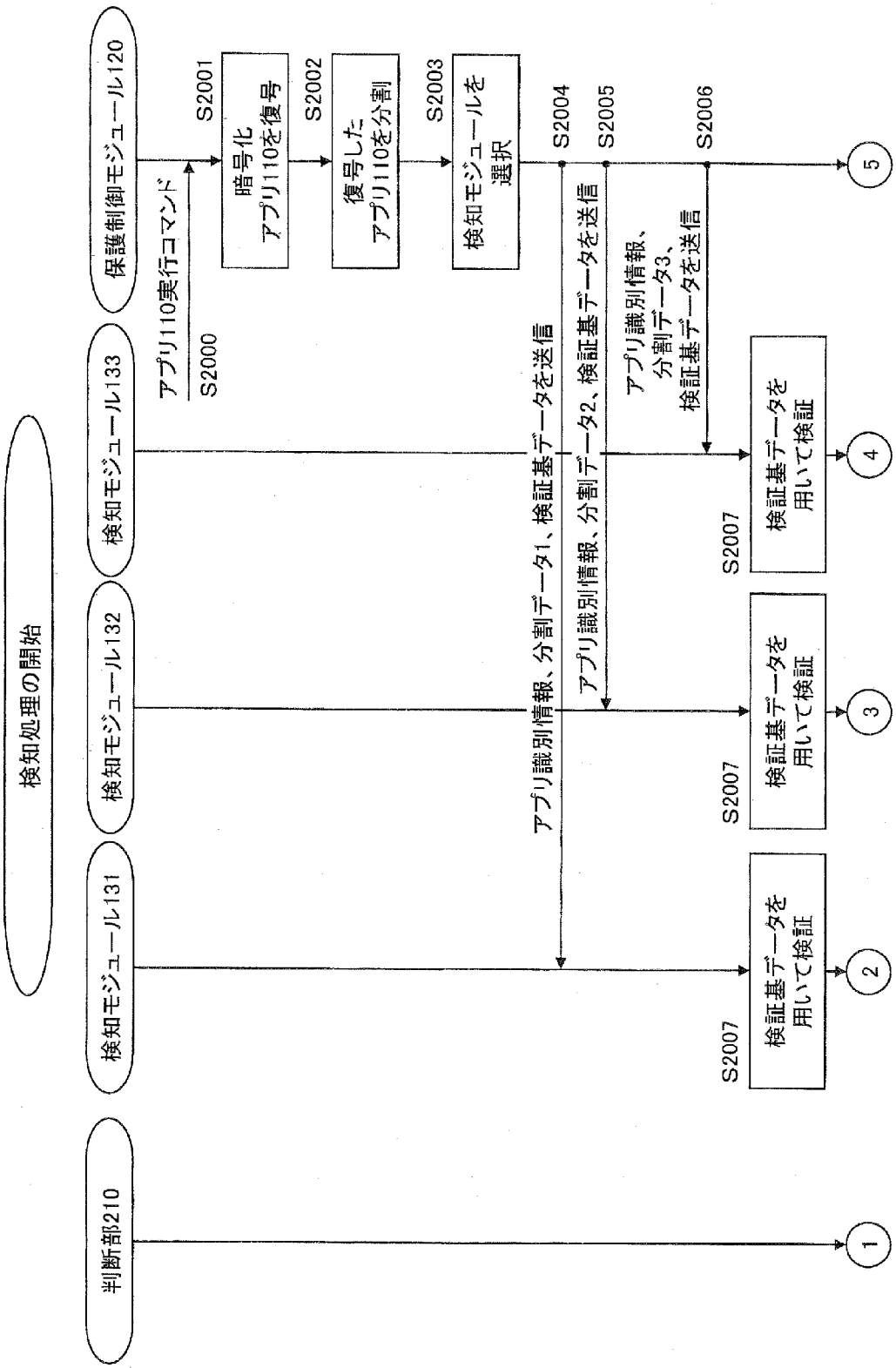

650
検証基データ
分割識別情報
判定情報
アプリ識別情報
データ
検証値
証明書
(3, 2)
3
110
アプリ110の暗号化データ
アプリ110の分割データ2の検証値
111
アプリ111の暗号化データ
アプリ111の分割データ2の検証値
112
アプリ112の暗号化データ
アプリ112の分割データ2の検証値
113
アプリ113の暗号化データ
アプリ113の分割データ2の検証値
114
アプリ114の暗号化データ
アプリ114の分割データ2の検証値
復号処理証明書
651
652

[図14]

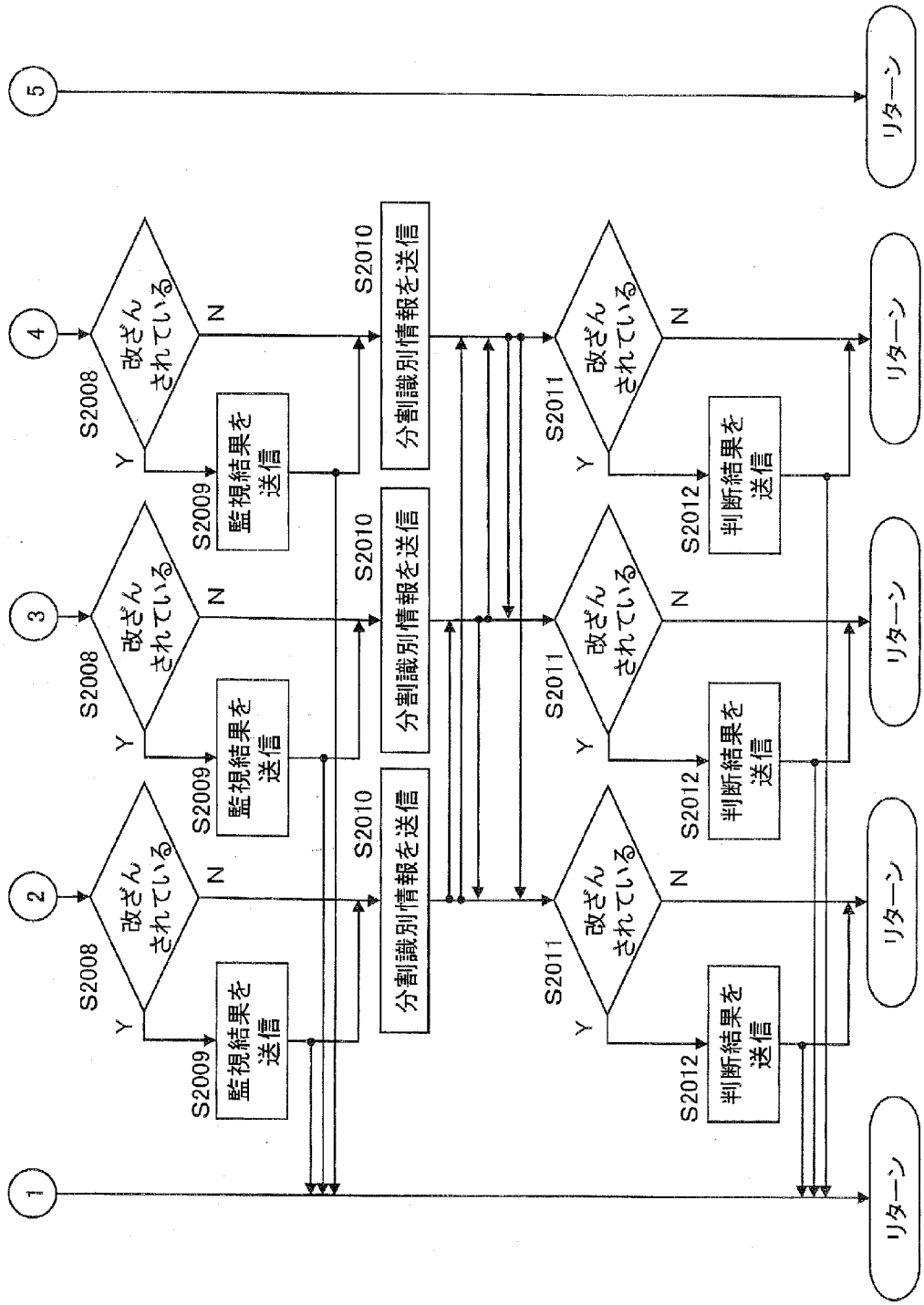


分割識別情報	判定情報	アプリ識別情報	データ	検証値	証明書
(3, 3)	3	110	アプリ110の暗号化データ	アプリ110の分割データ3の検証値	復号処理証明書
		111	アプリ111の暗号化データ	アプリ111の分割データ3の検証値	
		112	アプリ112の暗号化データ	アプリ112の分割データ3の検証値	
		113	アプリ113の暗号化データ	アプリ113の分割データ3の検証値	
		114	アプリ114の暗号化データ	アプリ114の分割データ3の検証値	

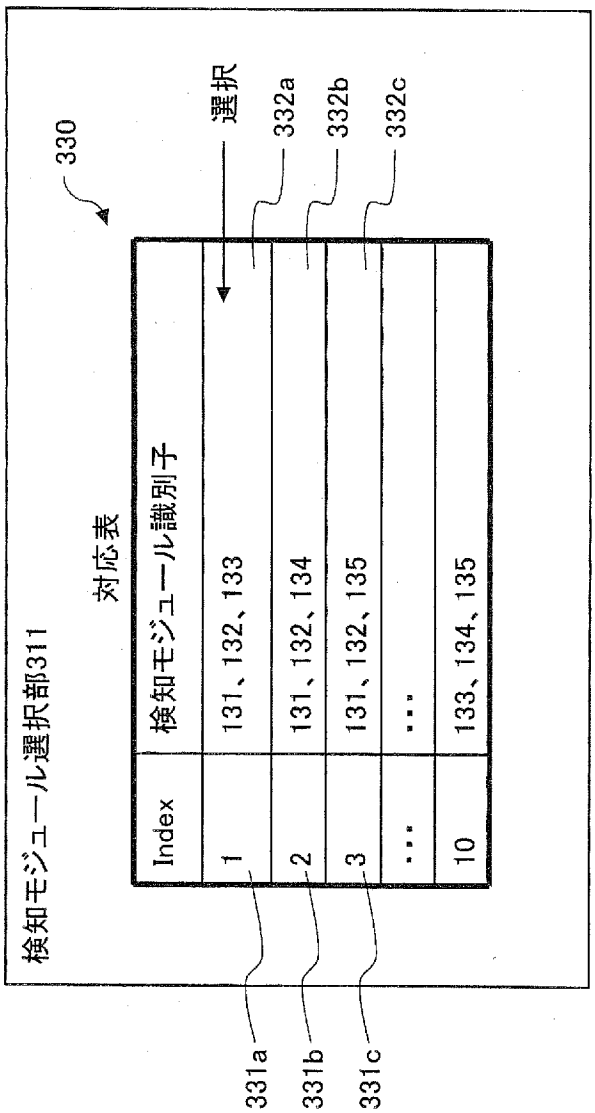
[図15]


検知処理の開始
判断部210
検知モジュール131
検知モジュール132
検知モジュール133
保護制御モジュール120
アプリ110実行コマンド
S2000
S2001
暗号化
アプリ110を復号
S2002
復号した
アプリ110を分割
S2003
検知モジュールを
選択
S2004
アプリ識別情報、分割データ1、検証基データを送信
S2005
アプリ識別情報、分割データ2、検証基データを送信
S2006
アプリ識別情報、
分割データ3、
検証基データを送信
S2007
検証基データを
用いて検証
S2007
検証基データを
用いて検証
S2007
検証基データを
用いて検証
1
2
3
4
5

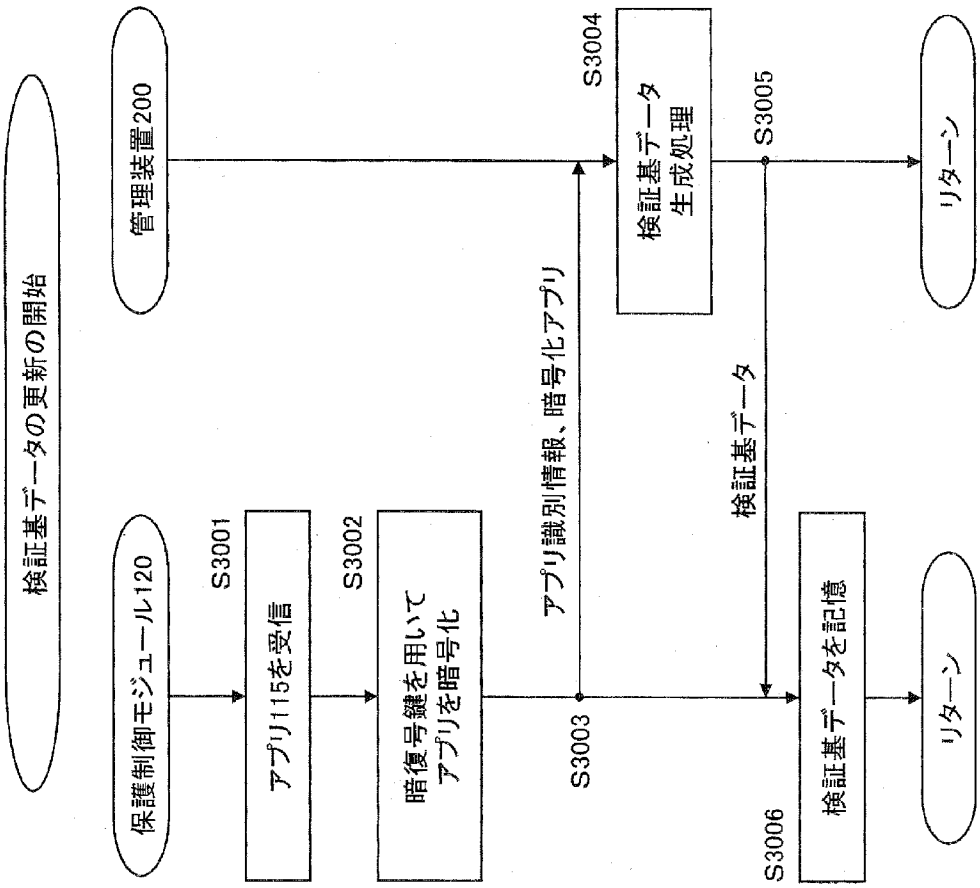
[図16]


1
2
3
4
5
S2008
改ざんされている
Y
N
S2009
監視結果を送信
S2010
分割識別情報を送信
S2011
改ざんされている
Y
N
S2012
判断結果を送信
リターン

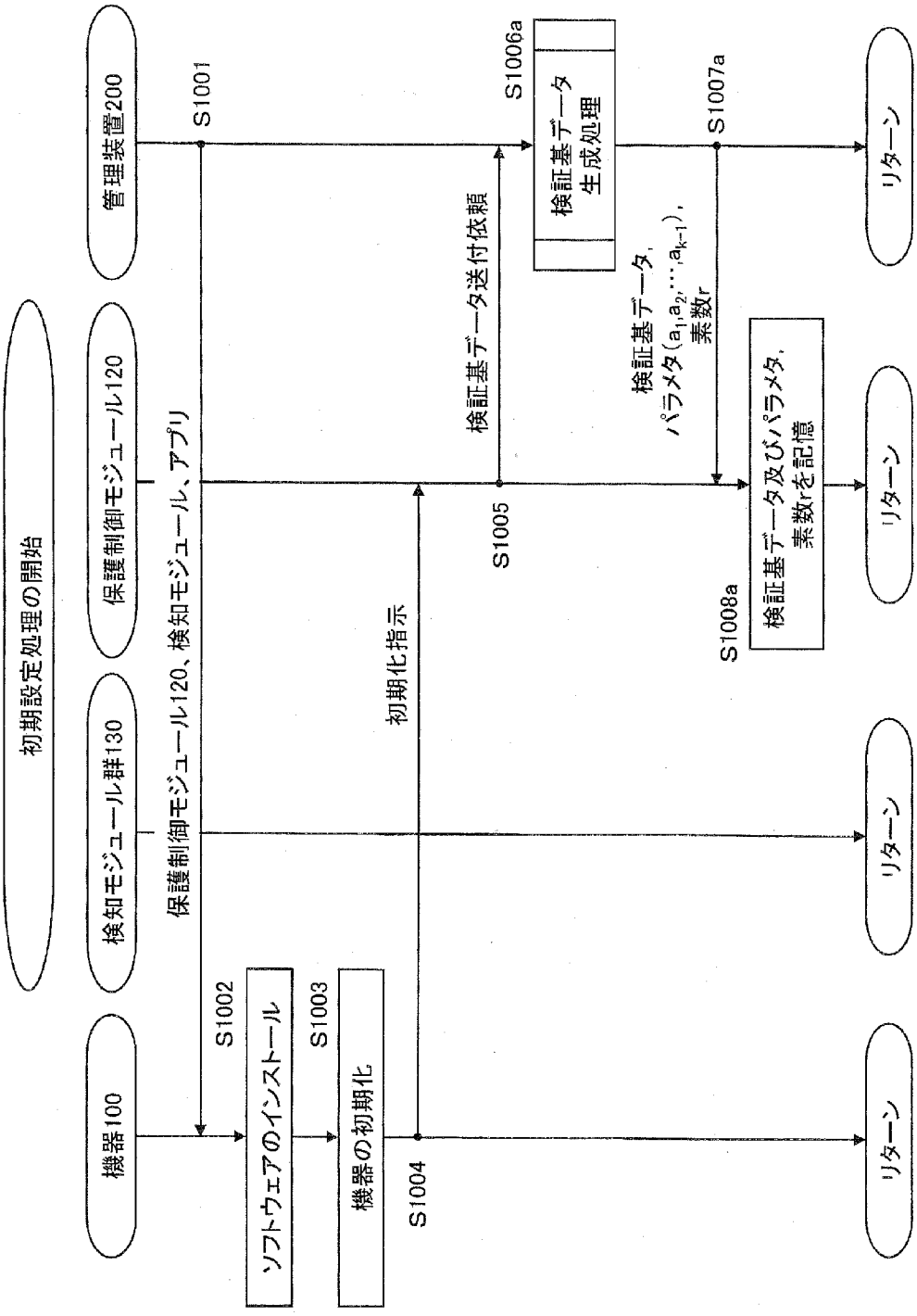
[図17]


検知モジュール選択部311
330
対応表
選択
332a
332b
332c
Index
検知モジュール識別子
1
131、132、133
2
131、132、134
3
131、132、135
...
...
10
133、134、135
331a
331b
331c

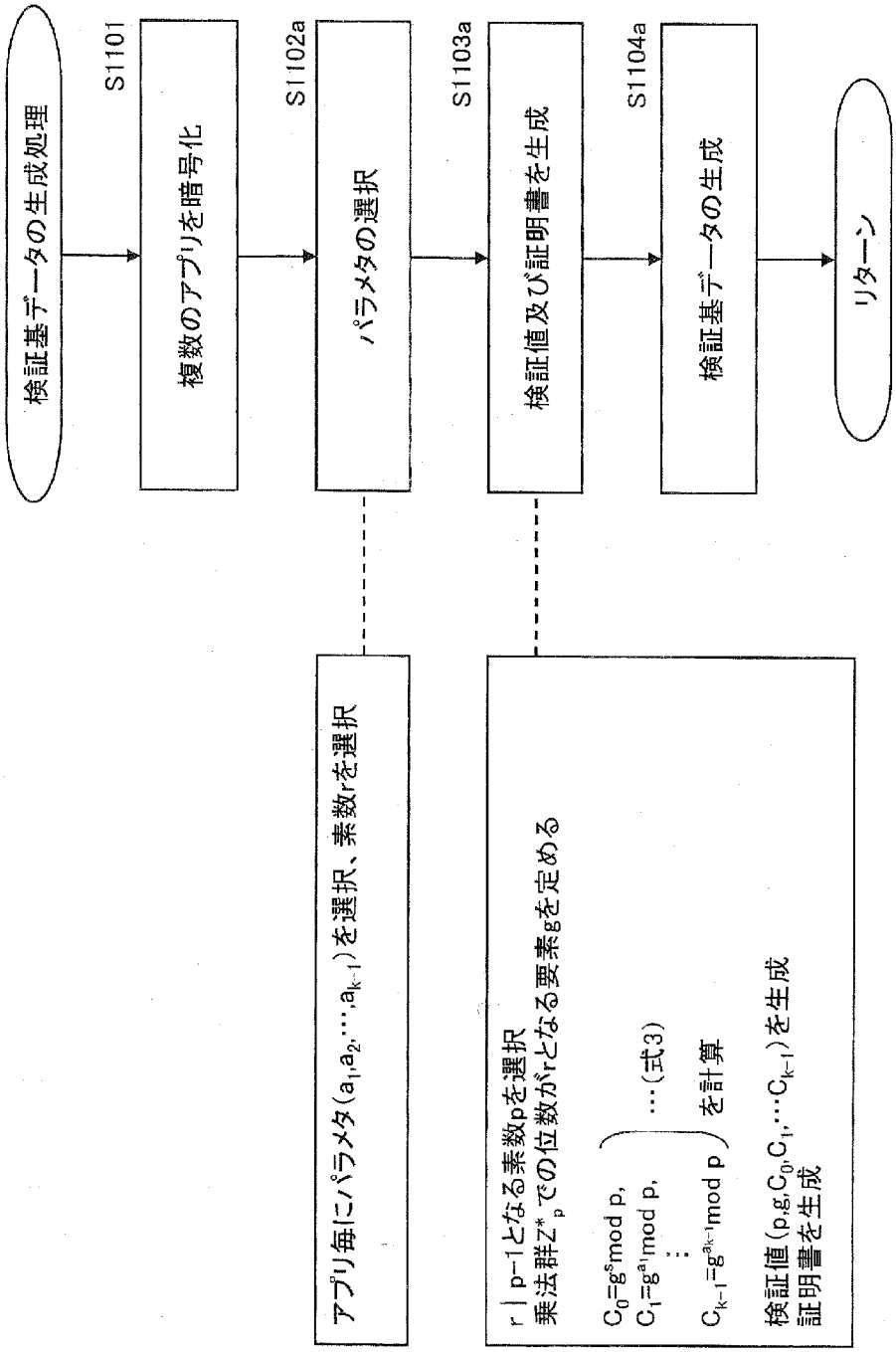
[図18]


検証基データの更新の開始
管理装置200
保護制御モジュール120
S3001
アプリ115を受信
S3002
暗復号鍵を用いて
アプリを暗号化
アプリ識別情報、暗号化アプリ
S3003
S3004
検証基データ
生成処理
S3005
検証基データ
S3006
検証基データを記憶
リターン
リターン

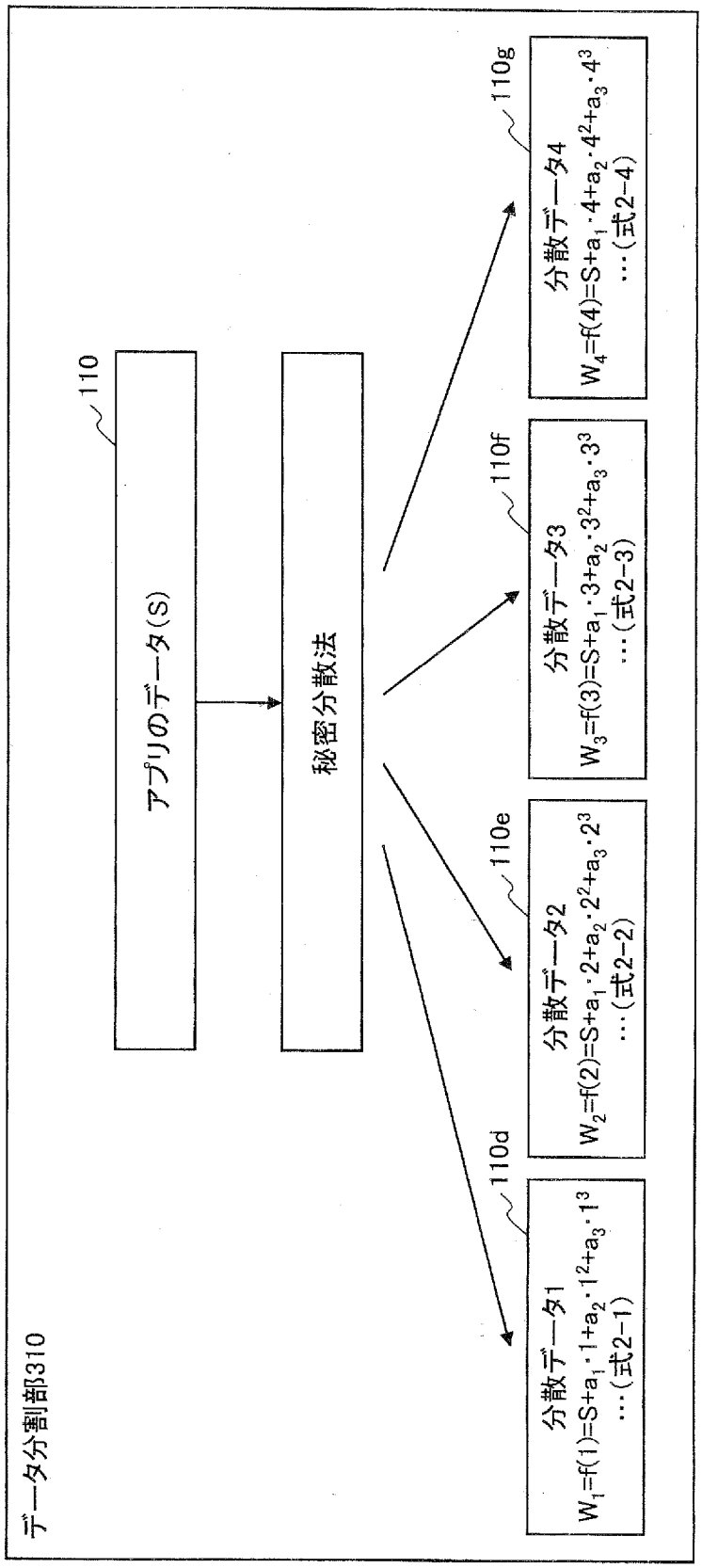
[図19]


初期設定処理の開始
機器100
検知モジュール群130
保護制御モジュール120
管理装置200
保護制御モジュール120、検知モジュール、アプリ
S1001
S1002
ソフトウェアのインストール
S1003
機器の初期化
S1004
初期化指示
S1005
検証基データ送付依頼
S1006a
検証基データ生成処理
S1007a
検証基データ,
パラメタ($a_1,a_2,\cdots,a_{k-1}$),
素数r
S1008a
検証基データ及びパラメタ,
素数rを記憶
リターン
リターン
リターン
リターン

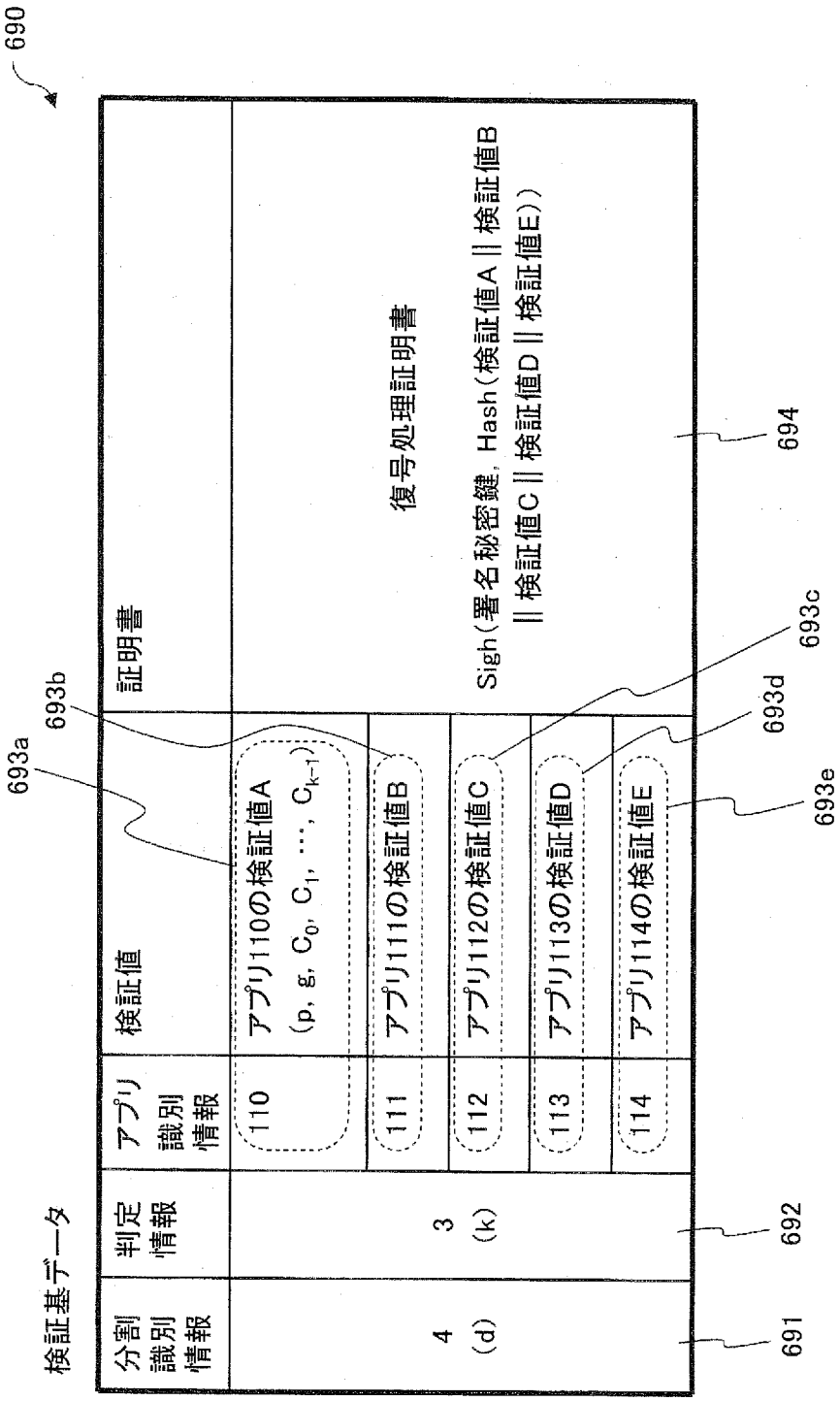
[図20]


検証基データの生成処理
S1101
複数のアプリを暗号化
S1102a
パラメタの選択
S1103a
検証値及び証明書を生成
S1104a
検証基データの生成
リターン
アプリ毎にパラメタ($a_1,a_2,\cdots,a_{k-1}$)を選択、素数rを選択
r | p−1となる素数pを選択
乗法群Z^*_pでの位数がrとなる要素gを定める
$C_0=g^s \bmod p$,
$C_1=g^{a_1} \bmod p$,
$C_{k-1}=g^{a_{k-1}} \bmod p$
…(式3)
を計算
検証値(p,g,$C_0,C_1,\cdots C_{k-1}$)を生成
証明書を生成

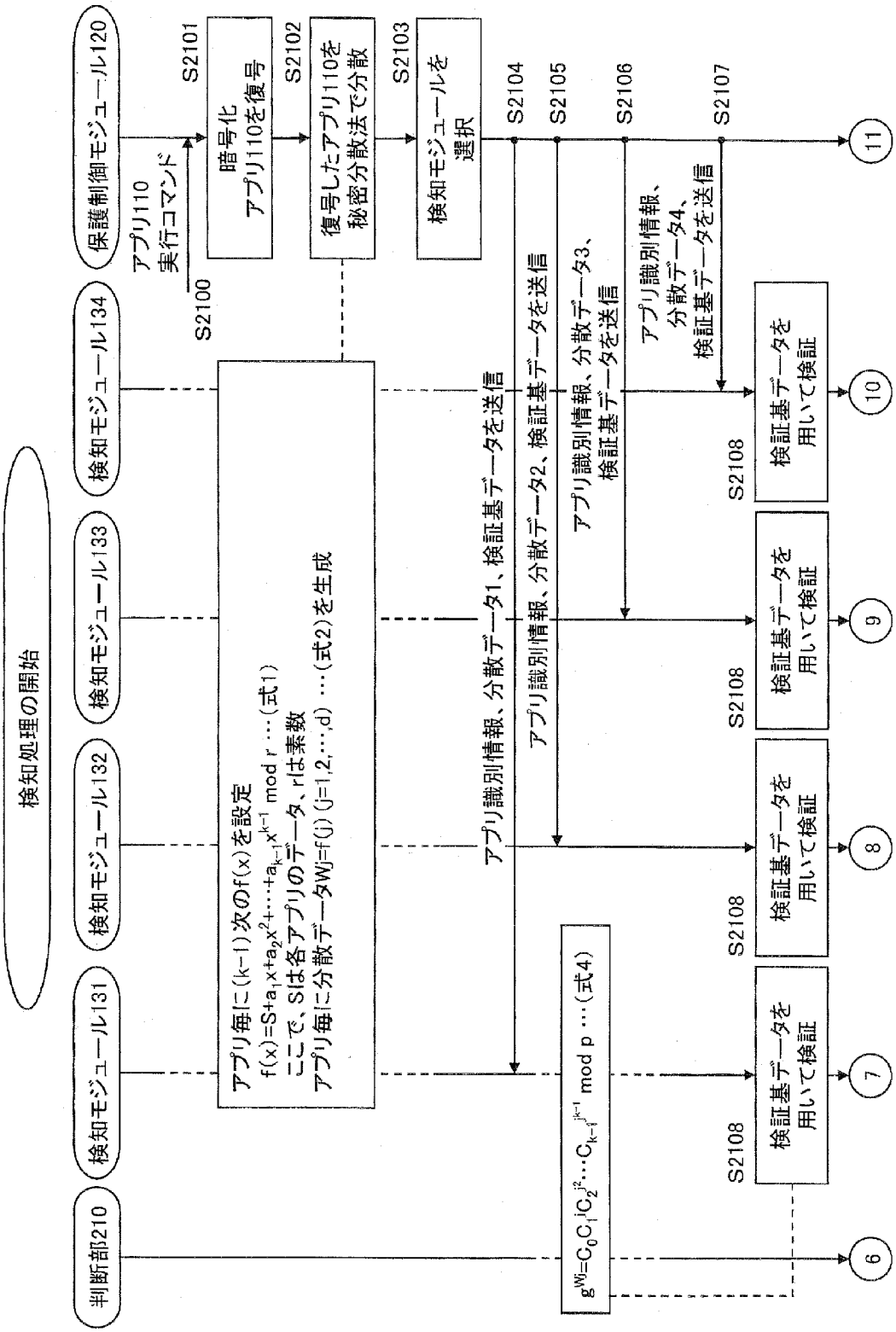
[図21]


データ分割部310
110
アプリのデータ(S)
秘密分散法
110d
分散データ1
$W_1=f(1)=S+a_1\cdot1+a_2\cdot1^2+a_3\cdot1^3$
…(式2-1)
110e
分散データ2
$W_2=f(2)=S+a_1\cdot2+a_2\cdot2^2+a_3\cdot2^3$
…(式2-2)
110f
分散データ3
$W_3=f(3)=S+a_1\cdot3+a_2\cdot3^2+a_3\cdot3^3$
…(式2-3)
110g
分散データ4
$W_4=f(4)=S+a_1\cdot4+a_2\cdot4^2+a_3\cdot4^3$
…(式2-4)

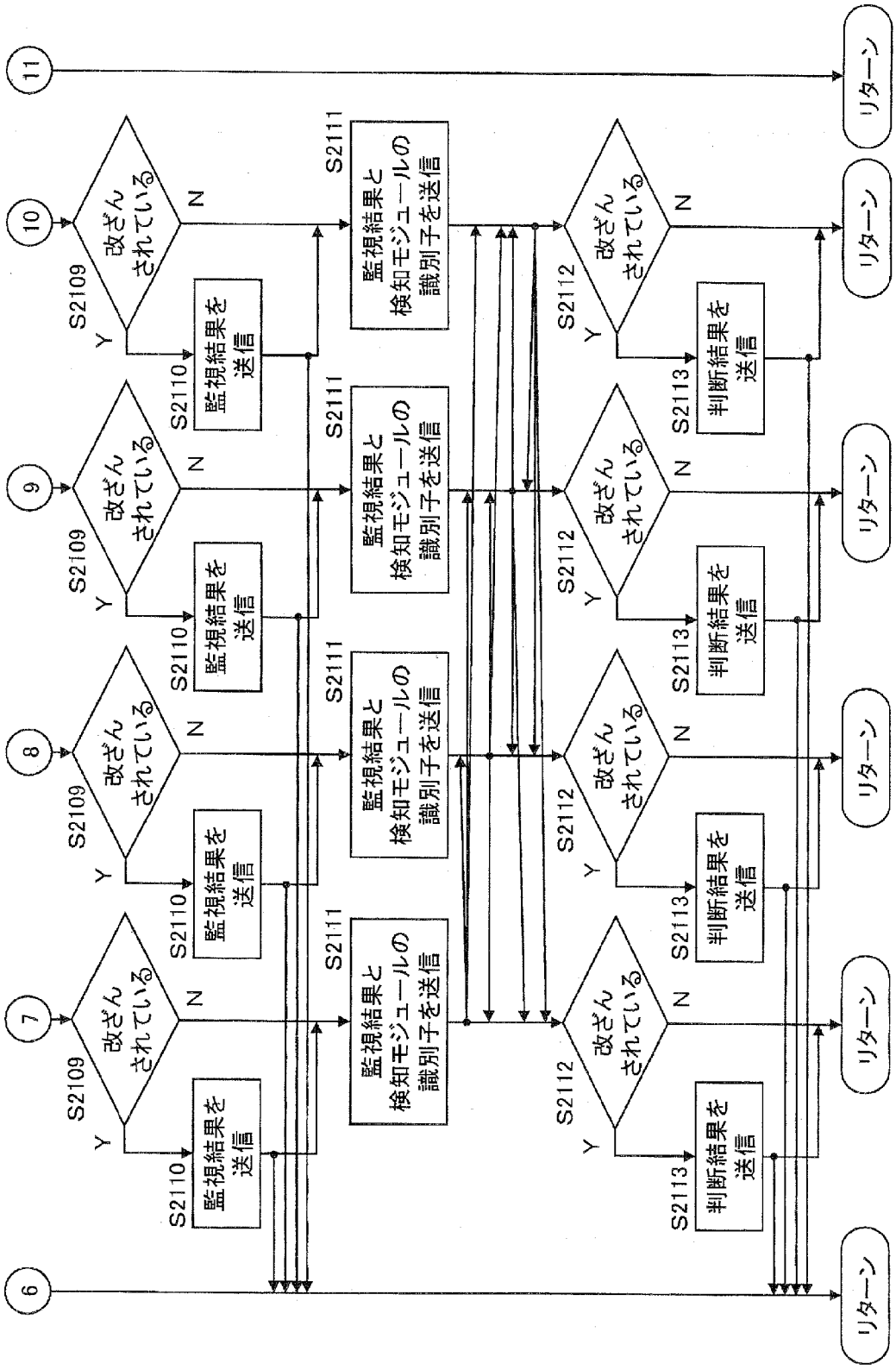
[図22]


690
検証基データ
分割識別情報
判定情報
アプリ識別情報
検証値
証明書
4
(d)
3
(k)
110
111
112
113
114
アプリ110の検証値A
(p, g, C_0, C_1, …, C_{k-1})
アプリ111の検証値B
アプリ112の検証値C
アプリ113の検証値D
アプリ114の検証値E
復号処理証明書
Sigh(署名秘密鍵, Hash(検証値A || 検証値B
|| 検証値C || 検証値D || 検証値E))
691
692
693a
693b
693c
693d
693e
694

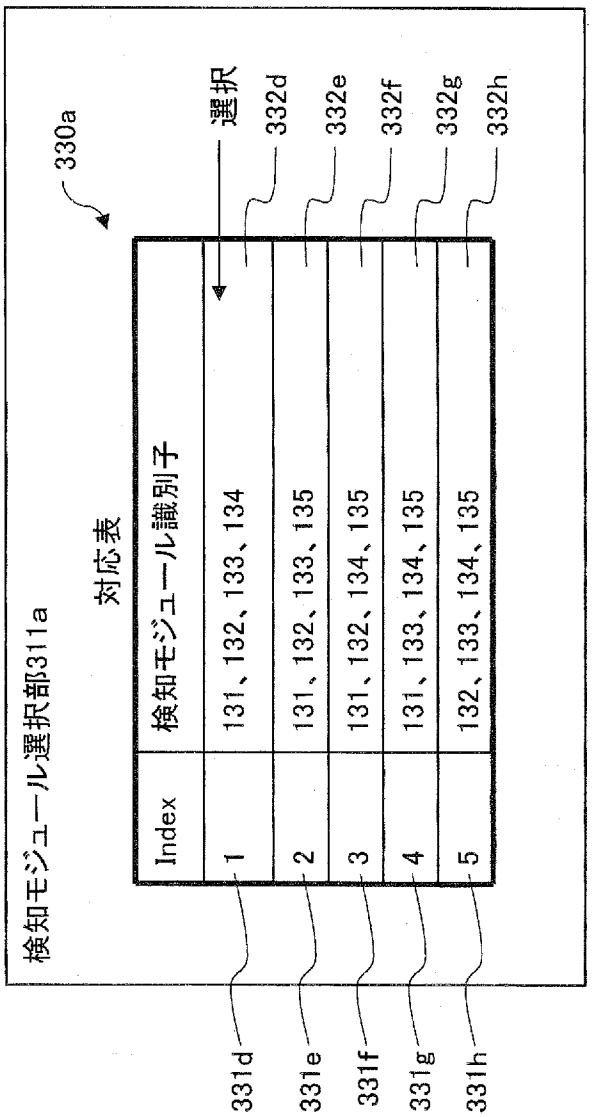
[図23]


検知処理の開始
判断部210
検知モジュール131
検知モジュール132
検知モジュール133
検知モジュール134
保護制御モジュール120
アプリ110
実行コマンド
S2100
S2101
暗号化
アプリ110を復号
S2102
復号したアプリ110を
秘密分散法で分散
S2103
検知モジュールを
選択
S2104
S2105
S2106
S2107
アプリ毎に(k−1)次のf(x)を設定
f(x)=S+a1x+a2x2+…+ak−1xk−1 mod r …(式1)
ここで、Sは各アプリのデータ、rは素数
アプリ毎に分散データWj=f(j) (j=1,2,…,d) …(式2)を生成
アプリ識別情報、分散データ1、検証基データを送信
アプリ識別情報、分散データ2、検証基データを送信
アプリ識別情報、分散データ3、
検証基データを送信
アプリ識別情報、
分散データ4、
検証基データを送信
gWj=C0C1jC2j2…Ck−1jk−1 mod p …(式4)
S2108
検証基データを
用いて検証
6
7
8
9
10
11

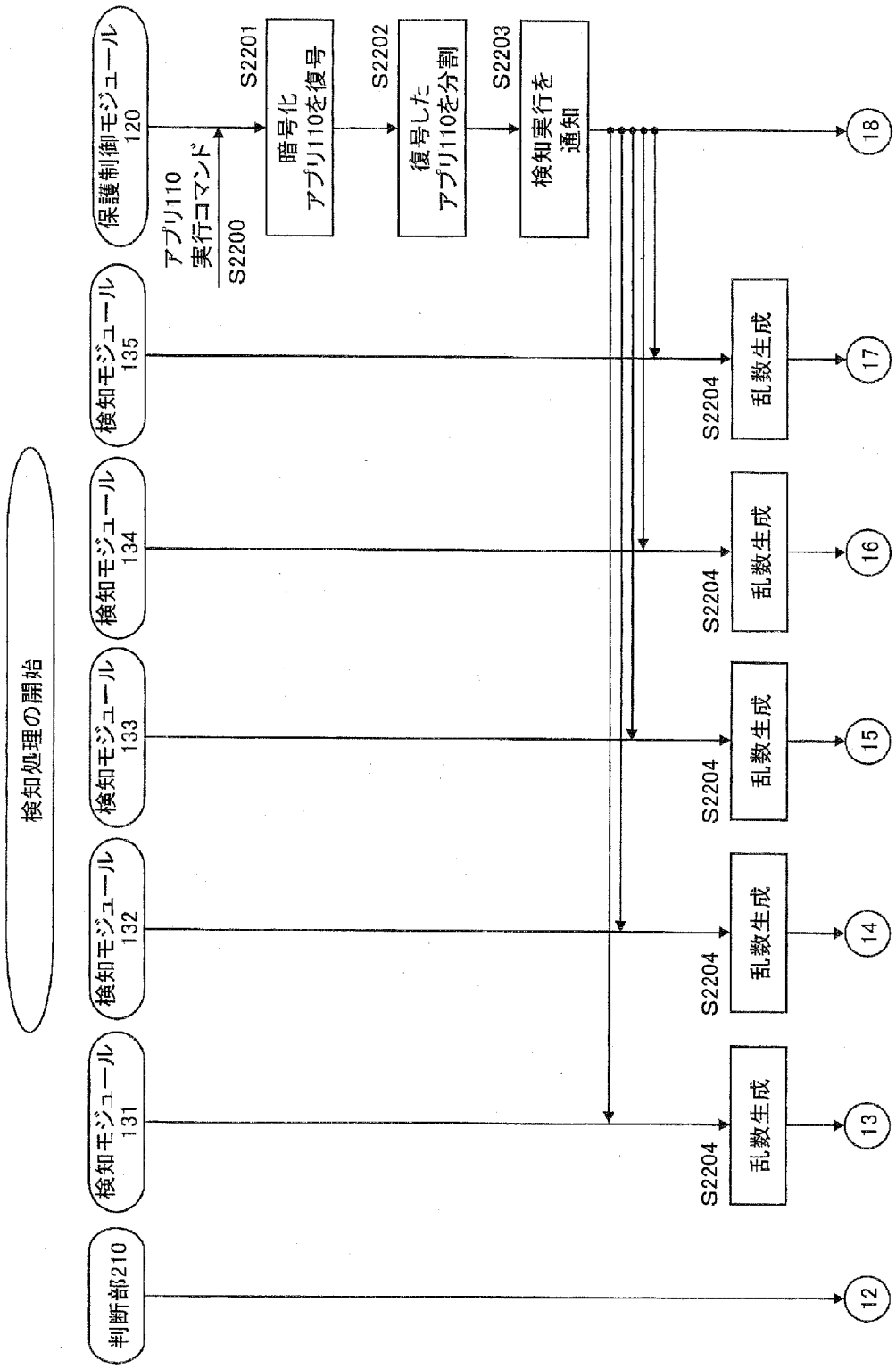
[図24]


6
7
8
9
10
11
S2109
改ざんされている
Y
N
S2110
監視結果を送信
S2111
監視結果と検知モジュールの識別子を送信
S2112
改ざんされている
Y
N
S2113
判断結果を送信
リターン

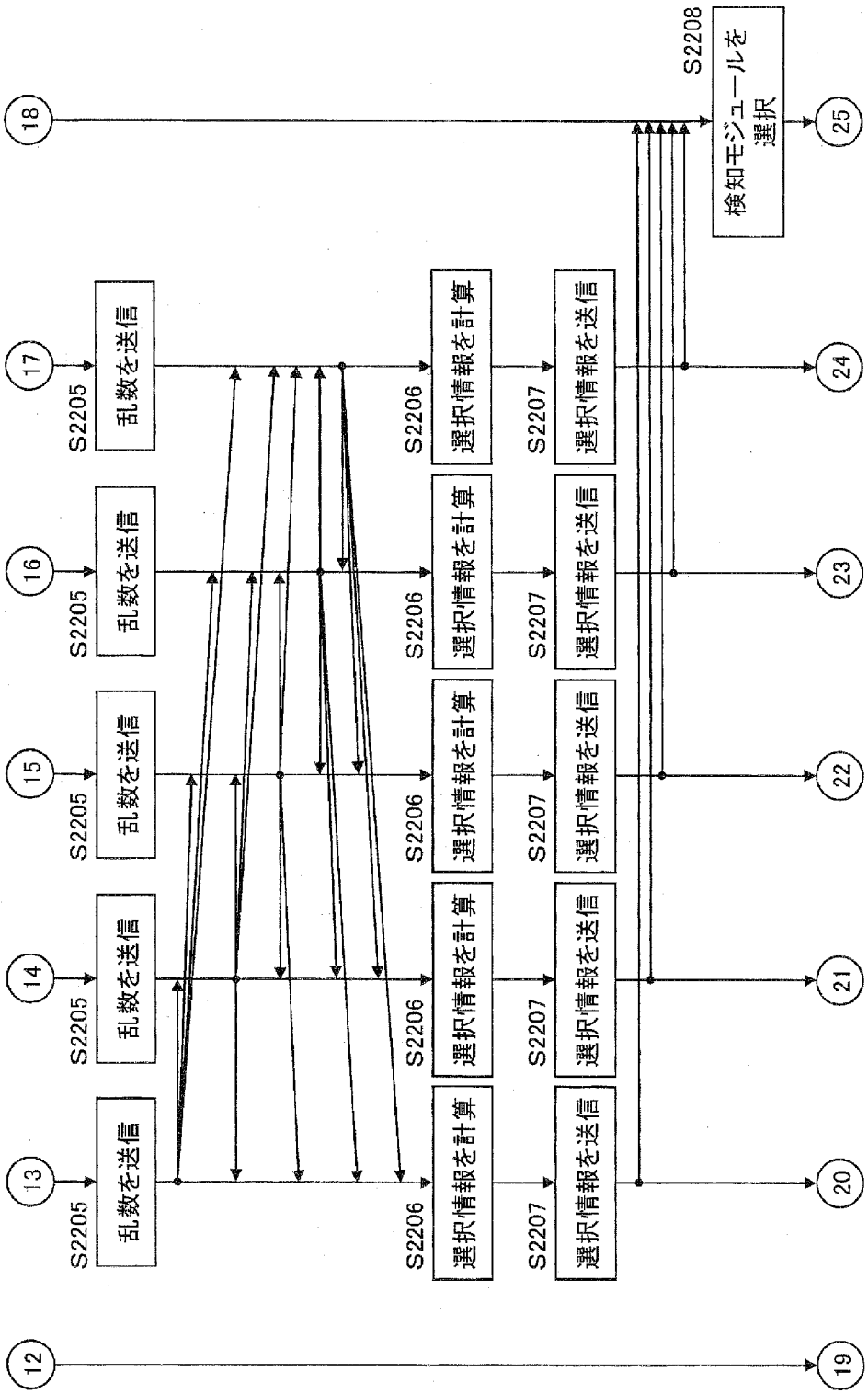
[図25]


検知モジュール選択部311a
330a
対応表
Index
検知モジュール識別子
選択
1
131、132、133、134
2
131、132、133、135
3
131、132、134、135
4
131、133、134、135
5
132、133、134、135
331d
331e
331f
331g
331h
332d
332e
332f
332g
332h

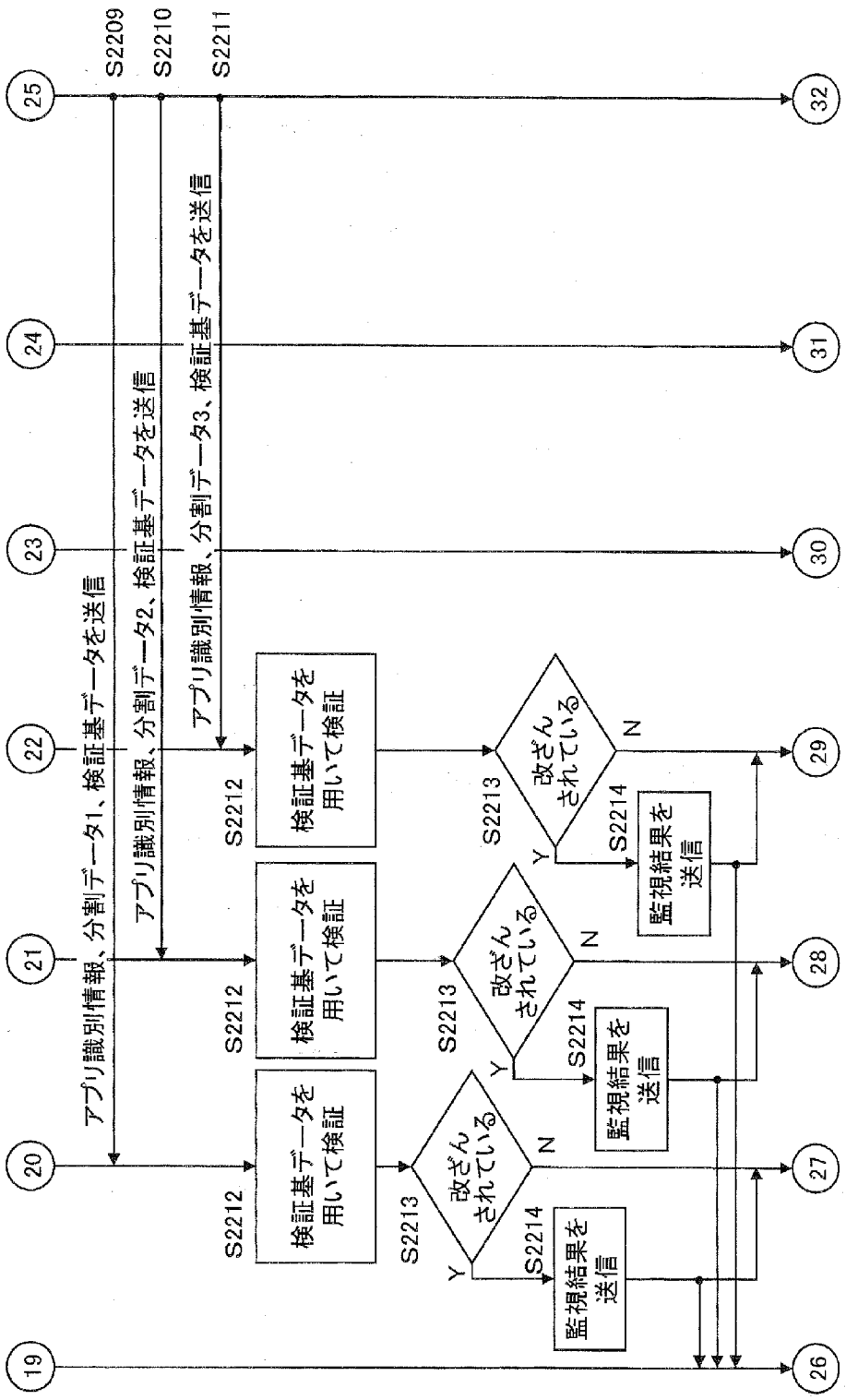
[図26]


検知処理の開始
判断部210
検知モジュール 131
検知モジュール 132
検知モジュール 133
検知モジュール 134
検知モジュール 135
保護制御モジュール 120
アプリ110 実行コマンド
S2200
S2201
暗号化 アプリ110を復号
S2202
復号した アプリ110を分割
S2203
検知実行を 通知
S2204
乱数生成
12
13
14
15
16
17
18

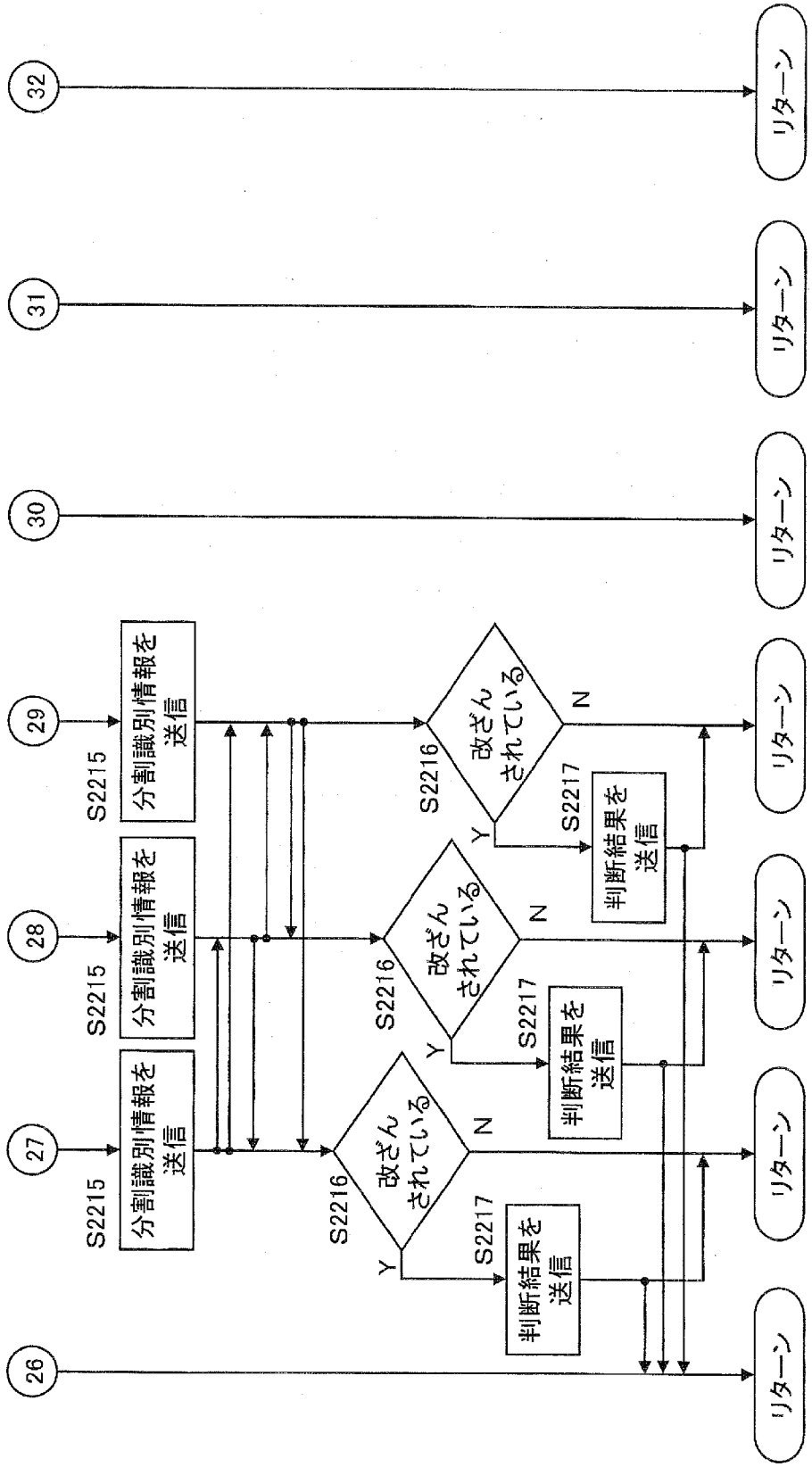
[図27]


12
13
14
15
16
17
18
19
20
21
22
23
24
25
S2205
乱数を送信
S2206
選択情報を計算
S2207
選択情報を送信
S2208
検知モジュールを選択

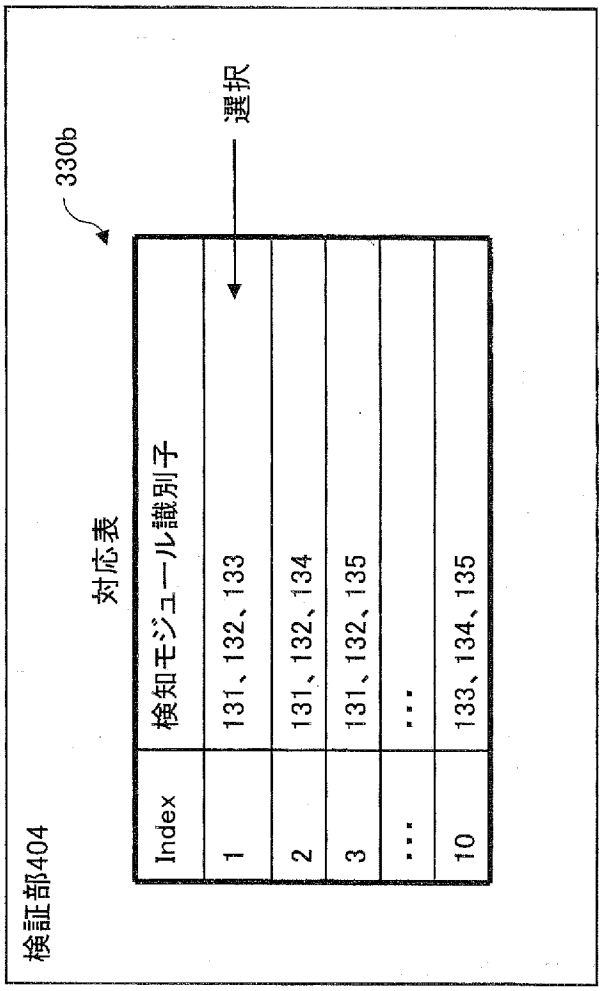
[図28]


S2209
S2210
S2211
アプリ識別情報、分割データ1、検証基データを送信
アプリ識別情報、分割データ2、検証基データを送信
アプリ識別情報、分割データ3、検証基データを送信
検証基データを用いて検証
改ざんされている
監視結果を送信
S2212
S2213
S2214
Y
N
19
20
21
22
23
24
25
26
27
28
29
30
31
32

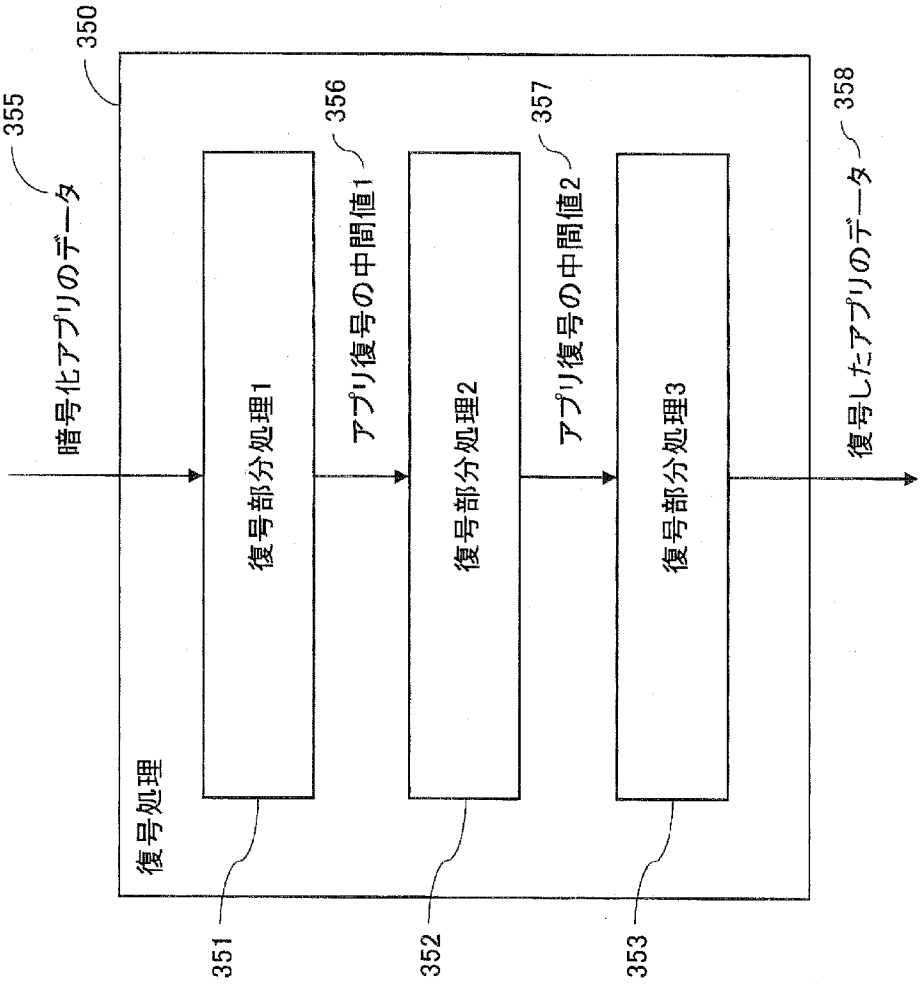
[図29]


32
31
30
29
28
27
26
S2215
分割識別情報を送信
S2216
改ざんされている
Y
N
S2217
判断結果を送信
リターン

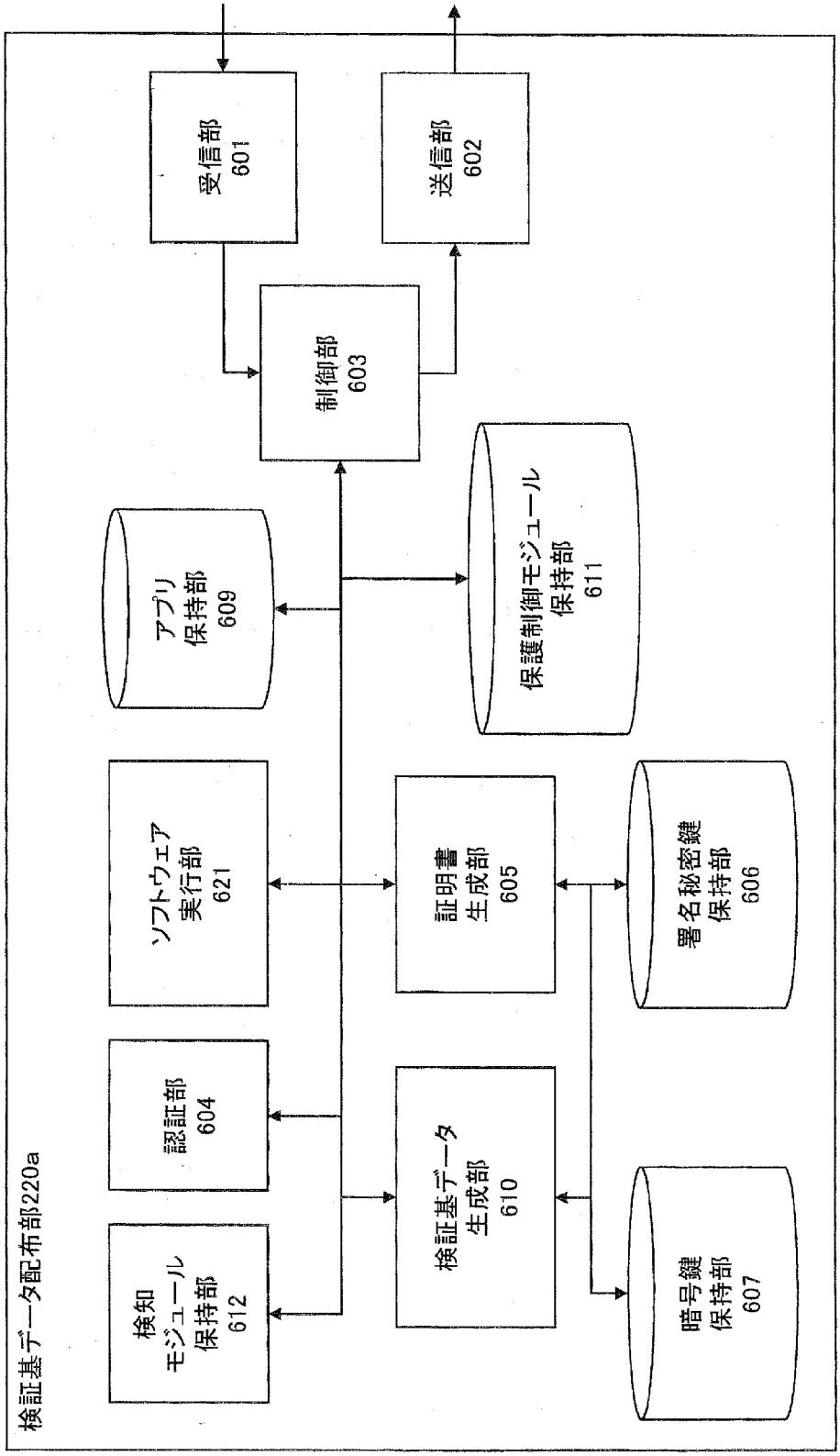
[図30]


検証部404
330b
対応表
選択
Index
検知モジュール識別子
1
131、132、133
2
131、132、134
3
131、132、135
...
...
10
133、134、135

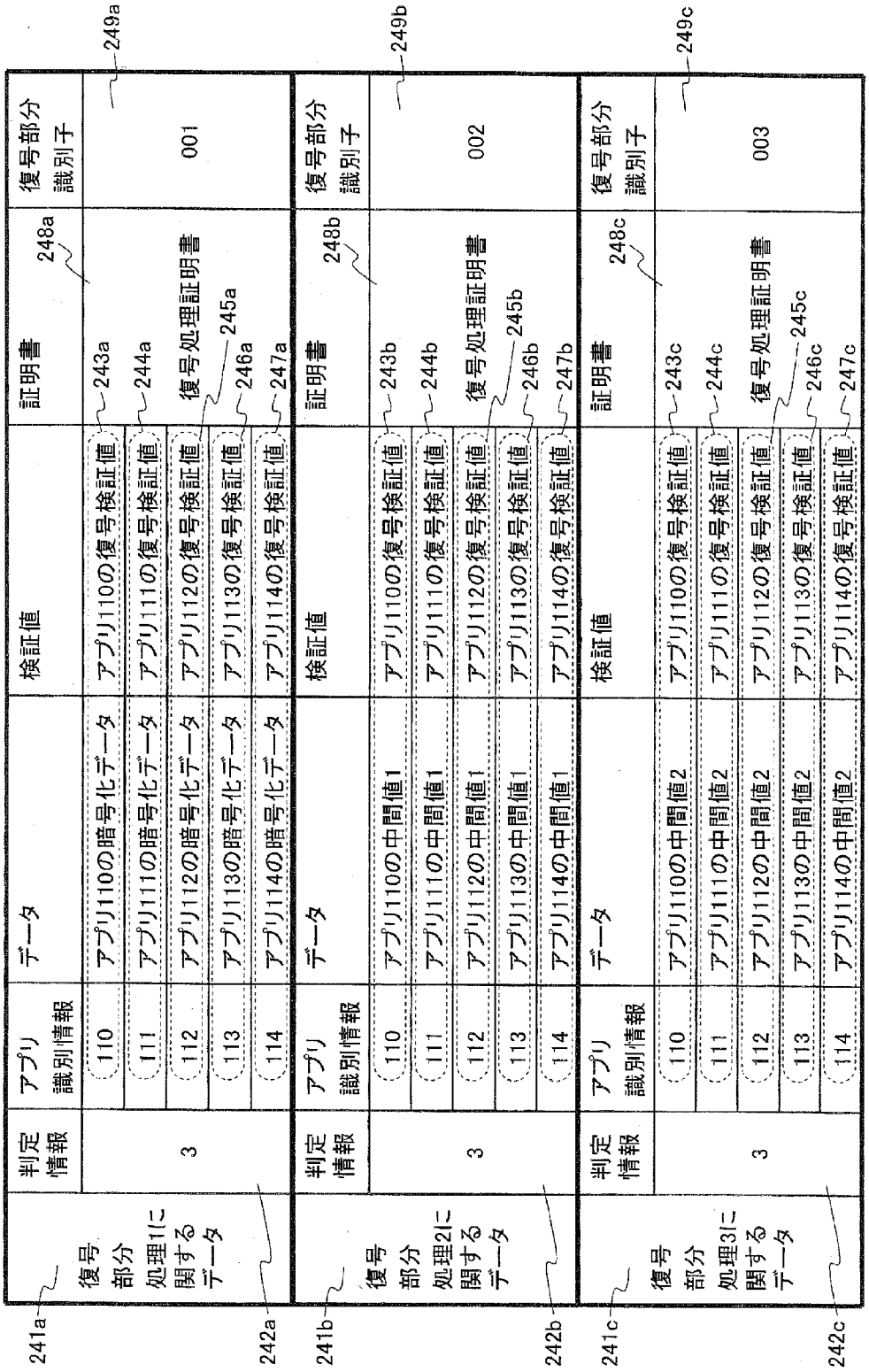
[図31]


350
355
暗号化アプリのデータ
356
アプリ復号の中間値1
357
アプリ復号の中間値2
358
復号したアプリのデータ
復号処理
復号部分処理1
復号部分処理2
復号部分処理3
351
352
353

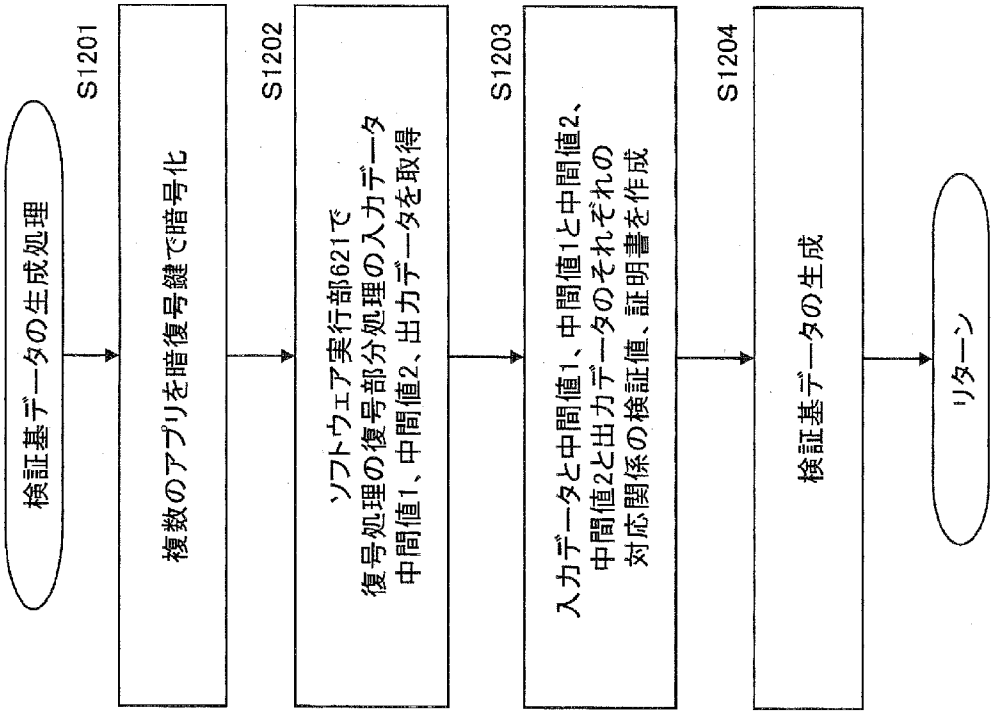
[図32]


検証基データ配布部220a
受信部 601
送信部 602
制御部 603
アプリ 保持部 609
保護制御モジュール 保持部 611
ソフトウェア 実行部 621
証明書 生成部 605
署名秘密鍵 保持部 606
認証部 604
検証基データ 生成部 610
検知 モジュール 保持部 612
暗号鍵 保持部 607

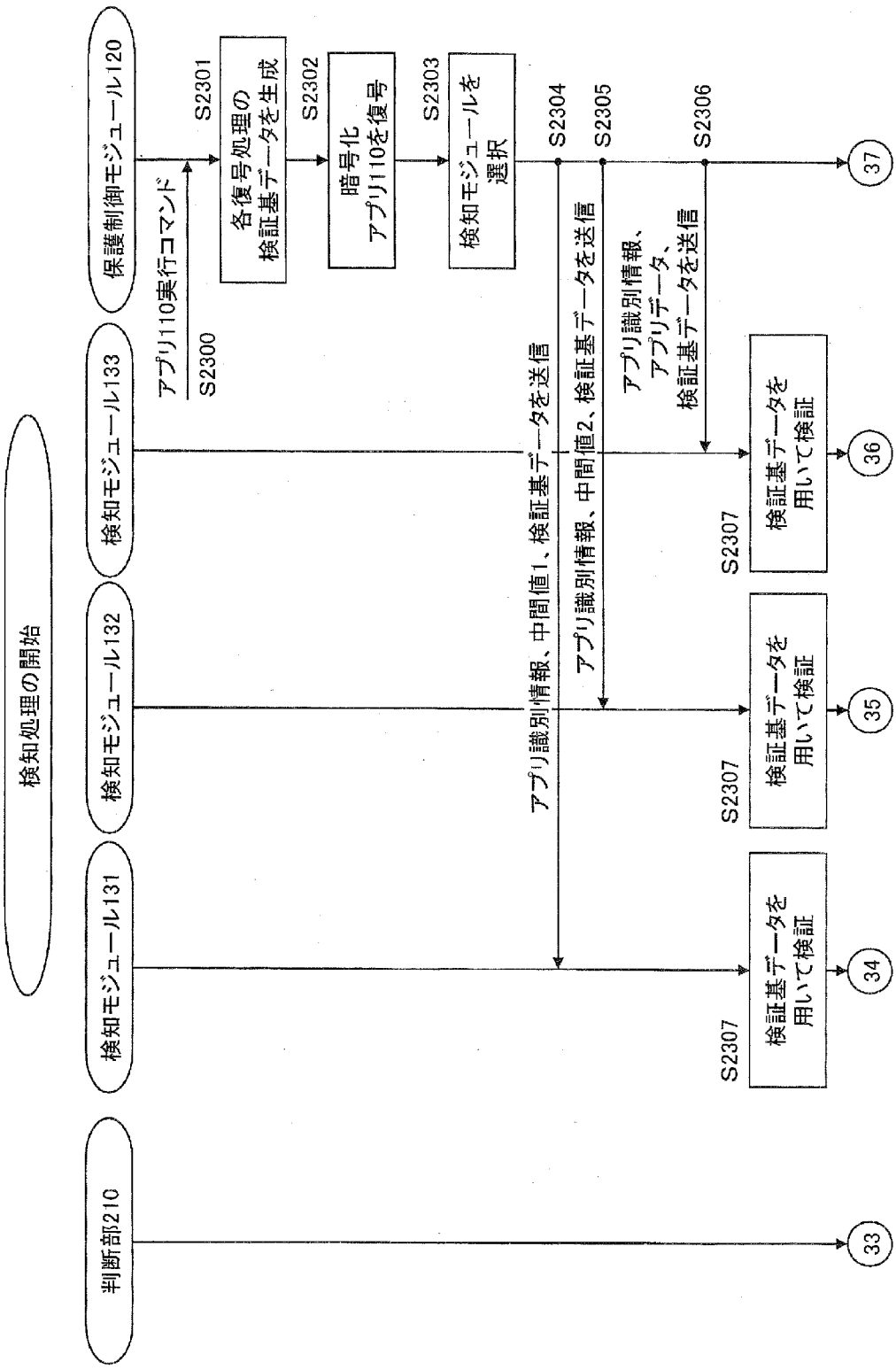
[図33]


240
検証基データ
241a
復号部分処理1に関するデータ
242a
241b
復号部分処理2に関するデータ
242b
241c
復号部分処理3に関するデータ
242c
判定情報
アプリ識別情報
データ
検証値
証明書
248a
復号部分識別子
249a
249b
249c
110
111
112
113
114
3
アプリ110の暗号化データ
アプリ111の暗号化データ
アプリ112の暗号化データ
アプリ113の暗号化データ
アプリ114の暗号化データ
アプリ110の復号検証値
アプリ111の復号検証値
アプリ112の復号検証値
アプリ113の復号検証値
アプリ114の復号検証値
243a
244a
245a
246a
247a
001
248b
243b
244b
245b
246b
247b
002
248c
243c
244c
245c
246c
247c
003
アプリ110の中間値1
アプリ111の中間値1
アプリ112の中間値1
アプリ113の中間値1
アプリ114の中間値1
アプリ110の中間値2
アプリ111の中間値2
アプリ112の中間値2
アプリ113の中間値2
アプリ114の中間値2
復号処理証明書

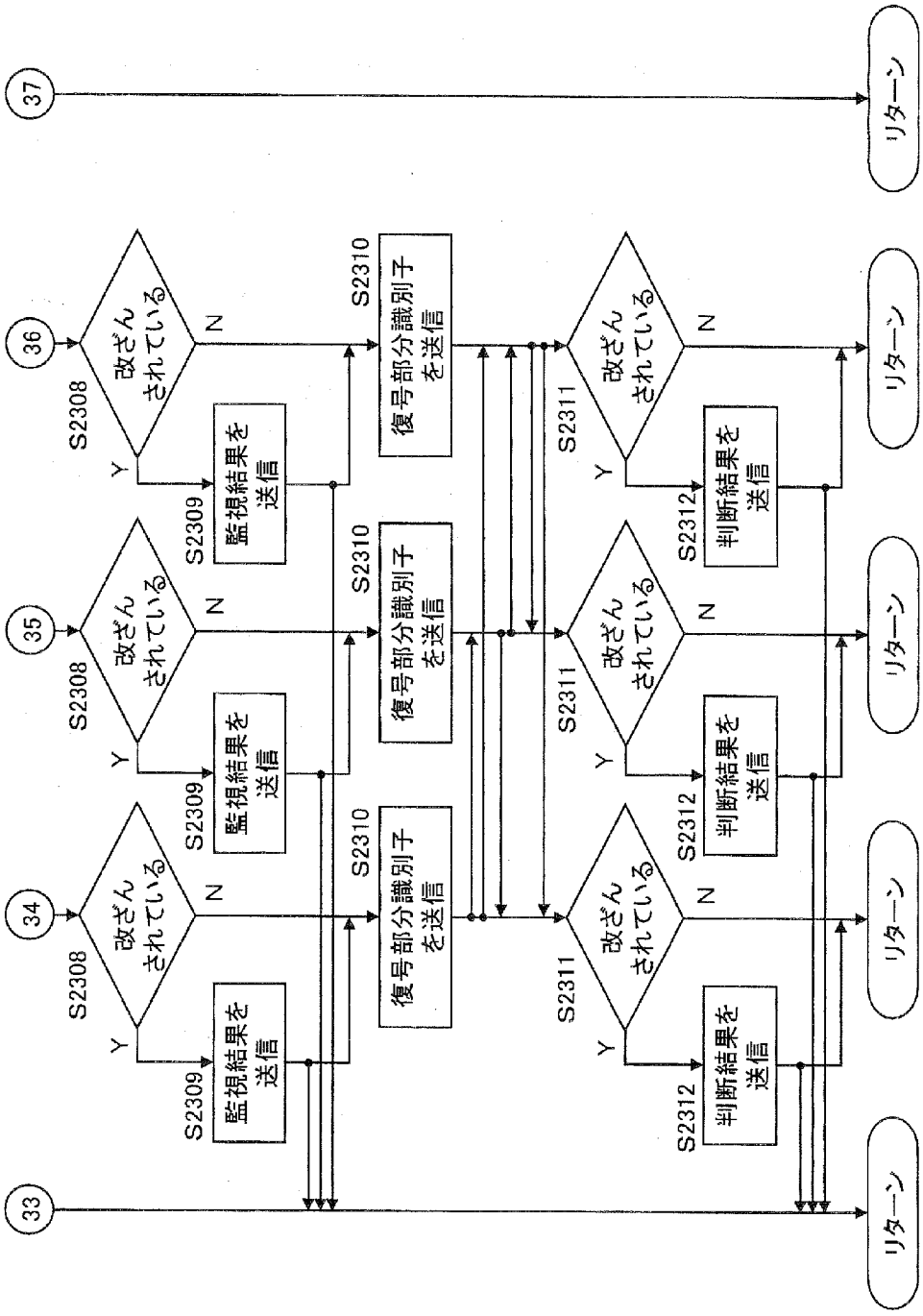
[図34]


検証基データの生成処理
S1201
複数のアプリを暗復号鍵で暗号化
S1202
ソフトウェア実行部621で
復号処理の復号部分処理の入力データ
中間値1、中間値2、出力データを取得
S1203
入力データと中間値1、中間値1と中間値2、
中間値2と出力データのそれぞれの
対応関係の検証値、証明書を作成
S1204
検証基データの生成
リターン

[図35]


検知処理の開始
判断部210
検知モジュール131
検知モジュール132
検知モジュール133
保護制御モジュール120
アプリ110実行コマンド
S2300
S2301
各復号処理の検証基データを生成
S2302
暗号化アプリ110を復号
S2303
検知モジュールを選択
S2304
アプリ識別情報、中間値1、検証基データを送信
S2305
アプリ識別情報、中間値2、検証基データを送信
S2306
アプリ識別情報、アプリデータ、検証基データを送信
S2307
検証基データを用いて検証
33
34
35
36
37

[図36]


37
リターン
36
S2308
改ざんされている
Y
N
S2309
監視結果を送信
S2310
復号部分識別子を送信
S2311
改ざんされている
Y
N
S2312
判断結果を送信
リターン
35
S2308
改ざんされている
Y
N
S2309
監視結果を送信
S2310
復号部分識別子を送信
S2311
改ざんされている
Y
N
S2312
判断結果を送信
リターン
34
S2308
改ざんされている
Y
N
S2309
監視結果を送信
S2310
復号部分識別子を送信
S2311
改ざんされている
Y
N
S2312
判断結果を送信
リターン
33
リターン

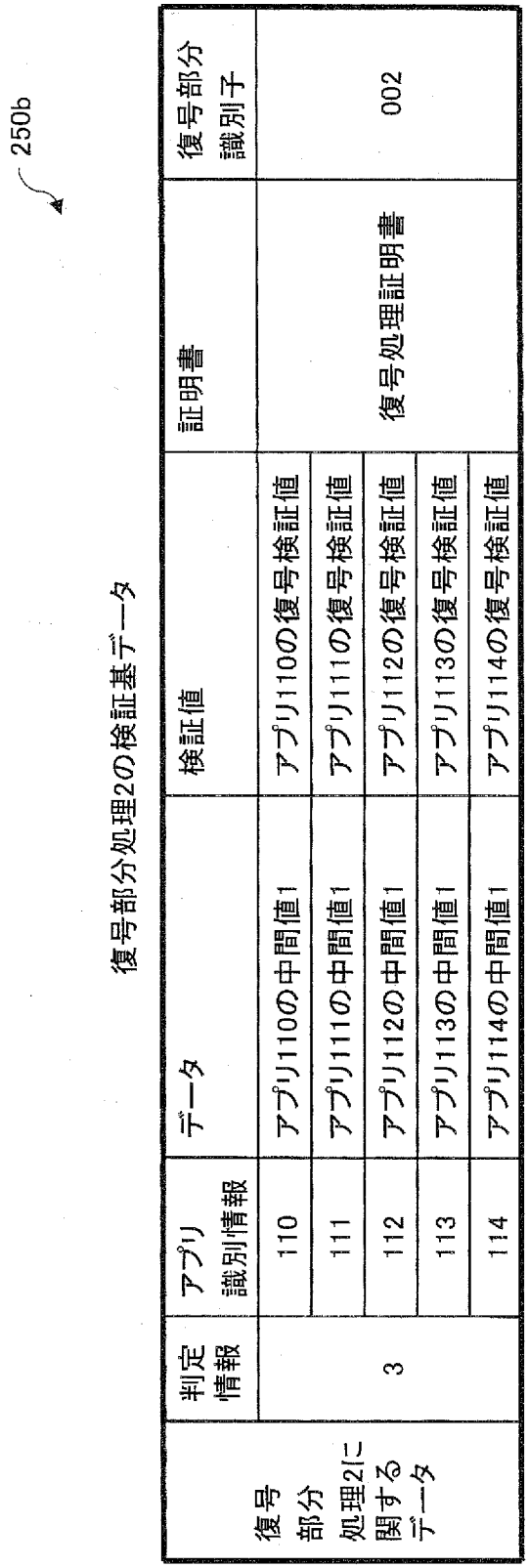
[図37]

250a

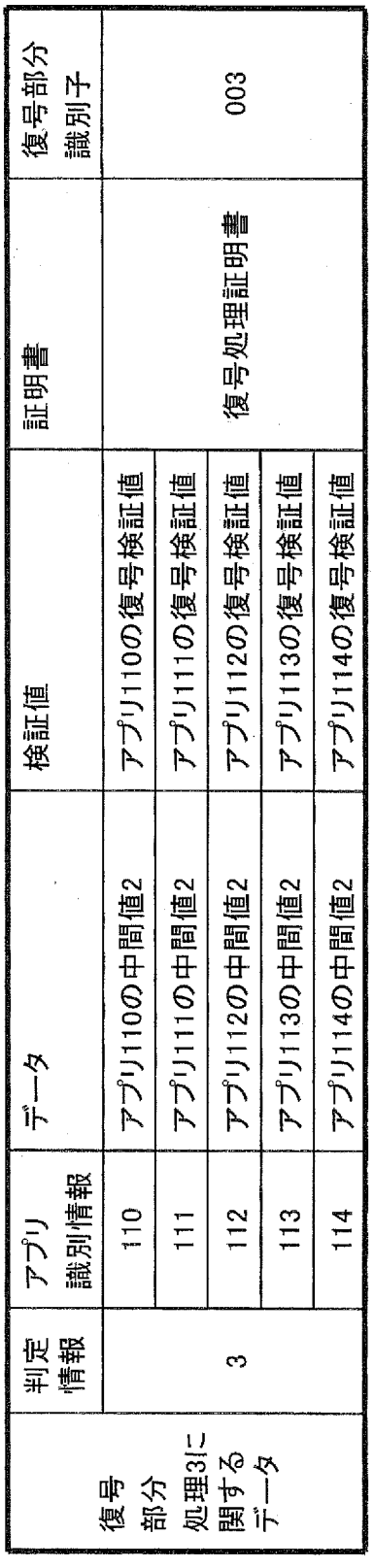
復号部分処理1の検証基データ

	判定情報	アプリ識別情報	データ	検証値	証明書	復号部分識別子
復号部分処理1に関するデータ	3	110	アプリ110の暗号化データ	アプリ110の復号検証値	復号処理証明書	001
		111	アプリ111の暗号化データ	アプリ111の復号検証値		
		112	アプリ112の暗号化データ	アプリ112の復号検証値		
		113	アプリ113の暗号化データ	アプリ113の復号検証値		
		114	アプリ114の暗号化データ	アプリ114の復号検証値		

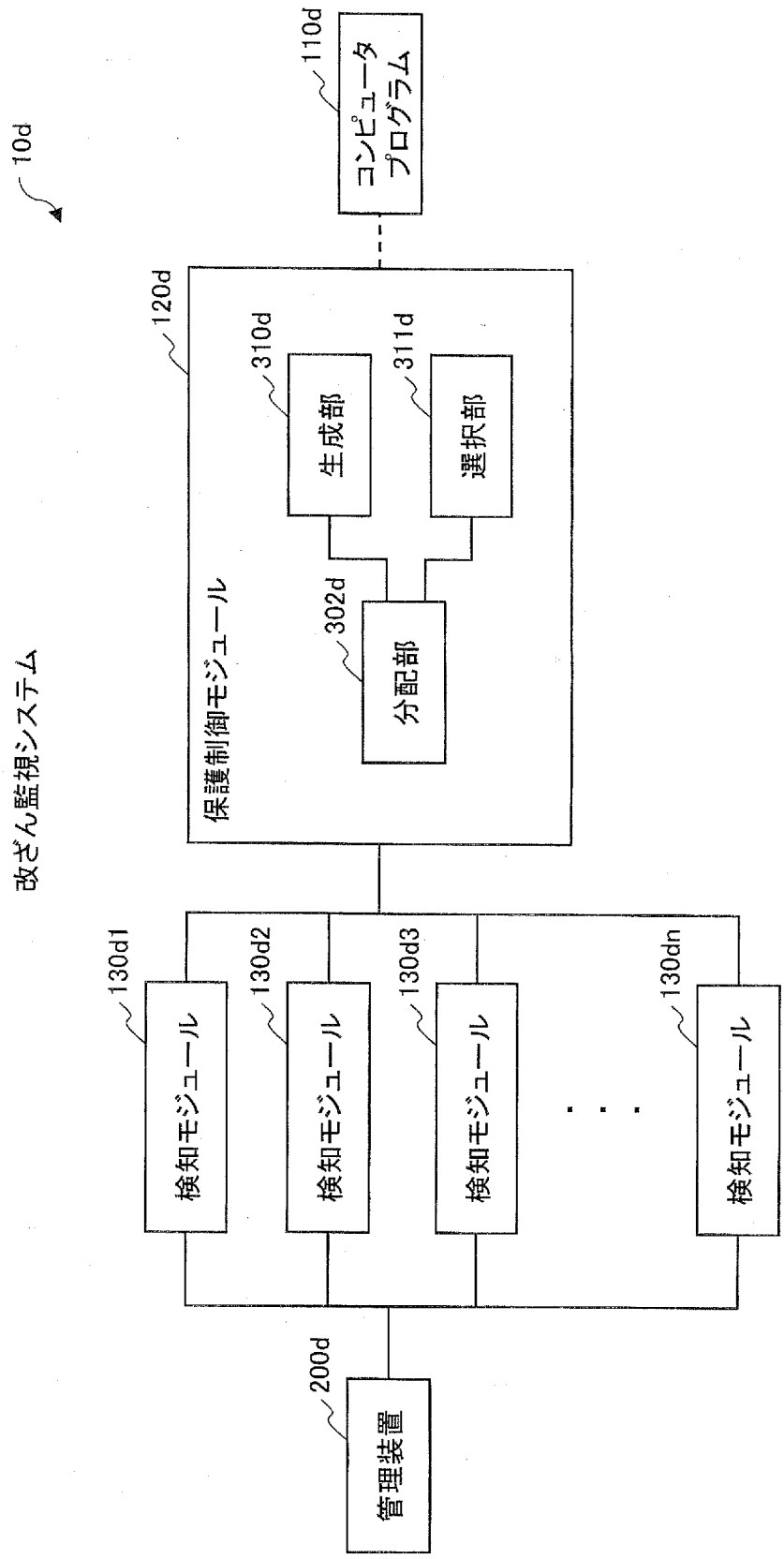
[図38]


250b
復号部分処理2の検証基データ
復号部分処理2に関するデータ
判定情報
3
アプリ識別情報
110
111
112
113
114
データ
アプリ110の中間値1
アプリ111の中間値1
アプリ112の中間値1
アプリ113の中間値1
アプリ114の中間値1
検証値
アプリ110の復号検証値
アプリ111の復号検証値
アプリ112の復号検証値
アプリ113の復号検証値
アプリ114の復号検証値
証明書
復号処理証明書
復号部分識別子
002

[図39]


250c
復号部分処理3の検証基データ
復号部分処理3に関するデータ
判定情報
3
アプリ識別情報
110
111
112
113
114
データ
アプリ110の中間値2
アプリ111の中間値2
アプリ112の中間値2
アプリ113の中間値2
アプリ114の中間値2
検証値
アプリ110の復号検証値
アプリ111の復号検証値
アプリ112の復号検証値
アプリ113の復号検証値
アプリ114の復号検証値
証明書
復号処理証明書
復号部分識別子
003

[図40]


10d
改ざん監視システム
110d
コンピュータプログラム
120d
保護制御御モジュール
310d
生成部
311d
選択部
302d
分配部
130d1
検知モジュール
130d2
検知モジュール
130d3
検知モジュール
130dn
検知モジュール
200d
管理装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/005858

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/22(2006.01)i, *G06F21/24*(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, G06F21/24

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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	WO 2009/118800 A1 (Panasonic Corp.), 01 October 2009 (01.10.2009), entire text; all drawings & US 2010/0180343 A1 & EP 2259205 A1	1-24
A	JP 10-333902 A (NEC Informatec Systems, Ltd.), 18 December 1998 (18.12.1998), entire text; all drawings (Family: none)	1-24
E,A	WO 2011/033773 A1 (Panasonic Corp.), 24 March 2011 (24.03.2011), entire text; all drawings (Family: none)	1-24

☐ 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
05 December, 2011 (05.12.11)	13 December, 2011 (13.12.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／００５８５８

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, G06F21/24(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, G06F21/24

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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	関連する請求項の番号
A	WO 2009/118800 A1 (パナソニック株式会社) 2009.10.01, 全文、全図 & US 2010/0180343 A1 & EP 2259205 A1	1-24
A	JP 10-333902 A (株式会社エヌイーシー情報システムズ) 1998.12.18, 全文、全図 (ファミリーなし)	1-24
EA	WO 2011/033773 A1 (パナソニック株式会社) 2011.03.24, 全文、全図 (ファミリーなし)	1-24

☐　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	国際調査報告の発送日
０５．１２．２０１１	１３．１２．２０１１

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　３９８３
岸野　徹
電話番号　０３－３５８１－１１０１　内線　３５４６