(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年8 月17 日 (17.08.2006)

PCT

(10) 国際公開番号
WO 2006/085647 A1

(51) 国際特許分類:
G06F 12/14 (2006.01) *G06Q 10/00* (2006.01)
G06F 21/22 (2006.01) *G06Q 30/00* (2006.01)
G06F 21/24 (2006.01) *G06Q 50/00* (2006.01)

(21) 国際出願番号: PCT/JP2006/302448

(22) 国際出願日: 2006 年2 月13 日 (13.02.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-036621 2005 年2 月14 日 (14.02.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): ライクセンリング ジェルマーノ (LEICHSENRING, Germano). 金丸 智一 (KANAMARU, Tomokazu).

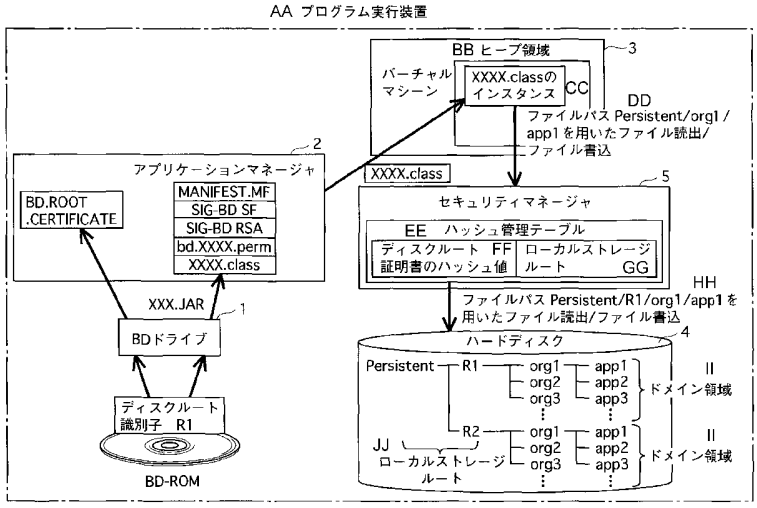
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,

[続葉有]

(54) Title: APPLICATION EXECUTING DEVICE, MANAGING METHOD, AND PROGRAM

(54) 発明の名称: アプリケーション実行装置、管理方法、プログラム



AA PROGRAM EXECUTING DEVICE
3 VIRTUAL MACHINE
BB HEAP AREA
CC INSTANCE OF XXXX.CLASS
DD FILE READ/FILE WRITE USING FILE PATH PERSITENT/ORG1/APP1
2 APPLICATION MANAGER
5 SECURITY MANAGER
EE HASH MANAGEMENT TABLE
FF HASH VALUE OF DISK ROUTE CERTIFICATE
GG LOCAL STORAGE ROUTE
HH FILE READ/FILE WRITE USING FILE PATH PERSITENT/R1/ORG1/APP1
4 HARD DISK
II DOMAIN AREA
1 BD DRIVE
R1 DISK ROUTE IDENTIFIER
JJ LOCAL STORAGE ROUTE

(57) **Abstract:** A disk route certificate (301) is recorded on a BD-ROM. The disk route certificate (301) is a route certificate issued by a route authentication station and allotted to the disk medium. An application manager (2) acquires a hash value from the disk route certificate (301) and judges the authentication of the application on the basis of the hash value. When the application is authenticated, a virtual machine (3) executes the application. A local storage (5) has domain areas. A security manager (4) allots a domain area corresponding to the acquired hash value out of the domain areas present in the local storage (5).

(57) 要約: BD-ROMには、ディスクルート証明書３０１が記録されている。このディスクルート証明書３０１は、ルート認証局から配布されたルート証明書を、当該ディスク媒体に割り当てたものである。アプリケーションマネージャ２は、ディスクルート証明書３０１からハッシュ値を取得し、当該ハッシュ値を用いてアプリケーションの正当性を判定する。正当であると判定した場合、バーチャルマシーン３は、アプリケーションを実行する。またローカルストレージ５は、複数のドメイン領域を有しており、セキュリティマネージャ４は、ローカルストレージ５内に存在する複数のドメイン領域のうち、取得されたハッシュ値に対応する

[続葉有]

WO 2006/085647 A1

RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

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

明 細 書

アプリケーション実行装置、管理方法、プログラム

技術分野

[0001] アプリケーションに対するリソース割当技術の分野に属する発明である。

背景技術

[0002] リソース割当技術とは、プラットフォームが有している記憶装置(ローカルストレージ)内の領域を、リソースとしてアプリケーションに割り当てる技術に属する発明である。世界中の様々な組織から供給される様々なアプリケーションを、体系的に管理するため、欧州向けデジタル放送受信装置であるMHP(Multimedei Home Platform)は、以下のような統一様式のファイルパスで、アクセスできるようにローカルストレージのディレクトリ構造を規定している。

ファイルパス:Root/組織ID/appID

ここで組織IDとは、アプリケーションの供給元となる組織を一意に示す識別子であり、appIDとは、アプリケーションを一意に示す識別子である。

[0003] 以上の領域割当を実現するにあたって、MHPとなる機器は、ルート証明書を用いて、アプリケーションの正当性を判定する。以下、機器(MHP)においてなされていた、アプリケーションの正当性チェックと、アプリケーションに対する領域割り当てについて説明を行う。

アプリケーションを作成した作成者は、アプリケーションを機器に引渡すにあたって、ルート証明書をアプリケーションに付加したうえでアプリケーションを機器に送信する。このルート証明書は、機器固有に割り当てられていたルート証明書と同じものであり、機器は、ルート証明書が付されたアプリケーションを受信して、このアプリケーションに付加されたルート証明書と、機器に割り当てられたルート証明書との同一性を判定する。もし同一性があるなら、そのアプリケーションの供給元の組織に対応する組織用ディレクトリを、当該アプリケーションに割り当てて、そのディレクトリ内のファイルのアクセスを、アプリケーションに行わせる。

[0004] アプリケーションのアクセス権限を適切にコントロールする技術は、非特許文献1に

記載されている。

非特許文献1:「JAVA(登録商標)Security」Scott Oaks著、O'Reilly発行、 May 2001、ISBN 0-596-00157-6

発明の開示

発明が解決しようとする課題

[0005] ところで上述した従来技術では、アプリケーション供給元の組織に対応する領域を設けて、その組織に対応するディレクトリの配下の領域を、アクセスを要求したアプリケーションに割り当てている。そのためアプリケーション実行装置が世界のあらゆる地域に配布され、世界中のあらゆる組織からアプリケーションが供給されるような場合は、世界の様々な組織の組織IDが重複しないような手当が必要になる。何故なら、そうしないと、ある組織に属するアプリケーションが、他の組織のためのディレクトリを自由にアクセスできることになり、アプリケーションが利用するデータの機密性が保てないからである。かかる手当が必要になるので、世界中の各組織に、ユニークな組織IDを割り当てる第3者機関が必要になり、アプリケーション実行装置の標準化に携わるメーカーは、かかる機関の設立・運営に、資本や人材を確保せねばならない。これは、アプリケーション実行装置の標準化に携わるメーカーにとって、多大な負担になる。しかし他の組織が、自組織のためのディレクトリを自由にアクセスするとなると、自組織のアプリケーションのためのデータが、他の組織により、盗用、無断使用され可能性が生じる。装置上において、かかる無法が放置されるとするならば、アプリケーションを作成する作成者は、装置へのアプリケーションの供給を躊躇する事態が多発すると考えられる。これでは、装置で動作するアプリケーションの充実化は望めず、アプリケーションの不足から、アプリケーション実行装置普及の道が閉ざされる恐れがある。

[0006] またMHPでは、装置に割り当てられたルート証明書を、アプリケーションの正当性判定に用いている。装置に割り当てられたるルート証明書が、悪意をもった者により暴露された場合、機器に割り当てられたデジタル証明書は、装置の製造元により新たなものにアップデートされる。かかるデジタル証明書のアップデートがあった場合、古いルート証明書が付加されていたアプリケーションは、正当性が正しく判断されず、ローカルストレージをアクセスすることが許されない。無論、MHPで利用されるアプリケー

ションのように、アプリケーションが、放送時にのみ利用されればよい一過性のものなら、絶えず新しいアプリケーションが送信されるため、そのような扱いで充分であるかもしれない。しかしアプリケーションが、DVD−Videoコンテンツ、BD−ROMコンテンツ等、ディスクに記録された映画作品に関する処理を行う場合、古い映画作品が何度も再生された場合でも、当該映画作品に関する処理を行うアプリケーションは、正しい動作を行うことが求められる。そのためデジタル証明書のアップデートにより、アプリケーションが動作しなくなるというのは、決して望ましくない。つまり従来の技術は、ルート証明書が暴露された場合の、動作保障が不徹底であるという問題がある。

[0007] 本発明の第1の目的は、世界的なレベルで、重複が生じないような組織IDの管理を必要とせずとも、様々な組織から供給されたアプリケーションにて利用されるファイルの機密性を高めることができるアプリケーション実行装置を提供することである。

本発明の第2の目的は、ルート証明書が暴露された場合でも、高いレベルの動作保障を実現しうるアプリケーション実行装置を提供することである。

課題を解決するための手段

[0008] 上記第1、第2の目的を達成するため、本発明にかかるアプリケーション実行装置は、ディスクルート証明書と、アプリケーションとが記録されたディスク媒体からアプリケーションを読み出して、実行するものであり、ディスクルート証明書は、ルート認証局から配布されたルート証明書を、当該ディスク媒体の作成者が当該ディスク媒体に割り当てたものであり、ディスクルート証明書からハッシュ値を取得し、当該ハッシュ値を用いてアプリケーションの正当性を判定する管理手段と、管理手段が正当であると判定した場合、アプリケーションを実行する実行手段と、複数のドメイン領域を有する記憶手段と、記憶手段内に存在する複数のドメイン領域のうち、取得されたハッシュ値に対応するものをアプリケーションに割り当てる割当手段とを備えることを特徴としている。

発明の効果

[0009] 本発明にかかるアプリケーション実行装置は、上述したような技術的事項(1)を有しているので、ローカルストレージの内部には、複数のドメイン領域が存在し、各ドメイン領域がルート証明書ハッシュ値のそれぞれに割り当てられている。そしてこれらのドメ

イン領域の配下に、組織毎、アプリケーション毎の領域を作成すれば、世界的なレベルで、組織IDがユニークでなくてもよい。“ドメイン領域”という閉じた世界において、複数の組織を区別できれば足りるので、組織IDを、世界的なレベルで、ユニークな値にする必要はなく、第3者機関による管理は不要になる。組織IDが重ならないような管理を行わずとも、世界中の組織から供給されるアプリケーションを1つのプラットフォームで動作させつつ、アプリケーションによる読み出し／書き込みの対象となるファイルの機密性を高めることができる。

[0010] 第3者機関による管理を必要とせずとも、アプリケーション提供を作成業者に躊躇させる障壁を取り除き、アプリケーションが利用するファイルの独立性・機密性を高めることができるので、アプリケーション実行装置用アプリケーションの提供を、映画作成者、映画配給者、放送局、出版者、ソフトハウスなど、世界中の多くの組織に、呼び掛けることができる。こうすることで、アプリケーションの豊富化を図ることができるため、装置用アプリケーションを充実させることができ、ディスク媒体再生装置としてのアプリケーション実行装置の普及に一層の弾みを付けることができる。

[0011] またルート証明書は、装置本体ではなく、記憶手段内のドメイン領域に割り当てられることになる。あるディスク媒体にて供給されるアプリケーションは、そのディスク媒体のディスクルート証明書に対応付けられていれば、そのディスク媒体がアプリケーション実行装置に装填される限りは、必ず動作することが保障される。もっとも、ディスクルート証明書が暴露される可能性がない訳ではないが、そうした場合、そのディスク媒体を使えないようにするか、また、そのディスク媒体についてのディスクルート証明書のみをアップデートすればよく、他のディスクにて供給されたアプリケーションは、従前通り、ディスクルート証明書を用いればよいので、確実な動作保障を実現することができる。

[0012] このように世界的なレベルでの組織IDの管理を必要とせず、また、従前のアプリケーションの同士保障を高いレベルに維持することができるので、本発明にかかるアプリケーション実行装置は、映画作品に関する処理を行うアプリケーションを実行するアプリケーション実行装置の世界的な標準化に大きく寄与することができる。

また、任意的であるが、上述したアプリケーション実行装置の技術的事項(1)に、以

下の技術的事項(2)(3)～を加え、アプリケーション実行装置を具体的な構成にすることにより、更なる効果をもたらすことができる。本願では、これらの技術的事項を、請求項1以下の従属形式の請求項に区分けして記載している。

・技術的事項(2) ディスク媒体には、第1デジタル証明書チェーンが記録されており、

前記管理手段による正当性判定は、

前記第1デジタル証明書チェーン中のルート証明書から取得されるハッシュ値と、前記ディスクルート証明書から取得されるハッシュ値とが一致するか否かのチェックを含み、

前記ドメイン領域は、複数の組織領域を含み、

前記割当手段による割り当ては、

ハッシュ値が一致している場合、アプリケーションに割り当てられたドメイン領域中の複数の組織領域のうち、第1デジタル証明書チェーン中のリーフ証明書に記載されている組織IDに対応するものの利用を、アプリケーションに許可することを含む。

アプリケーション実行装置に上述したような技術的事項が付加されれば、従来の認証局を利用したビジネスモデルを利用しながら第1アプリケーションが第2アプリケーションに割り当てられるリソースを不正に利用できないようにすることができる。かかる不正利用の防止は、複数の組織が同じディスクルート証明書を共用することでなされ、アプリケーション実行装置内にルート証明書を保持することはないので、アプリケーション実行装置における証明書をアップデートした場合の動作互換を維持することができる。

・技術的事項(3) 前記アプリケーションの供給元となる組織は、別の組織から領域利用の権限の提供を受けており、

前記ディスク媒体には更に、

領域利用権限の提供者となる組織を示す提供者組織ID、及び、領域利用権限の受領者となる組織を示す受領者組織IDを含むクレデンシャル情報が記録されており、

前記管理手段は更に、前記クレデンシャル情報の正当性の確認を行い、

前記割当手段による割り当ては、

前記クレデンシャル情報の正当性が確認された場合、アプリケーションに割り当てられたドメイン領域中の複数の組織領域のうち、提供者組織IDに対応するものの利用を、アプリケーションに許可することを含む。

・技術的事項(4)　前記クレデンシャル情報は、

提供者組織に固有なルート証明書から取得されるハッシュ値と、受領者組織に固有なルート証明書から取得されるハッシュ値とを含み、

前記管理手段によるクレデンシャル情報の正当性判定は、

ディスクルート証明書から取得されるハッシュ値が、受領者組織に固有なルート証明書から取得されるハッシュ値と一致するか否かのチェックと、

前記第1デジタル証明書チェーン中のリーフ証明書に記載されている組織IDと、クレデンシャル情報に示される受領者組織IDとが一致しているか否かのチェックとを含む。

アプリケーション実行装置に上述したような技術的事項が付加されれば、アプリケーション実行装置に対して、様々なディスク媒体の装填、排出が繰り返され、それら複数のディスク媒体に、別々のディスクルート証明書が割り当てられている場合において、個々のアプリケーションに対応するディスクルート証明書が違う場合でも、あるディスク媒体に記録される第1アプリケーションが、別のディスク媒体に記録される第2アプリケーションに割り当てられたドメイン領域をアクセスすることができる。このように、アプリケーションが別々のディスク媒体に記録されていて、割り当てられているディスクルート証明書が異なる場合でも、アプリケーションは、複数のドメイン領域を共有することができる。これにより作成者相互間の連帯、協調性を高めることができる。

・技術的事項(5)　ディスク媒体には、第2デジタル証明書チェーンが記録されており、

前記管理手段によるクレデンシャル情報の正当性判定は更に、

前記第2のデジタル証明書チェーンの中のルート証明書からハッシュ値を取得して、そのハッシュ値が前記提供者組織に固有なルート証明書から取得されるハッシュ値と一致するか否かのチェックと、

前記第2のデジタル証明書チェーンの中のリーフ証明書に記載されている組織IDが提供者組織IDと一致するか否かのチェックとを含む。

アプリケーション実行装置に上述したような技術的事項が付加されれば、クレデンシャル情報の改ざんを防止できると共に、クレデンシャル情報が無いと、他のアプリケーションのためのドメイン領域へとアクセスを行うことができなくなるので、不正なアクセスを防止できる。

。

[0013] ・技術的事項(6) 前記クレデンシャル情報は更にファイルリストを含み、

前記割当手段による組織領域の利用許可は、

組織領域配下に存在するファイルのうち、ファイルリストに示されるものを、前記アプリケーションにアクセスさせることを含む。

アプリケーション実行装置に上述したような技術的事項が付加されれば、クレデンシャル情報によるアクセス提供を細かい粒度で行うことが可能になり、アプリケーションの不具合によるデータの破壊リスクを抑制することができる。

[0014]

・技術的事項(7) 前記クレデンシャル情報は更に、ファイルのアクセス方法を示すアクセス情報を有し、

前記割当手段による組織領域の利用許可は、

組織領域配下に存在するファイルのうち、ファイルリストに示されるものを、アクセス情報に示されるアクセス方法で、前記アプリケーションにアクセスさせることを含む。

[0015] アプリケーション実行装置に上述したような技術的事項が付加されれば、クレデンシャル情報を用いたアプリケーションによるアクセスがある場合でもアプリケーションの不具合によるデータの破壊リスクを抑制することができる。

・技術的事項(8) ディスク媒体には、第1デジタル証明書チェーンが記録されており

、

前記管理手段による正当性判定は、

前記第1デジタル証明書チェーン内のルート証明書から取得されるハッシュ値と、前記ディスクルート証明書から取得されるハッシュ値とが一致するか否かのチェックを

含み、

、 前記実行手段によるアプリケーションの実行は、ハッシュ値が一致している場合になされる。

[0016] アプリケーション実行装置に上述したような技術的事項が付加されれば、アプリ間通信(Interprocess Communication、IPC)を悪用した攻撃を防止することができ、セキュリティを向上させることができる。

図面の簡単な説明

[0017] [図1](a)BD-ROMにおけるファイル・ディレクトリ構成を示す図である。 (b)Java(TM)アーカイブファイル302の中の構造の一例を示す図である。

[図2](a)Credentialのデータ構造の一例を示図である。

[0018] (b)Credentialの具体的な一例を示す図である。

[図3](a)BD-ROMにおいてルート証明書がどのように割り当てられるかを模式的に示す図である。 (b)MHPにおいてルート証明書がどのように割り当てられるかを模式的に示す図である。

[図4]権限の提供がない場合のSIG-BD.RSA、SIG-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MFの相互関係を示す図である。

[図5]権限の提供がある場合のSIG-BD.RSA、SIG-BD.SF、BD.ROOT.CERTIFICATE、MANIFEST.MF、bd.XXXX.permの相互関係を示す図である。

[図6]本実施の形態におけるアプリケーション実行装置の機能構成を示すブロック図である。

[図7]アプリケーションマネージャ2による、Java(TM)アーカイブファイル302内のクラスファイルに基づくアプリケーションの起動手順を示すフローチャートである。

[図8]アプリケーションマネージャ2による、Credentialの署名検証の手順を示すフローチャートである。

[図9]アプリケーションマネージャ2が保持する管理情報の一例を示す図である。

[図10]アプリケーションマネージャ2が保持する管理情報の一例を示す図である。

[図11]Java(TM)アプリケーションがハードディスク4を利用するにあたっての処理手順を示すフローチャートである。

[図12]セキュリティマネージャ5によるローカルストレージ名の取得手順の詳細を示すフローチャートである。

[図13]セキュリティマネージャ5が保持するハッシュ管理テーブルの一例を示す図である。

[図14]セキュリティマネージャ5による組織IDの取得関数の詳細を示すフローチャートである。

[図15]セキュリティマネージャ5によるファイル読出関数の詳細を示すフローチャートである。

[図16]セキュリティマネージャ5によるファイル読出関数の詳細を示すフローチャートである。

[図17]セキュリティマネージャ5によるファイル書込関数の詳細を示すフローチャートである。

[図18]セキュリティマネージャ5によるファイル書込関数の詳細を示すフローチャートである。

符号の説明

[0019]

1 BDドライブ

2 アプリケーションマネージャ

3 バーチャルマシーン

4 ハードディスク

5 セキュリティマネージャ

301 ディスクルート証明書

302 Java(TM)アーカイブファイル

401 クラスファイル

402 マニフェストファイル

403 シグネチャファイル

404 デジタルシグネチャファイル

405 パーミッションリクエストファイル

501 提供者ルート証明書のハッシュ値

502 提供者組織ID

503 受領者ルート証明書のハッシュ値

504 受領者組織ID

505 受領者アプリID

506 ファイルリスト

発明を実施するための最良の形態

[0020] 以下、本発明の実施の形態を、図面を参照しながら説明する。

(第1実施形態)

以降、本発明に係るアプリケーション実行装置の実施形態について説明する。まず始めに、アプリケーション実行装置に対して、アプリケーションを供給する記録媒体について説明する。かかる記録媒体として、本実施形態では、BD-ROMを題材に選ぶ。何故なら、BD-ROMにおけるアプリケーションは、上述したような映画作品に関する処理を行うからである。図1(a)は、BD-ROMにおけるファイル・ディレクトリ構成を示す図である。本図の第1段目にBD-ROMを示す。BD-ROMは、他の光ディスク、例えばDVDやCDなどと同様にその内周から外周に向けてらせん状に記録領域を持つ。第2段目は、この記録領域を示している。第2段目に示すように、記録領域は、内周の「リードイン領域」と、外周の「リードアウト領域」の間に論理データを記録できる「論理アドレス空間」を有している。また、リードインの内側にはBCA(Burst Cutting Area)と呼ばれるドライブでしか読み出せない特別な領域がある。この領域はアプリケーションから読み出せないため、例えば著作権保護技術などに利用されることがよくある。

[0021] 「論理アドレス空間」には、ファイルシステム情報(ボリューム)を先頭に映像データ、クラスファイルとその関連情報の入ったJava(TM)アーカイブファイル302などのデータが記録されている。ファイルシステムとは、UDF(Universal Disk Format)やISO9660などのことであり、通常のパーソナルコンピュータと同じように記録されている論理データをディレクトリ、ファイル構造を使って読み出しする事が可能になっている。第3段目は、BD-ROMのディレクトリ・ファイル構造を示す。このディレクトリ・ファイル構造は、ルートディレクトリ(ROOT)直下、BDDATAディレクトリが置かれるというものである。ディレクトリBDDATAには、次の2種類のファイルが記録されている。

[0022] (A)BD.ROOT.CERTIFICATE:ディスクルート証明書301

ディスクルート証明書301とは、このBD-ROMを作成した作成者が、ルート認証局から配布を受けたルート証明書を、BD-ROMに割り当てたものである。ディスクルート証明書301はたとえばX.509の形式で符号されている。X.509の仕様は国際電信電話諮問委員会より発行されており、CCITT Recommendation X.509 (1988), "The Directory - Authentication Framework"に記載されている。かかるルート証明書を、可搬型の記録媒体に記録することは、ルート証明書が暴露される可能性が高く、DVDでは、かかる割り当ては、ルート証明書の暴露の危険性があるとして、導入されていなかった。しかしBD-ROMには、DVDよりかなり高度な著作権保護技術が採用されており、かかる著作権保護技術の採用は、"BD-ROMに固有のルート証明書を割り当てる"との考えの導入の追い風になった。BD-ROMにおけるディスクルート証明書301の導入には、以上のような背景があることに留意されたい。

(B)XXX.JAR:Java(TM)アーカイブファイル302

これは、http://java(TM).sun.com/j2se/1.4.2/docs/guide/jar/jar.htmlに記載された仕様に準じた、Java(TM)アーカイブファイル302である。Java(TM)アーカイブファイル302は、ZIPファイルの形式を、Java(TM)に特化したものであり、市販されているZIP展開ソフトウェアにより中身を確認することができる。ここで「XXX」は可変、拡張子「JAR」は固定である。

[0023] Java(TM)アーカイブファイル302は複数のファイルをディレクトリ構造の形で格納している。図1(b)はJava(TM)アーカイブファイル302の中の構造の一例を示す図である。

この構造は、ルートディレクトリ直下にXXXX.classが存在し、META-INFディレクトリにファイルMANIFEST.MF、ファイルSIG-BD.SF、ファイルSIG-BD.RSA、ファイルbd.XXXX.permが存在するというものである。以下、これらのファイルについて個別に説明してゆく。

(i)XXXX.class:クラスファイル401

クラスファイル401は、バーチャルマシーン上で実行することができるJava(TM)アプリケーションを定義するような構造体を格納したクラスファイル401である。

[0024] このクラスファイル401にて定義されるJava(TM)アプリケーションは、Xletインターフェイスを通じて、アプリケーション実行装置のアプリケーションマネージャにより、制御されるJava(TM) Xletである。Xletインターフェイスは、“loaded”,“paused”、“active”,“destoryed”といった4つの状態をもつ。

(ii)MANIFEST.MF:マニフェストファイル402

マニフェストファイル402は、デジタル証明書に対応するものであり、Java(TM)アーカイブファイル302の属性、Java(TM)アーカイブファイル302内のクラスファイル401やデータファイルのハッシュ値が記載されているファイルである。Java(TM)アーカイブファイル302の属性には、クラスファイル401のインスタンスである、Java(TM)アプリケーションに付与されるアプリID、Java(TM)アーカイブファイル302を実行するために最初に実行すべきクラスファイル401名がある。上記の二つのJava(TM)アーカイブファイル302の属性が存在しない場合、Java(TM)アーカイブファイル302中のクラスファイル401のインスタンスであるJava(TM)アプリケーションを実行しない。

(iii)SIG-BD.SF:シグネチャファイル403、

シグネチャファイル403は、マニフェストファイル402のハッシュ値が記載されているファイルである。

(iv)SIG-BD.RSA:デジタルシグネチャファイル404、

デジタルシグネチャファイル404は、「デジタル証明書チェーン」、シグネチャファイル403の「署名情報」が記載されているファイルである。

[0025] シグネチャファイル403に対する「署名情報」は、署名処理をシグネチャファイル403に施すことで得られる。これらの署名処理には、デジタルシグネチャファイル404内のデジタル証明書チェーンにおける公開鍵に対応する秘密鍵が用いられる。

「デジタル証明書チェーン」とは、一つ目の証明書(ルート証明書)が二つ目の証明書を署名し、また同じようにn番目の証明書がn+1番目の証明書を署名している形をもつ複数の証明書群である。デジタル証明書チェーンの最後の証明書を「リーフ証明書」と呼ぶ。この構成を利用することにより、ルート証明書から順番に次の証明書を保障していくことにより、デジタル証明書チェーンの最後の証明書までを保障することができる。

[0026] 「ルート証明書」は、BD.ROOT.CERTIFICATEファイルに存在するディスクルート証明書301と同じ証明書を格納している。

「リーフ証明書」には、組織IDが記載されている。シグネチャファイル403は、PKCS#7という形式により格納されている。PKCS#7は署名および一つ以上のデジタル証明書を格納するためのファイル形式であり、IETF(Internet Engineering Task Force)より発行されたRFC2315に記載されている。RFC2315はhttp://www.ietf.org/rfc/rfc2315.txtより参照できる。

[0027] 通常、このデジタル証明書チェーンは、1つであるが、後述する権限の提供がある場合、このデジタル証明書チェーンは2つの作られる。これら2つのデジタル証明書チェーンを、第1デジタル証明書チェーン、第2デジタル証明書チェーンと呼ぶ。第1デジタル証明書チェーンのルート証明書は、権限提供を受ける側の組織のディスクルート証明書を示し、リーフ証明書は、権限提供を受ける側の組織の組織IDを示す。第2デジタル証明書チェーンのルート証明書は、権限を提供する側の組織のディスクルート証明書を示し、リーフ証明書は、権限を提供する側の組織の組織IDを示す。一方、権限の提供がない場合、デジタル証明書チェーンは、1つ(第1デジタル証明書チェーン)のみになる。

[0028] マニフェストファイル402、シグネチャファイル403、デジタルシグネチャファイル404の詳細はJava(TM)アーカイブファイルの仕様に記載されている。マニフェストファイル402、シグネチャファイル403、デジタルシグネチャファイル404は署名処理および署名検証処理を行うために利用される。最終的にJava(TM)アーカイブファイル302中のクラスファイル401のインスタンスであるJava(TM)アプリケーションやパーミッションリクエストファイル405をデジタル証明書により署名することが可能になる。以降マニフェストファイル402、シグネチャファイル403、デジタルシグネチャファイル404をまとめて「デジタル証明書による署名」と称する。

[0029] (v)bd.XXXX.perm:パーミッションリクエストファイル405

パーミッションリクエストファイル405は、実行されるJava(TM)アプリケーションにどのパーミッションを与えるのかの情報を格納するファイルである。具体的に以下の情報を格納する。

(ア)Credential(デジタル信用証明書)

(イ)アプリ間通信の許可情報

以降、(ア)Credentialについて説明する。"Credential"とは、ある組織に帰属する組織ディレクトリ内のファイルを共有化するための情報である。この共有化は、ある組織に属するアプリケーション用ファイルを利用する権限を、他の組織に属するアプリケーションに提供することでなされる。そのためCredentialは、権限を提供する側の組織を示す提供者組織ID、権限を受領する側の組織の識別を示す受領者組織IDを含む。

[0030] 図2(a)は、Credentialのデータ構造の一例を示す。Credentialには、ルート認証局から提供者組織に配布されたルート証明書のハッシュ値501、提供者組織に割り当てられた提供者組織ID502、ルート認証局から受領者に配布された受領者ルート証明書のハッシュ値503、受領者組織に割り当てられた受領者組織ID504、受領者アプリID505、提供ファイルリスト506からなる。提供ファイルリスト506には、一つ以上の提供ファイル名507とアクセス方法508(読み取り可・書き込み可)の情報が格納されている。Credentialが有効であるためには署名されなければならない。Credentialの署名にはデジタルシグネチャファイル404と同様にPKCS#7の方式を利用できる。

[0031] 図2(b)は、Credentialの具体的な一例を示す図である。本図におけるCredentialは、ファイル「4/5/scores.txt」に対して読み取り許可、ファイル「4/5/etc/settings.txt」に対して読み書き許可をCredentialにより与えていることになる。

続いて(イ)アプリ間通信の許可情報について説明する。一つのJava(TM)アーカイブファイル302に含まれるJava(TM)アプリケーションは通常、他のJava(TM)アーカイブファイル302に含まれるJava(TM)アプリケーションとの通信(アプリ間通信)が許可されない。パーミッションリクエストファイル405にアプリ間通信の許可が与えられている場合だけアプリ間通信が可能である。

[0032] 以上が、パーミッションリクエストファイル405についての説明である。続いて、ルート証明書についてのより詳しく説明する。

図3(a)は、BD-ROMにおいてルート証明書がどのように割り当てられるかを模式的に示す図である。本図の第3段目は、機器(アプリケーション実行装置)と、この機器

に装填されるBD-ROMを示し、第2段目は、これら機器及びBD-ROMを作成する業者(BD-ROMの作成者、機器の製造業者)を示す。第1段目は、ルート証明書を管理するルート認証局を示す。

[0033] 本図において、BD-ROMの作成者は、ルート認証局からルート証明書の配布を受け(f1)、配布されたルート証明書を、ディスクルート証明書301としてBD-ROMに割り当てた上で、このルート証明書をBD.ROOT.CERTIFICATEに格納して、BD-ROMに書き込む(w1)。一方、Java(TM)アーカイブファイル302を作成するにあたって、このルート証明書と、組織IDを示すリーフ証明書とをSIG-BD.SFに収録して、Java(TM)アーカイブファイル302に包含させる。

[0034] 本発明の実施形態の説明ではないが、対比のため、MHPにおけるルート証明書の割り当てについて説明する。

図3(b)は、MHPにおいてルート証明書がどのように割り当てられるかを示す図である。MHPでは、機器を製造する製造業者が、ルート認証局からルート証明書の配布を受け(f2)、当該製造業者は、このルート証明書を機器に割り当てる(w2)。一方放送コンテンツの作成業者は、このルート証明書と、自身の組織IDを示すリーフ証明書とを、アプリケーションを定義するクラスファイルに添付した上で、機器に送り込む。これらの図を比較すると、MHPでは機器に割り当てられていたルート証明書を、BD-ROMに割り当てており、このBD-ROMに割り当てたルート証明書から、証明書チェーンを形成していることがわかる。

[0035] BD-ROMではなく、Java(TM)アーカイブファイル302が、WWWサーバからダウンロードされて、アプリケーション実行装置内の記憶装置に書き込まれる場合も同様である。かかるダウンロードは、BD-ROMに記録されたコンテンツのアップデートを目的とするものだが、かかるダウンロードにおいて、BD.ROOT.CERTIFICATEに収録され、ディスクルート証明書301として書き込まれているルート証明書と同一性をもつルート証明書を、SIG-BD.SFに格納してJava(TM)アーカイブファイルに包含させる。こうすることで、BD-ROMに記録されたコンテンツのアップデートを目的とするJava(TM)アーカイブファイル302を、ダウンロードにてアプリケーション実行装置に供給する場合も、BD-ROMに割り当てたディスクルート証明書301を用いることにより、Java(TM)アーカイ

ブファイル302の正当性をアプリケーション実行装置に確認させることができる。

[0036] 図4は、権限の提供がない場合のSIG-BD.SF、BD.ROOT.CERTIFICATEの相互関係を示す図である。本図における矢印d1は、これらのファイルの内部構成の情報要素のうち、同一性があるものを示している。権限の提供がない場合、BD.ROOT.CERTIFICATE内のルート証明書(ディスクルート証明書301)は、SIG-BD.RSAにおける第1のデジタル証明書チェーン内のルート証明書と同一性を有したものになる。

[0037] MANIFEST.MFは、クラスファイルXXXX.classを署名し、SIG-BD.SFは、MANIFEST.MFから算出されたハッシュ値を含み、SIG-BD.RSAは、SIG-BD.SFから算出されたハッシュ値を含んでいるので(矢印h1)、これらの署名が正しいかどうかを確認し、これらの図に示す同一性を判定することで、アプリケーション実行装置は、Java(TM)アーカイブファイル302が正当なものか、改竄が加えられたものかを判断することができる。また権限の提供がないとの想定なので、本図では、bd.XXXX.permを示していない。

[0038] 図5は、権限の提供がある場合のSIG-BD.RSA、SIG-BD.SF、BD.ROOT.CERTIFICATE、bd.XXXX.permの相互関係を示す図である。本図における矢印d1～d6は、これらのファイルの内部構成の情報要素のうち、同一性があるものを示している。権限の提供権限の提供があった場合も、BD.ROOT.CERTIFICATE内のルート証明書(ディスクルート証明書)は、SIG-BD.RSAにおける第1のデジタル証明書チェーン内のルート証明書と同一性を有したものになる(矢印d1)。一方、権限の提供があると、BD.ROOT.CERTIFICATE内のディスクルート証明書301は、受領者のものになるので、bd.XXXX.permにおけるCredentialの、受領者ルート証明書が、BD.ROOT.CERTIFICATE内のルート証明書と同一性をもつ(矢印d2)。また、Credentialにおける受領者組織IDは、第1のデジタル証明書チェーンにおけるリーフの組織IDと同一性をもつ(矢印d3)。

[0039] bd.XXXX.permにおけるCredentialの、提供者組織のルート証明書は、SIG-BD.RSA内の第2のデジタル証明書チェーンにおけるルート証明書と同一性をもつ(矢印d4)。また、Credentialにおける提供者組織IDは、SIG-BD.RSAの第2のデジタル証明書チェーンにおけるリーフの組織IDと同一性をもつ(矢印d5)。Credentialにおける受領

者アプリIDは、bd.XXXX.permにおいてCredential以外の部分に存在するアプリIDと同一性をもつ(矢印d6)。

[0040] MANIFEST.MFは、クラスファイルXXXX.classから算出したハッシュ値を含み、SIG-BD.SFは、MANIFEST.Mから算出したハッシュ値を含み、SIG-BD.RSAは、SIG-BD.SFから取得したハッシュ値を含むので(矢印h1)、これらの署名が正しいかどうかを確認し、これらの図に示す同一性を判定することで、アプリケーション実行装置は、Java(TM)アーカイブファイル302が正当なものか、改竄が加えられたものかを判断することができる。あらかじめ断っておくが、本実施形態では、ルート証明書の同一性を、それぞれのルート証明書について算出されたハッシュ値を比較し、これらのハッシュ値が一致しているかどうかで判断するものとする。またハッシュ値の算出は一度行えばよく、算出したものをメモリ等に記憶して、利用することが一般的に行われる。ルート証明書からハッシュ値を算出することや、メモリに格納したハッシュ値を取出すことを、ハッシュ値の「取得」と呼ぶ。

[0041] 以上が、BD-ROMについての説明である。続いて、本発明にかかるアプリケーション実行装置の内部構成について説明する。

本実施形態にかかるアプリケーション実行装置は、CPU、ROM、RAM、ハードディスクドライブ、BD-ROMドライブ、AVデコーダ、入出力機器等を具備したコンピュータシステムに、Java(TM)2Micro_Edition(J2ME) Personal Basis Profile(PBP 1.0)と、Globally Executable MHP specification(GEM1.0.2)for package media targetsとをフル実装することでJava(TM)プラットフォームを構成し、以下に示す機能的な構成要素をこのJava(TM)プラットフォームに設けることで工業的に生産することができる。

[0042] 図6は、本実施の形態におけるアプリケーション実行装置の機能構成を示すブロック図である。アプリケーション実行装置はBDドライブ1、アプリケーションマネージャ2、バーチャルマシーン3、ハードディスク4、セキュリティマネージャ5で構成される。

(BDドライブ1)

BDドライブ1は、BD-ROMのローディング/イジェクトを行い、BD-ROM内のデータのアクセスを実行する。BD-ROMをBD-ROMドライブ1にローディング/イジェクトした場合、その旨を、BDドライブ1がアプリケーションマネージャ2を通知する。

[0043] (アプリケーションマネージャ2)

アプリケーションマネージャ2は、バーチャルマシーン3内のヒープ領域内で動作するシステムアプリケーションであり、アプリケーションシグナリングを実行する。“アプリケーションシグナリング”とは、GEM1.0.2が規定するMHP(Multimedei Home Platform)において、“サービス”を生存区間としてアプリケーションの起動、実行を行う制御をいう。本実施形態におけるアプリケーションマネージャ2は、この“サービス”の代わりに、BD-ROMにおける“タイトル”を生存区間にして、アプリケーションの起動、実行の制御を実現する。ここで、“タイトル”とは、BD-ROMに記録されている映像・音声データの再生単位であり、アプリケーション管理テーブル(AMT)が一意に割り当てられている。

[0044] アプリケーションを起動させるにあたって、アプリケーションマネージャ2は、起動しようとするアプリケーションが正当なものかどうかを判定する。この判定手順は以下の通りである。BD-ROMがローディングされれば、/BDDATA/BD.ROOT.CERTIFICATEというファイルの存在を確認する。ファイルが存在する場合、アプリケーションマネージャ2がこのディスクルート証明書301をBD-ROMから読み取り、メモリ上に保持する。その後、Java(TM)アーカイブファイル302を読みだし、このJava(TM)アーカイブファイル302に存在する署名を検証する。この検証が正しいのなら、アプリケーションマネージャ2はBD-ROM上に存在するJava(TM)アーカイブファイル302中のクラスファイル401を、バーチャルマシーン3内に読みだし、このクラスファイル401のインスタンスをヒープ領域に生成することで、Java(TM)アプリケーションを起動する。

[0045] (バーチャルマシーン3)

バーチャルマシーン3は、クラスファイルをBD-ROMから読み出すユーザクラスローダ、クラスファイルに対応するインスタンスをJava(TM)アプリケーションとして格納するヒープメモリ、スレッド、Java(TM)スタックから構成されるJava(TM)アプリケーションの実行主体である。ここでスレッドは、Java(TM)アプリケーションにおけるメソッドを実行する論理的な実行主体であり、ローカル変数や、オペランドスタックに格納された引数をオペランドにして演算を行い、演算結果を、ローカル変数又はオペランドスタックに格納する。スレッドによるメソッド実行は、メソッドをなすバイトコードを、CPUのネイティブ

コードに変換した上、CPUに発行することでなされる。このネイティブコード変換については、本願の主眼から外れるため、説明を省く。Java(TM)アーカイブファイル302内にパーミッションリクエストファイル405が存在する場合、マニフェストファイル402の中に、Java(TM)アプリケーションの正しいハッシュ値が入っていなければ、そのJava(TM)アプリケーションを実行してはならない。かかるハッシュ値の判定のため、バーチャルマシーン3は、実行するJava(TM)アプリケーションはどのJava(TM)アーカイブファイル302に格納されていたのかを示す情報をメモリ上に保持する。このパーミッションリクエストファイル405を参照することで、バーチャルマシーン3はアプリケーションマネージャ2が保持するアプリ間通信の許可を確認し、Java(TM)アプリケーションに対してアプリ間通信の機能を提供する。

[0046] (ハードディスク4)

ハードディスク4は、Java(TM) IO Packageからのメソッドを用いることにより、アクセスすることができるローカルストレージである。このローカルストレージは、複数のドメイン領域を有する。ここでドメイン領域とは、各ディスクルート証明書301に対応するディレクトリ(図中のR1,R2)のことであり、これらのディレクトリの配下に、組織毎のディレクトリ(図中のorg1,org2,org3)を格納するというものである。組織のアプリケーション毎のディレクトリ(図中のorg1/app1,org1/app2,org1/app3・・・・)は、MHPのものと同じである。つまりローカルストレージでは、MHPに規定された各組織のアプリケーション毎のディレクトリ(図中のorg1/app1,org1/app2,org1/app3・・・・)を、ルート証明書に対応したディレクトリ(図中のR1,R2)の配下に配置した構成になっている。こうすることで、MHPの格納方式と、互換を維持することができる。ここでローカルストレージのディレクトリ構成をアクセスするためのファイルパスのうち、ルート証明書に対応した部分まで(図中のRoot/R1,Root/R2)を、“ローカルストレージルート”という。

[0047] (セキュリティマネージャ5)

セキュリティマネージャ5は、ルート証明書から算出されたハッシュ値と、ローカルストレージルートとの組みを複数示したハッシュ管理テーブルを保持しており、アプリケーションから、ファイルの読み出し／書き込みが要求されれば、要求元のアプリケーションに対応するルート証明書について、ハッシュ値を算出して、そうして算出したハ

ッシュ値に対応したローカルストレージルートをハッシュ管理テーブルから選ぶ。そうして選んだローカルストレージルートを、ファイルパスに組み入れる。また、Credentialに基づきファイルパスの組織IDに対応するディレクトリを置き換える。こうすることで、アプリケーションのファイルパスの記述は、MHPに規定されたものと互換を保つことができる。

[0048] 以降、アプリケーションマネージャ2、セキュリティマネージャ5の具体的なソフトウェアによる実装について説明する。アプリケーションマネージャ2は、図7に示すようなプログラムを作成して、CPUに実行させることで、アプリケーション実行装置に実装することができる。

図7は、アプリケーションマネージャ2による、Java(TM)アーカイブファイル302内のクラスファイル401に基づくアプリケーションの起動手順を示すフローチャートである。アプリケーションマネージャ2はJava(TM)アーカイブファイル302の中にSIG-BD.SF、SIG-BD.RSA、bd.XXXX.permが存在するかどうかを確認する(SA01)。一つも存在しない場合、Java(TM)アプリケーションが改ざんされている可能性があり、Java(TM)アプリケーションの実行を行わない(SA04)。

[0049] 上記のファイル3つとも存在する場合、MANIFEST.MF、SIG-BD.SF、SIG-BD.RSAを利用しbd.XXXX.permおよびJava(TM)アプリケーションを署名検証する(SA03)。署名検証が成功しなかった場合、有効なbd.XXXX.permがないことを記憶し、デフォルトのパーミッションをを有するクラスファイル401をバーチャルマシーン3に実行させる(SA02)。

署名検証が成功した場合、第1のデジタル証明書チェーンに存在するルート証明書と、BD.ROOT.CERTIFICATE内のディスクルート証明書301との同一性を判定する(SA05)。それぞれのルート証明書が異なる場合、Java(TM)アーカイブファイル302が不正であると判断し、Java(TM)アプリケーションの実行を行わない(SA04)。

[0050] それぞれのルート証明書に同一性がある場合、第1のデジタル証明書チェーンにおけるリーフ証明書内に組織IDが存在しているか否かを確認する(SA06)。組織IDが存在しない場合、Java(TM)アーカイブファイル302が不正であると判断し、Java(TM)アプリケーションの実行を行わない(SA04)。

組織IDが存在する場合、bd.XXXX.permの中にCredentialが存在するかどうかを確認する(SA07)。存在しない場合、ステップSA10に続く。

[0051] Credentialが存在する場合、Credentialを検証する(SA08)。検証処理の詳細は後述する。Credentialが複数ある場合、このステップは各Credentialに対して行われる。

Credentialの検証に一つでも失敗した場合(SA09でNo)、Java(TM)アーカイブファイル302が不正であると判断し、Java(TM)アプリケーションの実行を行わない(SA04)。

Credentialの検証がすべて成功した場合、またはCredentialが存在しない場合、bd.XXXX.permと組織IDとMANIFEST.MF内に存在するアプリIDを記憶し、MANIFEST.MFに記載されている最初に実行すべきクラスファイル401をバーチャルマシーンに読み込ませて、これのインスタンスとなるJava(TM)アプリケーションを実行させる(SA10)。

[0052] 図8を参照して、アプリケーションマネージャ2がCredentialを検証するフローチャートを説明する。図8は、アプリケーションマネージャ2による、Credentialの署名検証の手順を示すフローチャートである。

先ず始めに、受領者ルート証明書のハッシュ値503が、BD.ROOT.CERTIFICATEにおけるディスクルート証明書301と一致するかどうかを確認する(SY01)。一致しない場合、検証が失敗する(SY02)。

[0053] 受領者組織ID504と、第1のデジタル証明書チェーンにおけるリーフ証明書に記載された組織IDと一致するかどうかを確認する(SY03)。一致しない場合、検証が失敗する(SY02)。

受領者アプリID505が、bd.XXXX.perm内のCredential以外の箇所に記載されたアプリIDと一致するかどうかを確認する(SY04)。一致しない場合、検証が失敗する(SY02)。Credentialにおける提供ファイルの名前の先頭が提供者組織ID502と一致するかどうかを確認する(SY05)。一致しない場合、検証が失敗する(SY02)。

[0054] SIG-BD.RSAにおける署名情報の正当性を確認する(SY06)。署名情報が正当でない場合、Credentialが改ざんされている可能性があり、検証が失敗する(SY02)。

署名情報が正当である場合、第2のデジタル証明書チェーンにおけるルート証明書のハッシュ値と、Credentialにおける提供者ルート証明書のハッシュ値との同一性

を確認する(SY07)。一致しない場合、Credentialが不正であり、検証が失敗する(SY02)。

[0055] 第2のデジタル証明書チェーンにおけるリーフ証明書の組織IDが、Credentialの提供者組織ID502と一致するかどうかを確認する(SY08)。一致しない場合、Credentialが不正であり、検証が失敗する(SY02)。

すべての確認が成功した場合、検証が成功する(SY09)。

図9は本発明に係わるアプリケーション実行装置においてアプリケーションマネージャ2が保持する管理情報の一例である。ディスクルート証明書301と、実行されているJava(TM)アーカイブファイル302の「Jarファイル名」と、「組織ID」と、「アプリID」と、「アプリ間通信」と、「Credential」とをテーブルの形で管理する。

[0056] 図10は本発明に係わるアプリケーション実行装置においてアプリケーションマネージャ2が保持する管理情報の中のCredentialテーブルの一行の一例である。Credentialテーブルには「提供者ルート証明書のハッシュ値」501、「提供者組織ID」502、「提供者ファイルリスト」506からなる。この「提供者ファイルリスト」506には、提供ファイル名507、提供者アクセス方法508が記載されている。

[0057] Java(TM)アーカイブファイル302にパーミッションが与えられる場合、バーチャルマシーン3がJava(TM)アプリケーションの実行前に以下の処理を行う。バーチャルマシーン3はMANIFEST.MFにあるJava(TM)アプリケーションのハッシュ値と、Java(TM)アプリケーションの実際のハッシュが一致するかどうかを確認し、一致しない場合実行しない。

Java(TM)アプリケーションはバーチャルマシーン3により実行される。図11を参照して、典型的なJava(TM)アプリケーションがローカルストレージを利用したい場合に行う処理手順を説明する。

[0058] 図11は、Java(TM)アプリケーションがハードディスク4を利用するにあたっての処理手順を示すフローチャートである。

Java(TM)アプリケーションは、仮想ローカルストレージルートを取得する(SC01)。ここで仮想ローカルストレージルートとは、MHPにおける形式で、アクセス先となるファイルを指定するファイルパスであり、/Root、又は、/Storage/Rootという名前で表現され

る。この仮想ローカルストレージルートは、MHPにおけるファイルパスの形式との互換を意図したに過ぎず、ハードディスク4におけるファイルアクセス時において、当該ローカルストレージ名は、ルート証明書ごとに決まるローカルストレージルートに変換される。

[0059] 続いてJava(TM)アプリケーションは組織IDを取得する(SC02)。組織IDはたとえば「4」の数字である。

Java(TM)アプリケーションはローカルストレージルートの名前と組織IDを組み合わせ、読み書きしたいファイルの名前を指定しファイルへの入出力を行う(SC03)。たとえばローカルストレージルートの名前が「/persistent/0003」、組織IDが「7」、読み書きしたいファイルの相対パスが「8/scores.txt」の場合、「/persistent/0003/7/8/scores.txt」のフルパスよりファイルを指定できる。

[0060] Java(TM)アプリケーションが図11のとおりの処理を行うためにセキュリティマネージャ5はJava(TM)アプリケーションに対して以下の関数呼び出しを提供する。

(ア)ローカルストレージルートの取得

(イ)組織IDの取得

(ウ)ファイルからの読み出し

(エ)ファイルへの書き込み

図12を参照して、Java(TM)アプリケーションによる「ローカルストレージルートの取得」関数呼び出しの処理のフローチャートを説明する。

[0061] まずセキュリティマネージャ5は、呼び出し元のJava(TM)アプリケーションにbd.XXXX.permがあるかどうかを確認する(SD01)。bd.XXXX.permがあるかどうかはバーチャルマシーン3からJava(TM)アプリケーションをインスタンスとするクラスファイル401を格納したJava(TM)アーカイブファイル302を取得し、アプリケーションマネージャ2より取得することができる。bd.XXXX.permがない場合、「ローカルストレージルートの取得」を拒否する(SD02)。

[0062] bd.XXXX.permがある場合、アプリケーションマネージャ2よりディスクルート証明書301のハッシュ値を取得する(SD03)。セキュリティマネージャ5はハッシュ管理テーブル(後述)を確認し、ディスクルート証明書301のハッシュ値が既に登録されているか

どうかを確認する(SD04)。登録されている場合、ディスクルート証明書301のハッシュ値に対応するローカルストレージルートをJava(TM)アプリケーションに返す(SD05)。

[0063] ハッシュ管理テーブルにディスクルート証明書301のハッシュ値が登録されていない場合、セキュリティマネージャ5はハッシュ管理テーブルに新たなエントリーを追加する(SD06)。そのエントリーにはディスクルート証明書301のハッシュ値と、テーブル内で一意となるローカルストレージルートが記載される。ハッシュ管理テーブルに新しく登録したエントリーのローカルストレージルートをJava(TM)アプリケーションに返す(SD07)。

[0064] 図13を参照して、セキュリティマネージャ5が保持するハッシュ管理テーブルの一例を示す。ハッシュ管理テーブルにはルート証明書のハッシュ値1301とローカルストレージルート1302が存在する。本図におけるローカルストレージルートの「/0001」,「0003」は、図6のディレクトリ名/R1,/R2をそれぞれ意味するものである。これらのローカルストレージルート1302は、ルート証明書のハッシュ値1301と一対一に対応している。そのため、同じディスクルート証明書301を持つBDディスクにあるJava(TM)アーカイブファイル302中のクラスファイル401のインスタンスであるJava(TM)アプリケーションに対しては同じローカルストレージルート1302を返し、異なるディスクルート証明書301を持つBD-ROMにあるJava(TM)アーカイブファイル302中のクラスファイル401のインスタンスであるJava(TM)アプリケーションに対しては異なるローカルストレージルート1302を返すことになる。

[0065] 図14を参照して、「組織IDの取得」関数呼び出しのフローチャートを説明する。

まずセキュリティマネージャ5は、呼び出し元のJava(TM)アプリケーションにbd.XXXX.permがあるかどうかを確認する(SF01)。bd.XXXX.permがない場合、組織IDを確定できないため「組織IDの取得」を拒否する(SF02)。 bd.XXXX.permがある場合、アプリケーションマネージャ2よりJava(TM)アプリケーションに対応する組織IDを取得しJava(TM)アプリケーションに返す(SF03)。

[0066] 「ファイル読み出し」関数呼び出しは読み出ししたいファイル名のフルパスをパラメータとしてJava(TM)アプリケーションからセキュリティマネージャ5へ伝える。このフル

パスは、組織ID/appID/という形式のものであり、アプリケーションは、MHPにおけるローカルストレージ内のファイルをアクセスするのと同じ手順で、アプリケーション実行装置内のファイルをアクセスしようとする。

[0067] ファイルアクセスが成功する場合、セキュリティマネージャ5がデータをJava(TM)アプリケーションに返す。図15と図16を参照して、「ファイル読み出し」関数呼び出しのフローチャートを説明する。

まずセキュリティマネージャ5は、呼び出し元のJava(TM)アプリケーションにbd.XXXX.permがあるかどうかを確認する(SH01)。bd.XXXX.permがない場合、「ファイル読み出し」を拒否する(SH02)。

[0068] bd.XXXX.permがある場合、アプリケーションマネージャ2よりディスクルート証明書301のハッシュ値を取得する(SH03)。

セキュリティマネージャはハッシュ管理テーブルを確認し、ディスクルート証明書301のハッシュ値に対応するローカルストレージルート1302を取得する(SH04)。

続いて、ファイル名を指定するフルパスの先頭のルート名が仮想ローカルストレージルートの名前と一致するかどうかを判定する(SH05)。これは、装置に依存した形式(ここではMHPと互換をもつ形式)のファイルパスでアクセス先ファイルを指定しているかどうかを、チェックするものであり、一致する場合はルート名を、ディスクルート証明書に対応した形式である、ローカルストレージルートに変換する(SH13)。一致しない場合はアクセスを拒否する(SH02)。

[0069] ここで、変換前後において、フルパスは以下のようになる。

アプリ指定のフルパス:

/仮想ローカルストレージルート/指定組織ID/指定パス

SH05による変換後のパス:

/ローカルストレージルート/指定組織ID/指定パス

その後、セキュリティマネージャ5はファイル名のフルパスを分解する(SH06)。ファイル名のフルパスは「ローカルストレージルート1302+“/”+指定組織ID+“/”+指定パス」の形式を利用するため、ファイル名のフルパスはローカルストレージルート1302と指定組織IDと指定パスに分解することができる。分解できない場合、読み出しを拒否

する(SH02)。

[0070] セキュリティマネージャ5はアプリケーションマネージャ2より呼び出し元のJava(TM)アプリケーションの組織IDを取得する(SH07)。そして、指定組織IDが提供者組織ID502と一致するCredentialをアプリケーションマネージャ2から取得できるかどうかを試みる(SH10)。Credentialを取得しえた場合、アクセスを拒否する(SH02)。

Credentialを取得し得た場合、Java(TM)アプリケーションからの指定パスがCredentialの提供ファイル名506に存在し、提供アクセス方法507にて読み出しが許可されているかどうかを確認する(SH11)。許可されている場合、セキュリティマネージャ5はCredential内にある提供者ルート証明書のハッシュ値501を取得する(SH12)。

[0071] 許可されていない場合、セキュリティマネージャ5は指定組織IDとJava(TM)アプリケーションの組織IDが一致するかどうかを確認する(SH08)。一致した場合、Java(TM)アプリケーションが指定したフルパスに基づき、ファイルをハードディスクより読み出しアプリに返す(SH09)。一致してない場合、読み出しを拒否する(SH02)。

セキュリティマネージャ5はハッシュ管理テーブルを確認し、提供者ルート証明書のハッシュ値501が既に登録されているかどうかを確認する(SH13)。登録されている場合、提供者ルート証明書のハッシュ値501に対応するローカルストレージルート1302を取得し、提供者ローカルストレージルートとして確定する(SH14)。

[0072] ハッシュ管理テーブルに提供者ルート証明書のハッシュ値501が登録されていない場合、セキュリティマネージャ5はハッシュ管理テーブルに新たなエントリーを追加する(SH15)。そのエントリーには提供者ルート証明書のハッシュ値501と、テーブル内で一意となるローカルストレージルート1302が記載される。

ハッシュ管理テーブルに新しく登録した行のローカルストレージルート1302を提供者ローカルストレージルートとして確定する(SH16)。

[0073] 提供者ローカルストレージルートが確定された後、セキュリティマネージャ5はファイル名のフルパスの中のローカルストレージルート1302を提供者ローカルストレージルートに置き換える(SH17)。

セキュリティマネージャ5は置き換えた後のファイル名のフルパスのファイルをハードディスク4より読み出して、Java(TM)アプリケーションに返す(SH18)。

[0074] 以上が、ファイル読み出しについての説明である。続いて、ファイル書き込みについて説明する。

「ファイル書き込み」関数呼び出し時は、書き込みしたいファイル名のフルパスと書き込みたいデータをパラメータとしてJava(TM)アプリケーションからセキュリティマネージャ5へ伝える。成功する場合、セキュリティマネージャ5がデータをファイルに書き込む。図17と図18を参照して、「ファイル書き込み」関数呼び出しのフローチャートを説明する。

[0075] まずセキュリティマネージャ5は、呼び出し元のJava(TM)アプリケーションにbd.XXXX.permがあるかどうかを確認する(SI01)。bd.XXXX.permがない場合、「ファイル書き込み」を拒否する(SI02)。

bd.XXXX.permがある場合、アプリケーションマネージャ2よりディスクルート証明書301のハッシュ値を取得する(SI03)。

[0076] セキュリティマネージャはハッシュ管理テーブルを確認し、ディスクルート証明書301のハッシュ値に対応するローカルストレージルート1302を取得する(SI04)。

そして、ファイル名を指定するフルパスの先頭のルート名が仮想ローカルストレージルートの名前と一致するかどうかを判定する(SI05)。一致する場合はルート名をローカルストレージルートに変換する(SI13)。一致しない場合はアクセスを拒否する(SI02)。

ここで、変換前後において、フルパスは以下のようになる。

アプリ指定のフルパス:

/仮想ローカルストレージルート/指定組織ID/指定パス

SH05による変換後のパス:

/ローカルストレージルート/指定組織ID/指定パス

その後、セキュリティマネージャ5はファイル名のフルパスを分解する(SI06)。ファイル名のフルパスは「ローカルストレージルート1302+“/”+指定組織ID+“/”+指定パス」の形式を利用するため、ファイル名のフルパスはローカルストレージルート1302と指定組織IDと指定パスに分解することができる。分解できない場合、書き込みを拒否する(SI02)。

[0077] セキュリティマネージャ5は呼び出し元のJava(TM)アプリケーションの組織IDを取得

する(SI07)。そして、指定組織IDが提供者組織ID502と一致するCredentialをアプリケーションマネージャ2より取得するかどうかを試みる(SI10)。存在しない場合、書き込みを拒否する(SI02)。

取得できた場合、Java(TM)アプリケーションからの指定パスがCredentialの提供ファイル名506として存在し、提供アクセス方法507にて書き込みが許可されているかどうかを確認する(SI11)。許可されていない場合、セキュリティマネージャ5は指定組織IDとJava(TM)アプリケーションの組織IDが一致するかどうかを確認する(SI08)。一致した場合、Java(TM)アプリケーションが指定したフルパスに基づき、ファイルにデータを書き込む(SI09)。一致しない場合、書き込みを拒否する(SI02)。

[0078] 書き込みが許可されていることが確認できた場合、セキュリティマネージャ5はCredential内にある提供者ルート証明書のハッシュ値501を取得する(SI12)。

セキュリティマネージャ5はハッシュ管理テーブルを確認し、提供者ルート証明書のハッシュ値501が既に登録されているかどうかを確認する(SI13)。登録されている場合、提供者ルート証明書のハッシュ値501に対応するローカルストレージルート1302を取得し、提供者ローカルストレージルートとして確定する(SI14)。

[0079] ハッシュ管理テーブルに提供者ルート証明書のハッシュ値501が登録されていない場合、セキュリティマネージャ5はハッシュ管理テーブルに新たな行を追加する(SI15)。その行には提供者ルート証明書のハッシュ値501と、テーブル内で一意となるローカルストレージルート1302が記載される。

ハッシュ管理テーブルに新しく登録した行のローカルストレージルート1302を提供者ローカルストレージルートとして確定する(SI16)。

[0080] 提供者ローカルストレージルートが確定された後、セキュリティマネージャ5はファイル名のフルパスの中のローカルストレージルート1302を提供者ローカルストレージルートに置き換える(SI17)。

セキュリティマネージャ5は置き換えた後のファイル名のフルパスのファイルを書き込む(SI18)。

[0081] 以上のように本実施形態によれば、ローカルストレージ4の内部にはルート証明書ハッシュ値のそれぞれに割り当てられたディレクトリが存在するので、これらのディレク

トリの配下に、組織毎、アプリケーション毎の領域を作成すれば、世界的なレベルで、組織IDがユニークでなくてもよい。“ドメイン領域”という閉じた世界において、複数の組織を区別できれば足りるので、組織IDを、世界的なレベルで、ユニークな値にする必要はなく、第3者機関による管理は不要になる。

[0082] またルート証明書は、装置本体ではなく、記憶手段内のドメイン領域に割り当てられるので、BD-ROMがアプリケーション実行装置に装填される限りは、必ず動作することが保障される。もっとも、ディスクルート証明書が暴露される可能性がない訳ではないが、そうした場合、そのBD-ROMを使えないようにするか、また、そのBD-ROMについてのディスクルート証明書のみをアップデートすればよく、他のBD-ROMにて供給されたアプリケーションは、従前通り、ディスクルート証明書を用いればよいので、確実な動作保障を実現することができる。

[0083] このように世界的なレベルでの組織IDの管理を必要とせず、また、従前のアプリケーションの同士保障を高いレベルに維持することができるので、本発明にかかるアプリケーション実行装置は、映画作品に関する処理を行うアプリケーションを実行するアプリケーション実行装置の世界的な標準化に大きく寄与することができる。

(備考)

以上、本願の出願時点において、出願人が知り得る最良の実施形態について説明したが、以下に示す技術的トピックについては、更なる改良や変更実施を加えることができる。各実施形態に示した通り実施するか、これらの改良・変更を施すか否かは、何れも任意的であり、実施する者の主観によることは留意されたい。

[0084] (「Java(TM)アーカイブファイル302の選択)

BD-ROMに映像などのデータが共存する場合、映像再生におけるイベント(チャプター2の再生開始等)により指定されるJava(TM)アーカイブファイル302や、ユーザの画面上の選択に応じたJava(TM)アーカイブファイル302を選択することも考えられる。

デジタル証明書チェーンが一つの証明書から構成される場合もある。その場合、ルート証明書もリーフ証明書も同じ証明書である。

[0085] (パーミッションの種類)

もっと豊富な機能を持つアプリケーション実行装置の場合、bd.XXXX.permに他の種類のパーミッションが含まれていてもよい。bd.XXXX.permの中に複数のデジタル信用証明書312が含まれても良い。

(組織ID)

実施の形態によっては組織IDがBD-ROM上の異なるファイルに記載されることが考えられる。そのとき、「組織IDの取得」を拒否する必要はなく、別の方法により確定された組織IDを返すことにしてもよい。

[0086] (ファイルの読み出し／書き込み)

図15、図16、図17、図18ではファイルの読み出しを中心に説明しているが、同様にJava(TM)アプリケーションからディレクトリにアクセスすることも可能である。ディレクトリにアクセスする場合、ファイル名のフルパスに指定パスがない場合も考えられる。

[0087] また図15と図16ではファイル全体を読み取る関数呼び出しとして説明しているが、同様にファイルを部分的に取得したりして典型的なファイルアクセスをすることも可能である。

図11に示す制御フローは一例であり、Java(TM)アプリケーションのつくりによって大きく異なることもある。

[0088] (他の方式との併用)

本方式は他のファイルアクセスパーミッション方式(たとえばUNIX(登録商標)によく利用されるユーザ・グループ・ワールドアクセスモデル)と併用することが可能である。たとえば、本方式と第2の方式を併用し以下の優先度を決めるようにしても良い。

(ア)ステップSH06においてフルパスに分解できなかった場合、あるいはステップSH10においてデジタル信用証明書が存在しない場合、第2の方式のアクセス制御を利用する。

[0089] (イ)ステップSH09において第2の方式のアクセス制御を利用する。

(ウ)その他に関しては本方式を優先する。

(ハッシュ値)

本実施の形態におけるハッシュ値とはSHA-1やMD5などのセキュアハッシュ関数を利用した結果の値である。セキュアハッシュ関数は、同じハッシュ値を持つ異なるデ

ータを見つけるのは実質不可能であるという特徴を持っている。

[0090] (ルート証明書のハッシュ値)

本実施の形態におけるルート証明書のハッシュ値とは、必ずしもルート証明書全体のデータから算出する必要はなく、少なくともルート証明書の中に含まれる公開鍵のデータのみから算出することにしてもよい。MANIFEST.MF、SIG-BD.SF、SIG-BD.RSAの中に格納されるハッシュ値の計算に利用されるセキュアハッシュ関数はディスク作成者が明示的に選択できる。

[0091] 本実施の形態ではbd.XXXX.permの中にあるデジタル信用証明書には提供者ルート証明書のハッシュ値501および受領者ルート証明書のハッシュ値503の計算に利用されるセキュアハッシュ関数が固定されていることを接続相手にしているが、bd.XXXX.permの中にあるデジタル信用証明書の中に、提供者ルート証明書のハッシュ値501および受領者ルート証明書のハッシュ値503の計算に利用されるセキュアハッシュ関数を明示するようにしても良い。

[0092] (ルート証明書の比較)

ステップSA05におけるルート証明書の比較は、ルート証明書が同じとあるかどうかの比較、ルート証明書の中に含まれる公開鍵が同じであるかどうかの比較を行うようにしても良い。また別の方式としては、デジタルシグネチャファイルの中にある一つ目の証明書(ルート証明書)を無視し、ルート証明書に続く二つ目の証明書がディスクルート証明書301により署名されているかどうかを確認するようにしてもよい。どの方式を使ってもディスクルート証明書301がデジタルシグネチャファイルの中の二つ目の証明書を保障していることになるためセキュリティ観点での効果が同じである。

[0093] ステップSA05による比較はアプリケーション間通信を悪用した攻撃を防ぐのが主な目的である。アプリケーション間通信を悪用した攻撃は以下のとおりに作られた攻撃用BD-ROMを利用し試みることが考えられる。

1.攻撃対象のディスク作成者により作成された正当なBD-ROMから、デジタル証明書により署名されている攻撃対象のJava(TM)アーカイブファイル302を読み取る

2.攻撃するためのJava(TM)アーカイブファイル302を作成し、デジタル証明書により署名を行う

3.攻撃対象のJava(TM)アーカイブファイル302と攻撃するためのJava(TM)アーカイブファイル302を攻撃用BD-ROMに記録

攻撃するためのJava(TM)アーカイブファイル302と攻撃対象のJava(TM)アーカイブファイル302はともにデジタル証明書により署名されているが、どちらも異なるルート証明書を利用する。アプリケーション実行装置において二つのJava(TM)アーカイブファイル302にあるJava(TM)アプリケーションに対してアプリ間通信のパーミッションが与えられれば、攻撃するためのJava(TM)アーカイブファイル302が攻撃対象のJava(TM)アーカイブファイル302に対して不正なアプリ間通信を行うことが可能になり、攻撃対象のJava(TM)アーカイブファイル302は自身で利用する記憶領域に対して攻撃対象のディスク作成者により予期しない動作をしうる。

[0094] 上記の攻撃を防止するためにステップSA05においてルート証明書の比較が必要である。尚、ステップSA05の変わりに異なるルート証明書を利用するJava(TM)アプリケーション同士のアプリ間通信を防止するようにしてもよい。そのとき、一つのBD-ROMに複数のディスクルート証明書301を持つようにしてもよい。

(ローカルストレージ名の名前取得関数)

実施形態では、ローカルストレージ名の名前取得関数のステップSC01において、MHPと互換をもつ形式のファイルパスである、仮想ローカルストレージ名を一旦アプリケーションに返してから、SH05,SI05において、アプリケーション実行装置におけるローカルストレージ名に変換したが、ローカルストレージ名の名前取得関数のステップSC01において、直接、ハッシュ管理テーブルに記述されたローカルストレージ名を直接、Java(TM)アプリケーションに返し、仮想ローカルストレージ名からローカルストレージ名への変換を省いてもよい。

[0095] (タイトル)

BD-ROM再生装置として、アプリケーション実行装置を製造する場合、BD-ROMの装填やユーザ操作、装置の状態に応じてタイトルを選択する“モジュールマネージャ”をアプリケーション実行装置に設けるのが望ましい。BD-ROM再生装置内のデコーダは、この“モジュールマネージャ”によるタイトル選択に応じて、プレイリスト情報に基づくAVClipの再生を行う。

[0096] アプリケーションマネージャ2は、“モジュールマネージャ”がタイトルの選択を行った際、前のタイトルに対応するAMTと、カレントタイトルに対応するAMTとを用いてシグナリングを実行する。このシグナリングは、前のタイトルに対応するAMTには記載されているが、カレントタイトルに対応するAMTには記載されていないアプリケーションの動作を終了させ、前のタイトルに対応するAMTには記載されておらず、カレントタイトルに対応するAMTには記載されているアプリケーションの動作を開始させるという制御を行う。そして、このアプリケーションシグナリングがなされる度に、上述したようなディスクルート証明書を用いた検証を行うのが望ましい。

[0097] (BD-BOX)

長編の映画作品やグループ物の映画作品を複数のBD-ROMに記録して、いわゆるBD-BOXを構成する際、これらのBD-ROMには、同一のディスクルート証明書301を割り当てるのが望ましい。このように、複数BD-ROMに同一のディスクルート証明書301を割り当てた場合、アプリケーションによっては、ディスクの交換前後で、動作するものもでてくる。このように、ディスクの交換前後で動作するアプリケーションを“ディスクアンバウンダリィアプリケーション”という。ここでアプリケーションマネージャ2は、BD-ROMの交換がなされた場合において、新たに装填されたBD-ROMのディスクルート証明書301を読みだし、そのディスクアンバウンダリィアプリケーションを定義するJava(TM)アーカイブファイル302内のディスクルート証明書301との同一性を確認するという処理を行うのが望ましい。そして、同一性があれば、ディスクアンバウンダリィアプリケーションの同士を継続させ、もし同一性がなければ、ディスクアンバウンダリィアプリケーションを強制的に終了させる。このようにすることで、BD-ROMの交換の前後において、正当なアプリケーションのみを、動作させることができる。

[0098] (Credential)

・Credentialは、複数のXML文書のうち、特定のタグにて囲まれた部分を取出して、これらを結合することで構成するのが望ましい。

・Credentialのデータを提供者組織のリーフ証明書(の公開鍵)により署名した値を、Credentialの署名情報として、bd.XXXXX.permの中に記載してもよい。

・「権限の提供」を行う場合において、bd.XXXXX.permは複数あってもよいが、複数あ

る場合、bd.XXXXX.permにおいて、SIG-BD.SFのどのリーフ証明書がどのCredentalとの照合に使われるかの情報を記述するのが望ましい。

・Credentialのやり方として、bd.XXXXX.perm中に提供者ファイル名を書いておき、Credentialの実体を、他のファイルに書いてある値から算出してもよい。

・そして、これらを全部組み合わせて、提供者ファイル、リーフ証明書を特定する情報、署名情報がbd.XXXXX.permに得られるようにするのが望ましい。

(ローカルストレージ)

本実施形態においてローカルストレージは、装置組込み型のハードディスクであるとしたが、セキュアな記録媒体であれば、過搬型のものを採用してもよい。例えば、SDメモリカードを採用してもよい。

[0099] (実装すべきパッケージ)

アプリケーション実行装置の実施にあたっては、以下のBD-J Extentionをアプリケーション実行装置に実装するのが望ましい。BD-J Extentionは、GEM[1.0.2]を越えた機能を、Java(TM)プラットフォームに与えるために特化された、様々なパッケージを含んでいる。BD-J Extentionにて供給されるパッケージには、以下のものがある。

・org.bluray.media

このパッケージは、Java(TM) Media FrameWorkに追加すべき、特殊機能を提供する。アングル、音声、字幕の選択についての制御が、このパッケージに追加される。

・org.bluray.ti

このパッケージは、GEM[1.0.2]における“サービス”を“タイトル”にマップして動作するためのAPIや、BD-ROMからタイトル情報を問い合わせる機構や新たなタイトルを選択する機構を含む。

・org.bluray.application

このパッケージは、アプリケーションの生存区間を管理するためのAPIを含む。また、アプリケーションを実行させるにあたってのシグナリングに必要な情報を問い合わせるAPIを含む。

・org.bluray.ui

このパッケージは、BD-ROMに特化されたキーイベントのための定数を定義し、映

像再生との同期を実現するようなクラスを含む。

・org.bluray.vfs

このパッケージは、データの所在に拘らず、データをシームレスに再生するため、BD-ROMに記録されたコンテンツ(on-discコンテンツ)と、BD-ROMに記録されていないLocal Storage上のコンテンツ(off-discコンテンツ)とをバインドする機構(Binding Scheme)を提供する。

[0100] Binding Schemeとは、BD-ROM上のコンテンツ(AVClip、字幕、BD-Jアプリケーション)と、Local Storage上の関連コンテンツとを関連付けるものである。このBinding Schemeは、コンテンツの所在に拘らず、シームレス再生を実現する。

(ローカルストレージのアクセス)

例えば、ファイルパス「／Persistent／1／1／streams／に、所望のファイルが存在するか確認するは、java(TM).ioのexits()メソッドを用いることで行われる。所望のファイルがO.m2tsである場合の、java(TM).ioのexits()メソッドの用例を以下に示す。

例:

new java(TM).io.File("／Persistent／1／1／streams／0.m2ts").exists();

(パーミッションリクエストファイル)

パーミッションリクエストファイルは、以下の機能を許可するか否かを定めてもよい。

[0101] ・ネットワーク接続の利用

・BD-ROMのアクセス

・BD-ROMにおける他のタイトルの選択

・他のプラットフォームの実行制御

(映像・音声)

図1(a)に示したBD-ROMのディレクトリ構造において、ROOTディレクトリの配下にBDMVディレクトリを設け、このディレクトリに、MPEG2-TS形式のAVストリームであるAVClipや、これの再生経路を規定するプレイリスト情報を記録してもよい。そしてプレイリスト情報を通じた再生を行うようJava(TM)アプリケーションを記述してもよい。

[0102] プレイリスト情報が00001.mplsというファイルに格納された場合、Java(TM)アプリケー

ションは、JMFライブラリに基づき、JMFプレーヤインスタンスを生成する。JMF A"BD://00001.mpls";は、PLを再生するプレーヤインスタンスの生成をバーチャルマシンに命じるメソッドである。A.playは、JMFプレーヤインスタンスに再生を命じるメソッドである。

[0103] (BD-ROMコンテンツ)

BD-ROMに記録されるアプリケーションは、映画作品を構成するものであるとしたが、ローカルストレージにインストールして利用されるアプリケーションではなく、BD-ROMに記録された状態で利用されるアプリケーションであるなら、これ以外のものを構成するものであってもよい。例えば、ゲームソフトを構成するアプリケーションであってもよい。また、本実施形態ではディスク媒体として、BD-ROMを題材に選んだが、可搬体であり、著作権保護がなされた記録媒体であるなら、他の記録媒体を採用してもよい。

[0104] (Virtual Package)

Virtual Packageを生成させるような処理をセキュリティマネージャ5に行わせてもよい。Virtual Packageとは、BD-ROM等のリードオンリー型の記録媒体に記録されているデジタルストリームと、ハードディスク等のリライタブル型の記録媒体に記録されているデジタルストリームとを動的に組み合わせて、仮想的なパッケージを構築することにより、リードオンリー型記録媒体の内容拡張を図る技術である。ここBD-ROMに記録されているデジタルストリームが、映画作品の本編を構成するものであり、ハードディスクに記録されているデジタルストリームが、映画作品の続編を構成するものである場合、上述したVirtual Packageを構築することにより、BD-ROM上の本編と、ハードディスク上の続編とを、1つの長編の映画作品として取り扱い、再生に供することができる。

[0105] これは、セキュリティマネージャ5がVirtual Package情報を生成することでなされる。Virtual Package情報とは、BD-ROMにおけるボリューム管理情報を拡張した情報である。ここでボリューム管理情報は、ある記録媒体上に存在するディレクトリ－ファイル構造を規定する情報であり、ディレクトリについてのディレクトリ管理情報、ファイルについてのファイル管理情報とからなる。Virtual Package情報とは、BD-ROMのディレク

トリーファイル構造を示すボリューム管理情報に、新たなファイル管理情報を追加することにより、BD-ROMにおけるディレクトリーファイル構造の拡張を図ったものである。かかるVirtual Package情報の生成により、アプリケーションは、BD-ROMをアクセスするのと同じ感覚で、ローカルストレージにおけるディスクルート証明書毎のドメイン領域の、組織毎の領域をアクセスすることができる。

[0106] (制御手順の実現)

各実施形態においてフローチャートを引用して説明した制御手順や、機能的な構成要素による制御手順は、ハードウェア資源を用いて具体的に実現されていることから、自然法則を利用した技術的思想の創作といえ、"プログラムの発明"としての成立要件を満たす。

[0107] ・本発明に係るプログラムの生産形態

本発明に係るプログラムは、コンピュータが実行することができる実行形式のプログラム(オブジェクトプログラム)であり、実施形態に示したフローチャートの各ステップや、機能的構成要素の個々の手順を、コンピュータに実行させるような1つ以上のプログラムコードから構成される。ここでプログラムコードは、プロセッサのネィティブコード、JAVAバイトコードというように、様々な種類がある。またプログラムコードによる各ステップの実現には、様々な態様がある。外部関数を利用して、各ステップを実現することができる場合、この外部関数をコールするコール文が、プログラムコードになる。また、1つのステップを実現するようなプログラムコードが、別々のオブジェクトプログラムに帰属することもある。命令種が制限されているRISCプロセッサでは、算術演算命令や論理演算命令、分岐命令等を組合せることで、フローチャートの各ステップが実現されることもある。

[0108] 本発明にかかるプログラムは、以下のようにして作ることができる。先ず初めに、ソフトウェア開発者は、プログラミング言語を用いて、各フローチャートや、機能的な構成要素を実現するようなソースプログラムを記述する。この記述にあたって、ソフトウェア開発者は、プログラミング言語の構文に従い、クラス構造体や変数、配列変数、外部関数のコールを用いて、各フローチャートや、機能的な構成要素を具現するソースプログラムを記述する。

[0109] 記述されたソースプログラムは、ファイルとしてコンパイラに与えられる。コンパイラは、これらのソースプログラムを翻訳してオブジェクトプログラムを生成する。

コンパイラによる翻訳は、構文解析、最適化、資源割付、コード生成といった過程からなる。構文解析では、ソースプログラムの字句解析、構文解析および意味解析を行い、ソースプログラムを中間プログラムに変換する。最適化では、中間プログラムに対して、基本ブロック化、制御フロー解析、データフロー解析という作業を行う。資源割付では、ターゲットとなるプロセッサの命令セットへの適合を図るため、中間プログラム中の変数をターゲットとなるプロセッサのプロセッサが有しているレジスタまたはメモリに割り付ける。コード生成では、中間プログラム内の各中間命令を、プログラムコードに変換し、オブジェクトプログラムを得る。

[0110] オブジェクトプログラムが生成されるとプログラマはこれらに対してリンカを起動する。リンカはこれらのオブジェクトプログラムや、関連するライブラリプログラムをメモリ空間に割り当て、これらを1つに結合して、ロードモジュールを生成する。こうして生成されるロードモジュールは、コンピュータによる読み出しを前提にしたものであり、各フローチャートに示した処理手順や機能的な構成要素の処理手順を、コンピュータに実行させるものである。以上の処理を経て、本発明に係るプログラムを作ることができる。

・本発明に係るプログラムの使用形態

本発明に係るプログラムは、以下のようにして使用することができる。

[0111] (i)組込プログラムとしての使用

本発明に係るプログラムを組込プログラムとして使用する場合、プログラムにあたるロードモジュールを、基本入出力プログラム(BIOS)や、様々なミドルウェア(オペレーションシステム)と共に、命令ROMに書き込む。こうした命令ROMを、制御部に組み込み、CPUに実行させることにより、本発明に係るプログラムを、アプリケーション実行装置の制御プログラムとして使用することができる。

[0112] (ii)アプリケーションとしての使用

アプリケーション実行装置が、ハードディスク内蔵モデルである場合は、基本入出力プログラム(BIOS)が命令ROMに組み込まれており、様々なミドルウェア(オペレーシ

ョンシステム)が、ハードディスクにプレインストールされている。また、ハードディスクから、システムを起動するためのブートROMが、アプリケーション実行装置に設けられている。

[0113] この場合、ロードモジュールのみを、過搬型の記録媒体やネットワークを通じて、アプリケーション実行装置に供給し、1つのアプリケーションとしてハードディスクにインストールする。そうすると、アプリケーション実行装置は、ブートROMによるブートストラップを行い、オペレーションシステムを起動した上で、1つのアプリケーションとして、当該アプリケーションをCPUに実行させ、本発明に係るプログラムを使用する。

[0114] ハードディスクモデルのアプリケーション実行装置では、本発明のプログラムを1つのアプリケーションとして使用しうるので、本発明に係るプログラムを単体で譲渡したり、貸与したり、ネットワークを通じて供給することができる。

(アプリケーションマネージャ2～セキュリティマネージャ4)

アプリケーションマネージャ2～セキュリティマネージャ4は、一個のシステムLSIとして実現することができる。

[0115] システムLSIとは、高密度基板上にベアチップを実装し、パッケージングしたものをいう。複数個のベアチップを高密度基板上に実装し、パッケージングすることにより、あたかも1つのLSIのような外形構造を複数個のベアチップに持たせたものも、システムLSIに含まれる(このようなシステムLSIは、マルチチップモジュールと呼ばれる。)。

ここでパッケージの種別に着目するとシステムLSIには、QFP(クッド フラッド アレイ)、PGA(ピン グリッド アレイ)という種別がある。QFPは、パッケージの四側面にピンが取り付けられたシステムLSIである。PGAは、底面全体に、多くのピンが取り付けられたシステムLSIである。

[0116] これらのピンは、他の回路とのインターフェイスとしての役割を担っている。システムLSIにおけるピンには、こうしたインターフェイスの役割が存在するので、システムLSIにおけるこれらのピンに、他の回路を接続することにより、システムLSIは、アプリケーション実行装置の中核としての役割を果たす。

システムLSIにパッケージングされるベアチップは、“フロントエンド部”、“バックエンド部”、“デジタル処理部”からなる。“フロントエンド部”は、アナログ信号を、デジタル

化する部分であり、“バックエンド部”はデジタル処理の結果、得られたデータを、アナログ化して出力する部分である。

[0117] 各実施形態において内部構成図として示した各構成要素は、このデジタル処理部内に実装される。

先に“組込プログラムとしての使用”で述べたように、命令ROMには、プログラムにあたるロードモジュールや、基本入出力プログラム(BIOS)、様々なミドルウェア(オペレーションシステム)が書き込まれる。本実施形態において、特に創作したのは、このプログラムにあたるロードモジュールの部分なので、プログラムにあたるロードモジュールを格納した命令ROMを、ベアチップとしてパッケージングすることにより、本発明に係るシステムLSIは生産することができる。

[0118] 具体的な実装については、SoC実装やSiP実装を用いることが望ましい。SoC(System on chip)実装とは、1チップ上に複数の回路を焼き付ける技術である。SiP(System in Package)実装とは、複数チップを樹脂等で1パッケージにする技術である。以上の過程を経て、本発明に係るシステムLSIは、各実施形態に示したアプリケーション実行装置の内部構成図を基に作ることができる。

[0119] 尚、上述のようにして生成される集積回路は、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。

さらに、各記録アプリケーション実行装置の構成要素の一部又は全てを1つのチップとして構成してもよい。集積回路化は、上述したSoC実装,SiP実装に限るものではなく、専用回路又は汎用プロセスで実現してもよい。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シリコンフィギュラブル・プロセッサを利用することが考えられる。更には、半導体技術の進歩又は派生する技術により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回路化を行っても良い。例えば、バイオ技術の適応などが可能性としてありうる。

産業上の利用可能性

[0120] 本発明に係るアプリケーション実行装置は、上記実施形態に内部構成が開示されており、この内部構成に基づき量産することが明らかなので、資質において工業上利

用することができる。このことから本発明に係るアプリケーション実行装置は、産業上の利用可能性を有する。

請求の範囲

[1] ディスクルート証明書と、アプリケーションとが記録されたディスク媒体からアプリケーションを読み出して、実行するアプリケーション実行装置であって、

ディスクルート証明書は、ルート認証局から配布されたルート証明書を、当該ディスク媒体の作成者が当該ディスク媒体に割り当てたものであり、

ディスクルート証明書からハッシュ値を取得し、当該ハッシュ値を用いてアプリケーションの正当性を判定する管理手段と、

管理手段が正当であると判定した場合、アプリケーションを実行する実行手段と、

複数のドメイン領域を有する記憶手段と、

記憶手段内に存在する複数のドメイン領域のうち、取得されたハッシュ値に対応するものをアプリケーションに割り当てる割当手段と

を備えることを特徴とするアプリケーション実行装置。

[2] ディスク媒体には、第1デジタル証明書チェーンが記録されており、

前記管理手段による正当性判定は、

前記第1デジタル証明書チェーン中のルート証明書から取得されるハッシュ値と、前記ディスクルート証明書から取得されるハッシュ値とが一致するか否かのチェックを含み、

前記ドメイン領域は、複数の組織領域を含み、

前記割当手段による割り当ては、

ハッシュ値が一致している場合、アプリケーションに割り当てられたドメイン領域中の複数の組織領域のうち、第1デジタル証明書チェーン中のリーフ証明書に記載されている組織IDに対応するものの利用を、アプリケーションに許可することを含む、請求項1記載のアプリケーション実行装置。

[3] 前記アプリケーションの供給元となる組織は、別の組織から領域利用の権限の提供を受けており、

前記ディスク媒体には更に、

領域利用権限の提供者となる組織を示す提供者組織ID、及び、領域利用権限の受領者となる組織を示す受領者組織IDを含むクレデンシャル情報が記録されており

、

前記管理手段は更に、前記クレデンシャル情報の正当性の確認を行い、

前記割当手段による割り当ては、

前記クレデンシャル情報の正当性が確認された場合、アプリケーションに割り当てられたドメイン領域中の複数の組織領域のうち、提供者組織IDに対応するものの利用を、アプリケーションに許可することを含む、請求項2記載のアプリケーション実行装置。

[4] 前記クレデンシャル情報は、

提供者組織に固有なルート証明書から取得されるハッシュ値と、受領者組織に固有なルート証明書から取得されるハッシュ値とを含み、

前記管理手段によるクレデンシャル情報の正当性判定は、

ディスクルート証明書から取得されるハッシュ値が、受領者組織に固有なルート証明書から取得されるハッシュ値と一致するか否かのチェックと、

前記第1デジタル証明書チェーン中のリーフ証明書に記載されている組織IDと、クレデンシャル情報に示される受領者組織IDとが一致しているか否かのチェックとを含む

ことを特徴とする請求項3記載のアプリケーション実行装置。

[5] ディスク媒体には、第2デジタル証明書チェーンが記録されており、

前記管理手段によるクレデンシャル情報の正当性判定は更に、

前記第2のデジタル証明書チェーンの中のルート証明書からハッシュ値を取得して、そのハッシュ値が前記提供者組織に固有なルート証明書から取得されるハッシュ値と一致するか否かのチェックと、

前記第2のデジタル証明書チェーンの中のリーフ証明書に記載されている組織IDが提供者組織IDと一致するか否かのチェックとを含む、請求項4記載のアプリケーション実行装置。

[6] 前記クレデンシャル情報は更にファイルリストを含み、

前記割当手段による組織領域の利用許可は、

組織領域配下に存在するファイルのうち、ファイルリストに示されるものを、前記アプ

リケーションにアクセスさせることを含む、請求項5記載のアプリケーション実行装置。

[7] 前記クレデンシャル情報は更に、ファイルのアクセス方法を示すアクセス情報を有し、

前記割当手段による組織領域の利用許可は、

組織領域配下に存在するファイルのうち、ファイルリストに示されるものを、アクセス情報に示されるアクセス方法で、前記アプリケーションにアクセスさせることを含む、請求項6記載のアプリケーション実行装置。

[8] ディスク媒体には、第1デジタル証明書チェーンが記録されており、

前記管理手段による正当性判定は、

前記第1デジタル証明書チェーン内のルート証明書から取得されるハッシュ値と、前記ディスクルート証明書から取得されるハッシュ値とが一致するか否かのチェックを含み、

、 前記実行手段によるアプリケーションの実行は、

ハッシュ値が一致している場合になされる、請求項1記載のアプリケーション実行装置。

[9] ディスクルート証明書と、アプリケーションとが記録されたディスク媒体からアプリケーションを読み出して、コンピュータに実行させる管理方法であって、

ディスクルート証明書は、ルート認証局から配布されたルート証明書を、当該ディスク媒体の作成者が当該ディスク媒体に割り当てたものであり、

ディスクルート証明書からハッシュ値を取得し、当該ハッシュ値を用いてアプリケーションの正当性を判定する管理ステップと、

管理ステップが正当であると判定した場合、アプリケーションを実行する実行ステップと、

コンピュータの記憶手段内に存在する複数のドメイン領域のうち、取得されたハッシュ値に対応するものをアプリケーションに割り当てる割当ステップと

を有することを特徴とする管理方法。

[10] ディスクルート証明書と、アプリケーションとが記録されたディスク媒体からアプリケーションを読み出して、コンピュータに実行させるプログラムであって、

ディスクルート証明書は、ルート認証局から配布されたルート証明書を、当該ディスク媒体の作成者が当該ディスク媒体に割り当てたものであり、

ディスクルート証明書からハッシュ値を取得し、当該ハッシュ値を用いてアプリケーションの正当性を判定する管理ステップと、

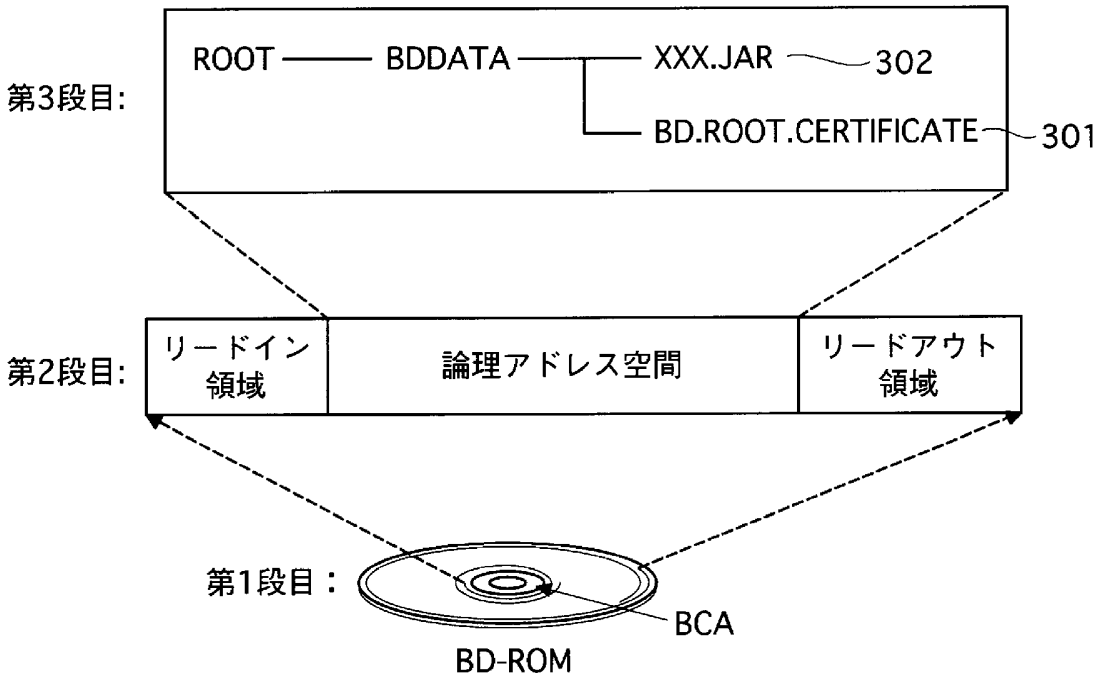
管理ステップが正当であると判定した場合、アプリケーションを実行する実行ステップと、

コンピュータの記憶手段内に存在する複数のドメイン領域のうち、取得されたハッシュ値に対応するものをアプリケーションに割り当てる割当ステップと

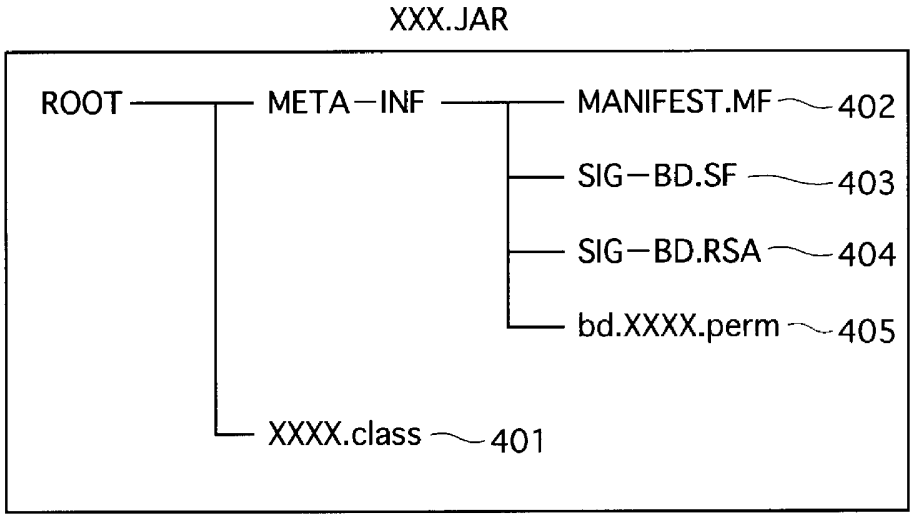
をコンピュータに実行させることを特徴とするプログラム。

[図1]

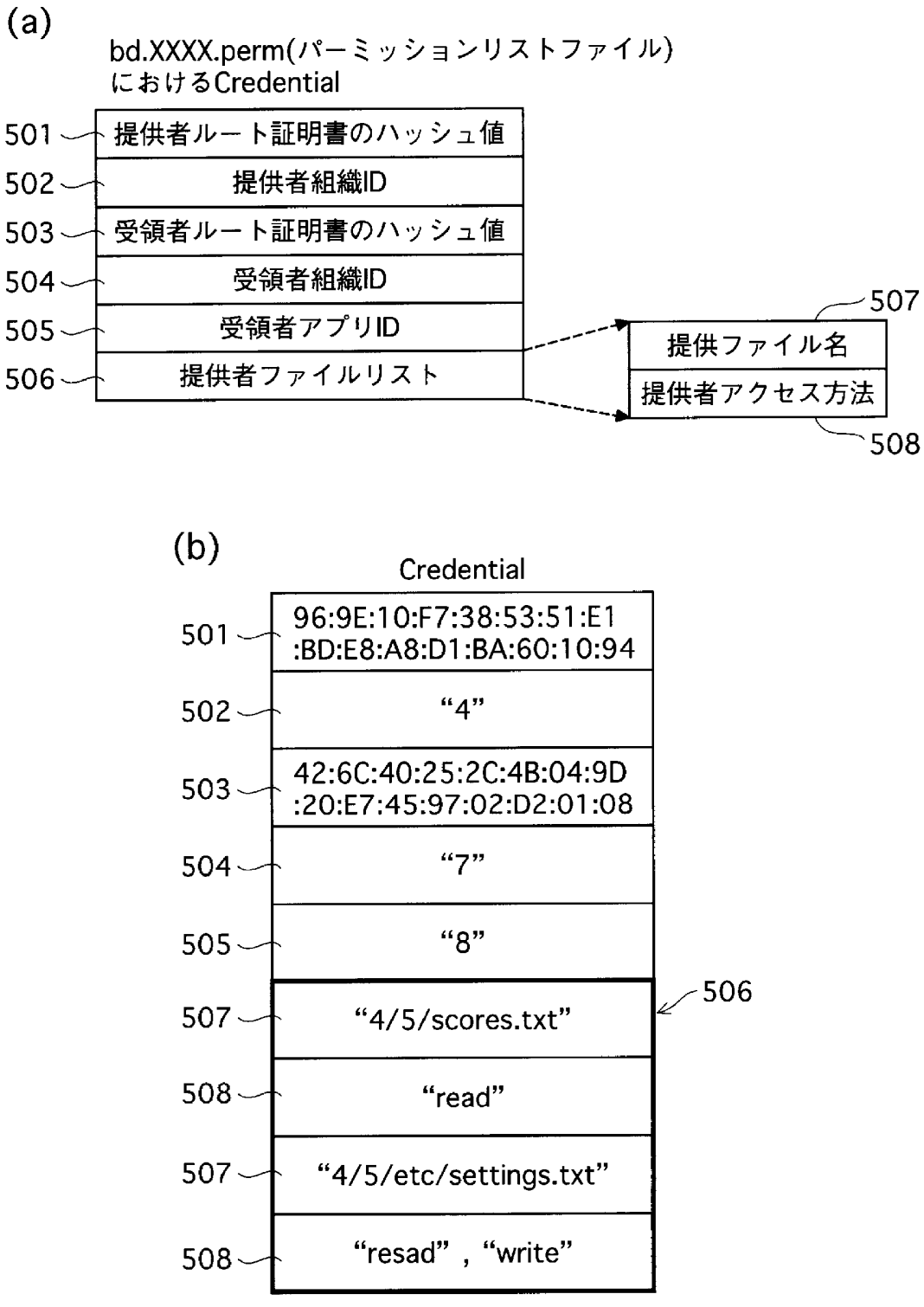
(a)


第3段目:
ROOT
BDDATA
XXX.JAR
302
BD.ROOT.CERTIFICATE
301
第2段目:
リードイン領域
論理アドレス空間
リードアウト領域
第1段目:
BCA
BD-ROM

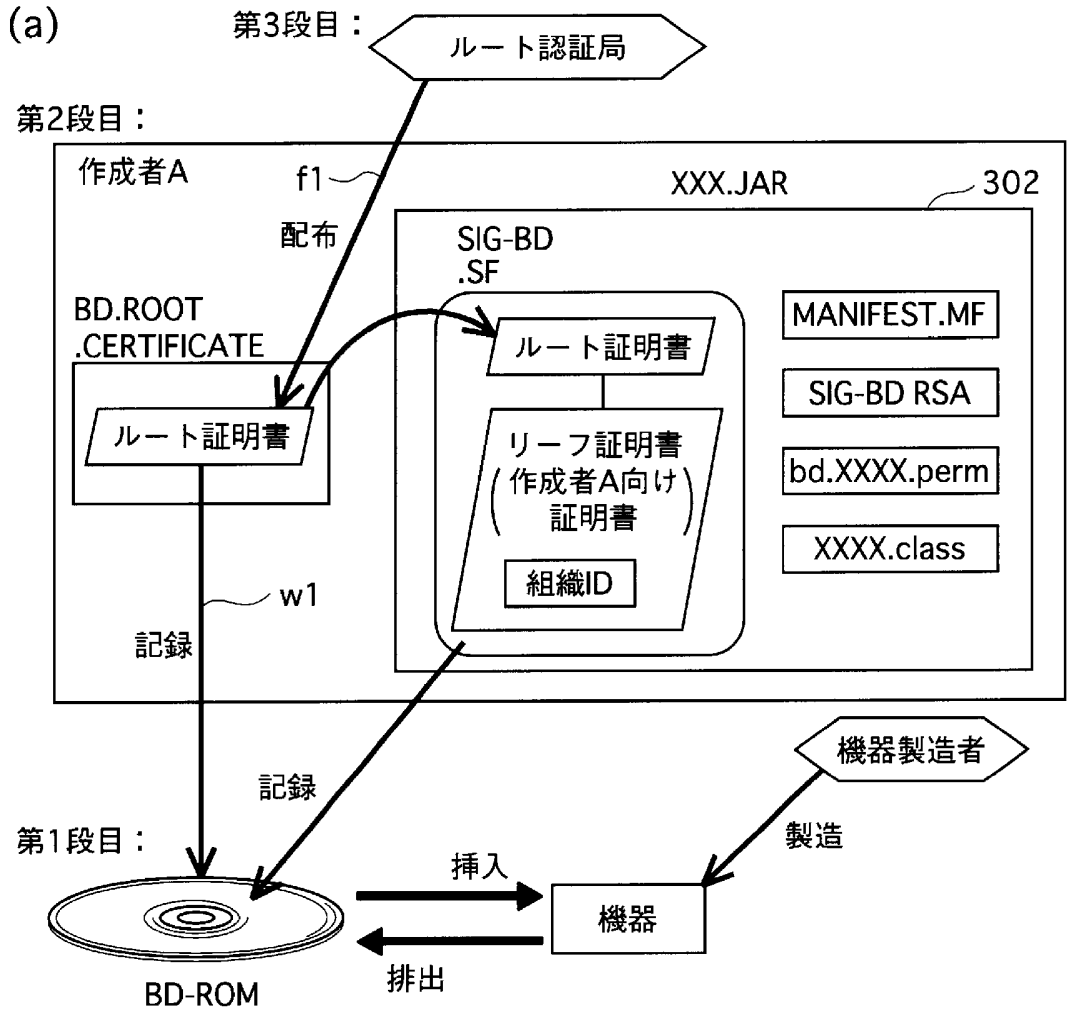
(b)

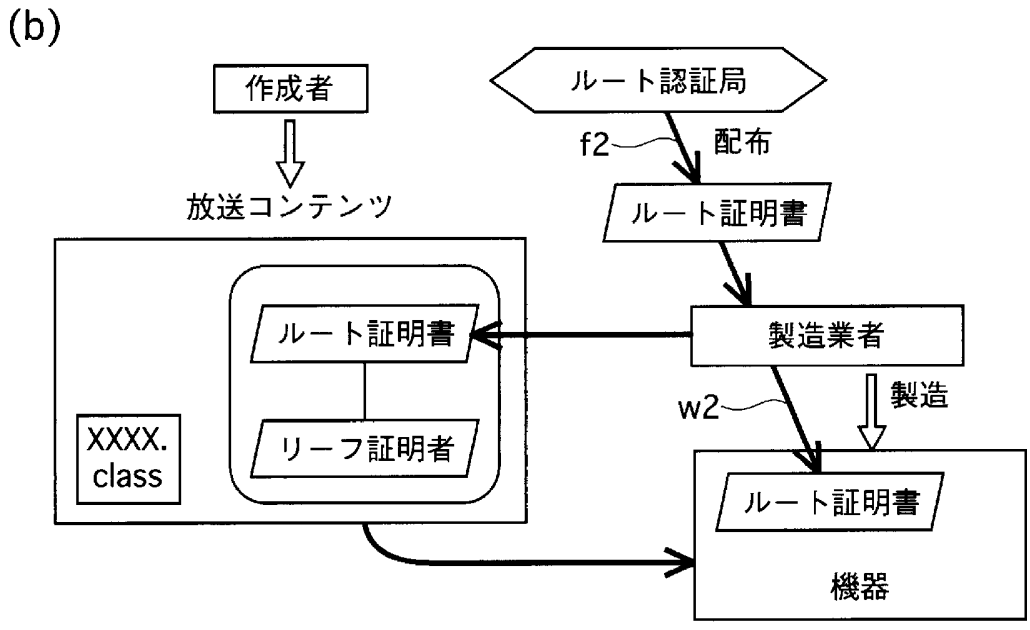

XXX.JAR
ROOT
META-INF
MANIFEST.MF
402
SIG-BD.SF
403
SIG-BD.RSA
404
bd.XXXX.perm
405
XXXX.class
401

[図2]

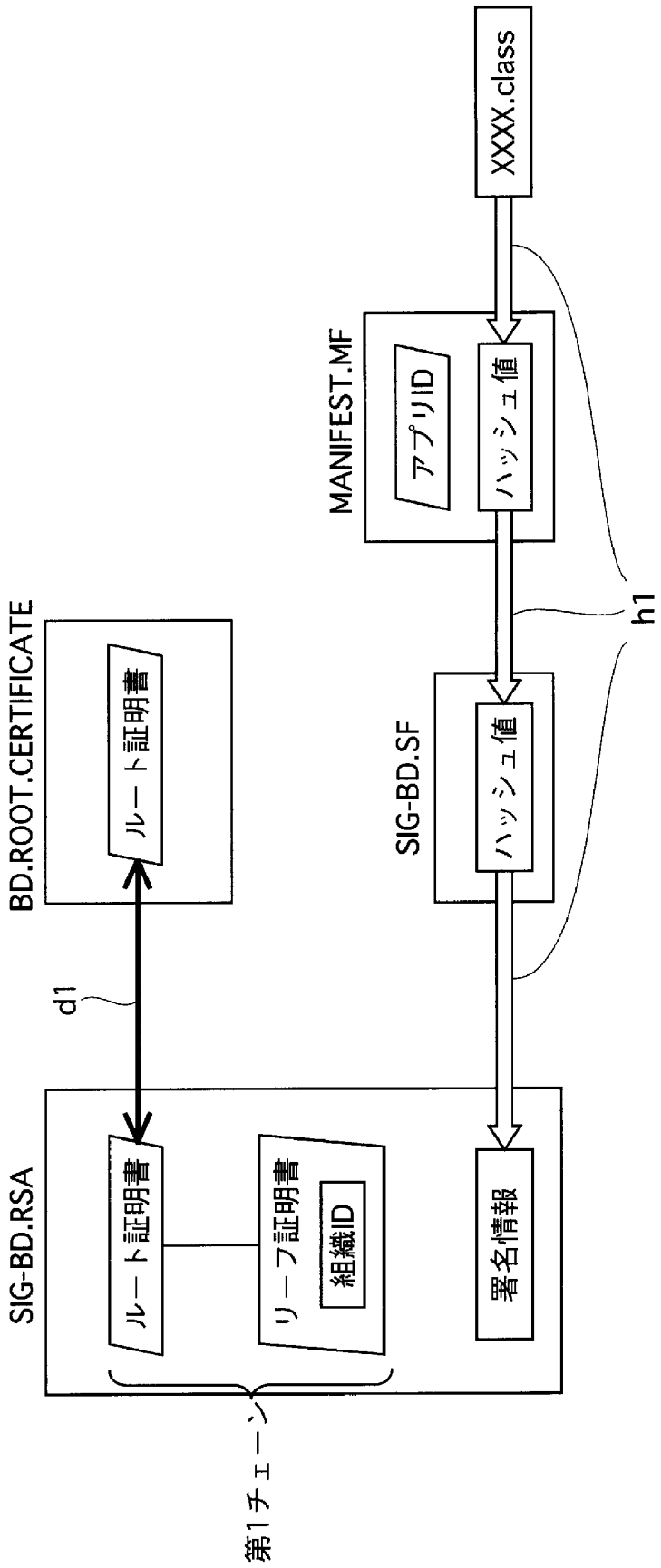

(a)
bd.XXXX.perm(パーミッションリストファイル)
におけるCredential
501
提供者ルート証明書のハッシュ値
502
提供者組織ID
503
受領者ルート証明書のハッシュ値
504
受領者組織ID
505
受領者アプリID
506
提供者ファイルリスト
507
提供ファイル名
提供者アクセス方法
508
(b)
Credential
501
96:9E:10:F7:38:53:51:E1
:BD:E8:A8:D1:BA:60:10:94
502
“4”
503
42:6C:40:25:2C:4B:04:9D
:20:E7:45:97:02:D2:01:08
504
“7”
505
“8”
507
“4/5/scores.txt”
506
508
“read”
507
“4/5/etc/settings.txt”
508
“resad” , “write”

[図3]

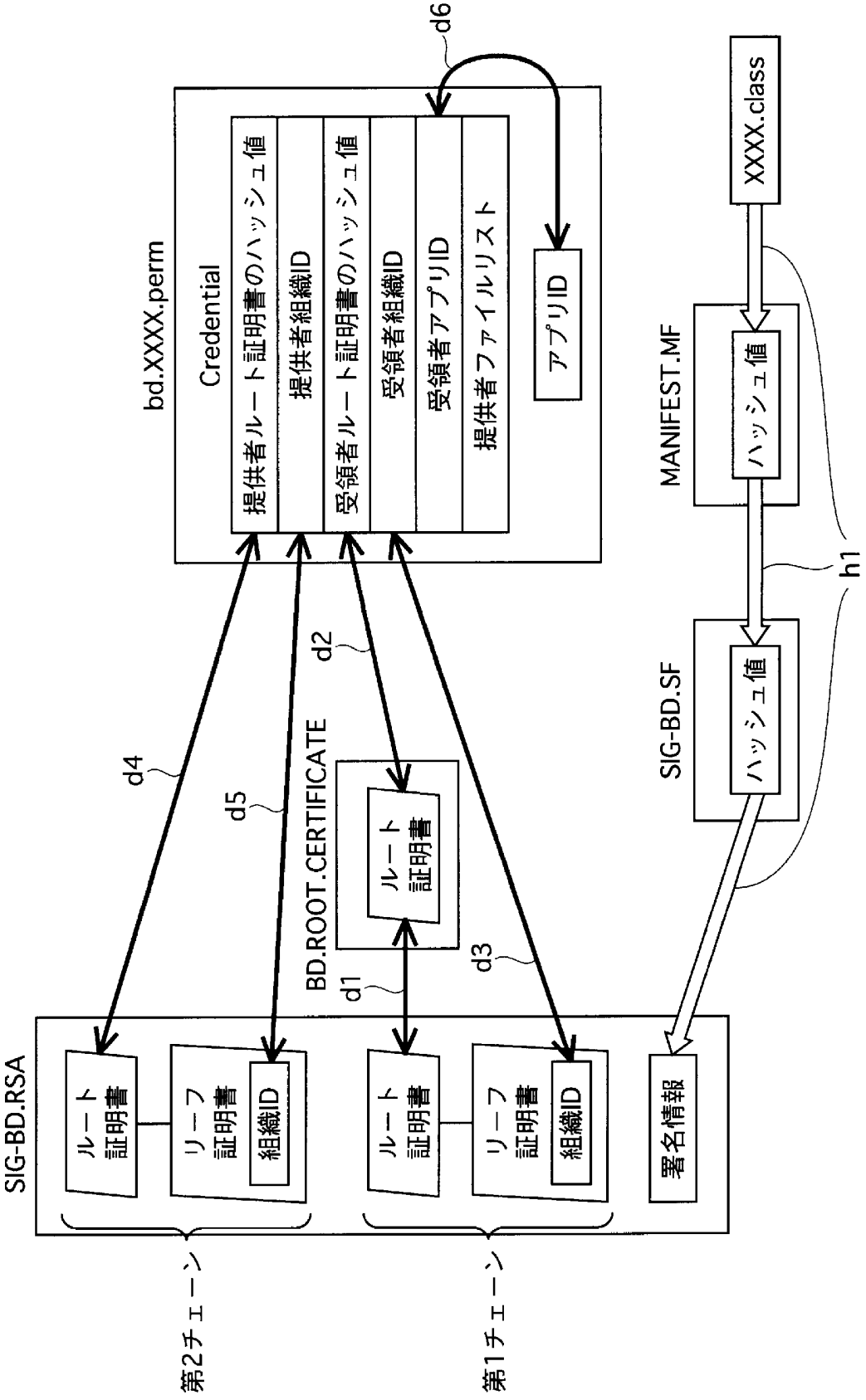

(a)
第3段目：
ルート認証局
第2段目：
作成者A
f1
配布
XXX.JAR
302
SIG-BD
.SF
BD.ROOT
.CERTIFICATE
ルート証明書
ルート証明書
リーフ証明書
(作成者A向け
証明書)
組織ID
MANIFEST.MF
SIG-BD RSA
bd.XXXX.perm
XXXX.class
w1
記録
記録
機器製造者
製造
第1段目：
挿入
機器
排出
BD-ROM


(b)
作成者
放送コンテンツ
ルート認証局
f2
配布
ルート証明書
ルート証明書
リーフ証明者
XXXX.
class
製造業者
w2
製造
ルート証明書
機器

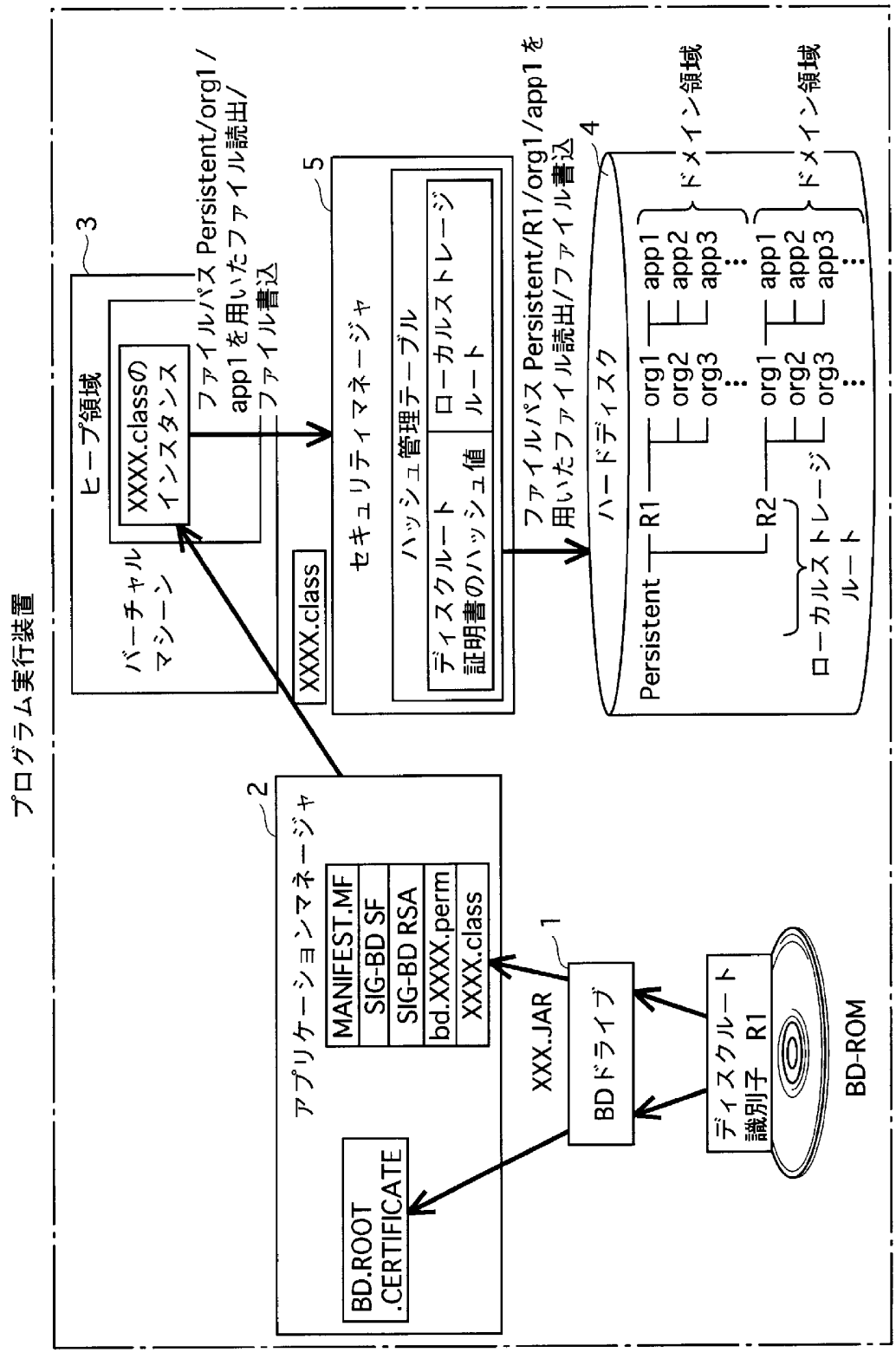
[図4]


XXXX.class
MANIFEST.MF
アプリID
ハッシュ値
h1
BD.ROOT.CERTIFICATE
ルート証明書
SIG-BD.SF
ハッシュ値
d1
SIG-BD.RSA
ルート証明書
リーフ証明書
組織ID
署名情報
第1チェーン

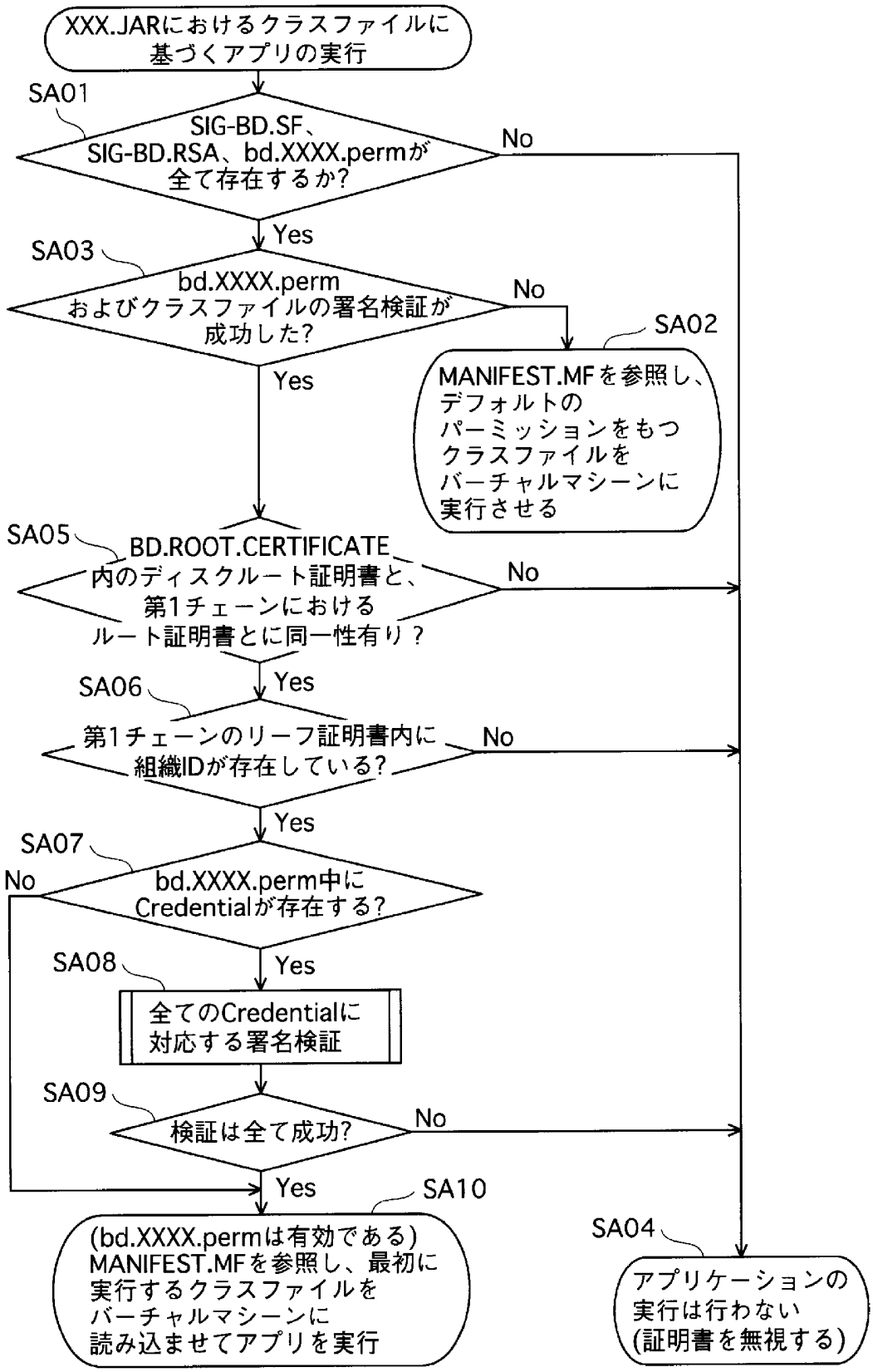
[図5]


d6
bd.XXXX.perm
Credential
提供者ルート証明書のハッシュ値
提供者組織ID
受領者ルート証明書のハッシュ値
受領者組織ID
受領者アプリID
提供者ファイルリスト
アプリID
XXXX.class
MANIFEST.MF
ハッシュ値
h1
SIG-BD.SF
ハッシュ値
d2
d4
d5
BD.ROOT.CERTIFICATE
ルート証明書
d1
d3
SIG-BD.RSA
ルート証明書
リーフ証明書
組織ID
ルート証明書
リーフ証明書
組織ID
署名情報
第2チェーン
第1チェーン

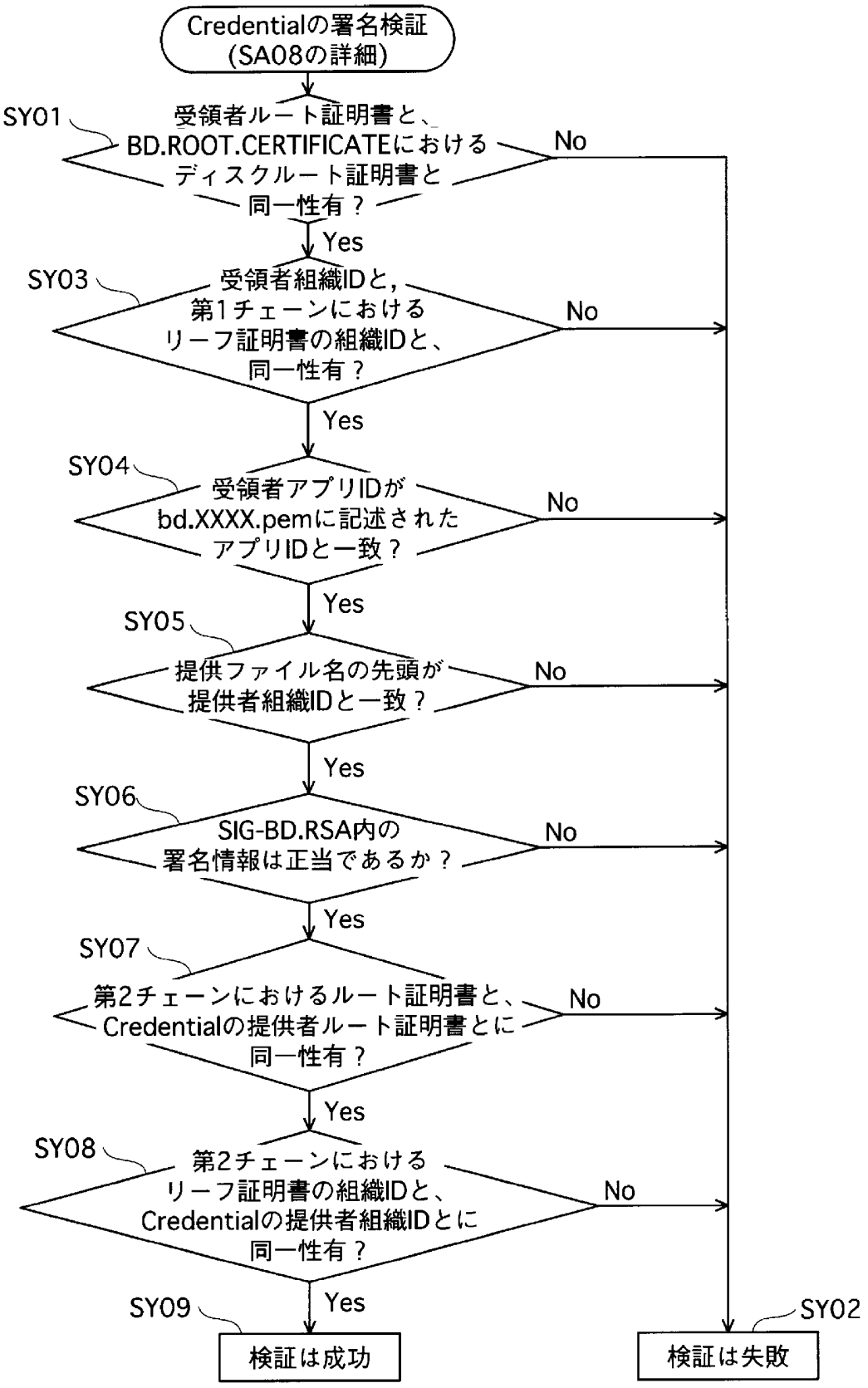
[図6]


プログラム実行装置
ヒープ領域
XXXX.classの
インスタンス
バーチャル
マシーン
3
ファイルパス Persistent/org1/
app1を用いたファイル読出/
ファイル書込
XXXX.class
セキュリティマネージャ
5
ハッシュ管理テーブル
ディスクルート
証明書のハッシュ値
ローカルストレージ
ルート
ファイルパス Persistent/R1/org1/app1を
用いたファイル読出/ファイル書込
4
ハードディスク
Persistent
R1
R2
org1
org2
org3
app1
app2
app3
ドメイン領域
ローカルストレージ
ルート
アプリケーションマネージャ
2
MANIFEST.MF
SIG-BD SF
SIG-BD RSA
bd.XXXX.perm
XXXX.class
BD.ROOT
.CERTIFICATE
XXX.JAR
1
BDドライブ
ディスクルート
識別子 R1
BD-ROM

[図7]


XXX.JARにおけるクラスファイルに基づくアプリの実行
SA01
SIG-BD.SF、SIG-BD.RSA、bd.XXXX.permが全て存在するか?
No
Yes
SA03
bd.XXXX.perm およびクラスファイルの署名検証が成功した?
No
Yes
SA02
MANIFEST.MFを参照し、デフォルトのパーミッションをもつクラスファイルをバーチャルマシーンに実行させる
SA05
BD.ROOT.CERTIFICATE内のディスクルート証明書と、第1チェーンにおけるルート証明書とに同一性有り?
No
Yes
SA06
第1チェーンのリーフ証明書内に組織IDが存在している?
No
Yes
SA07
No
bd.XXXX.perm中にCredentialが存在する?
Yes
SA08
全てのCredentialに対応する署名検証
SA09
検証は全て成功?
No
Yes
SA10
(bd.XXXX.permは有効である)MANIFEST.MFを参照し、最初に実行するクラスファイルをバーチャルマシーンに読み込ませてアプリを実行
SA04
アプリケーションの実行は行わない(証明書を無視する)

[図8]


Credentialの署名検証
(SA08の詳細)
SY01
受領者ルート証明書と、
BD.ROOT.CERTIFICATEにおける
ディスクルート証明書と
同一性有？
No
Yes
SY03
受領者組織IDと，
第1チェーンにおける
リーフ証明書の組織IDと、
同一性有？
No
Yes
SY04
受領者アプリIDが
bd.XXXX.pemに記述された
アプリIDと一致？
No
Yes
SY05
提供ファイル名の先頭が
提供者組織IDと一致？
No
Yes
SY06
SIG-BD.RSA内の
署名情報は正当であるか？
No
Yes
SY07
第2チェーンにおけるルート証明書と、
Credentialの提供者ルート証明書とに
同一性有？
No
Yes
SY08
第2チェーンにおける
リーフ証明書の組織IDと、
Credentialの提供者組織IDとに
同一性有？
No
Yes
SY09
検証は成功
SY02
検証は失敗

[図9]

アプリケーションマネージャーが保持する管理情報
パーションリクエストファイル(bd.XXXX.perm)

ディスクルート証明書	(X.509形式のファイル)	302

Jarファイル名	“0001.jar”	“0002.jar”
組織ID	“7”	なし
アプリID	“8”	“35”
アプリ間通信	“enable”	“disable”
Credential	Credential list	なし

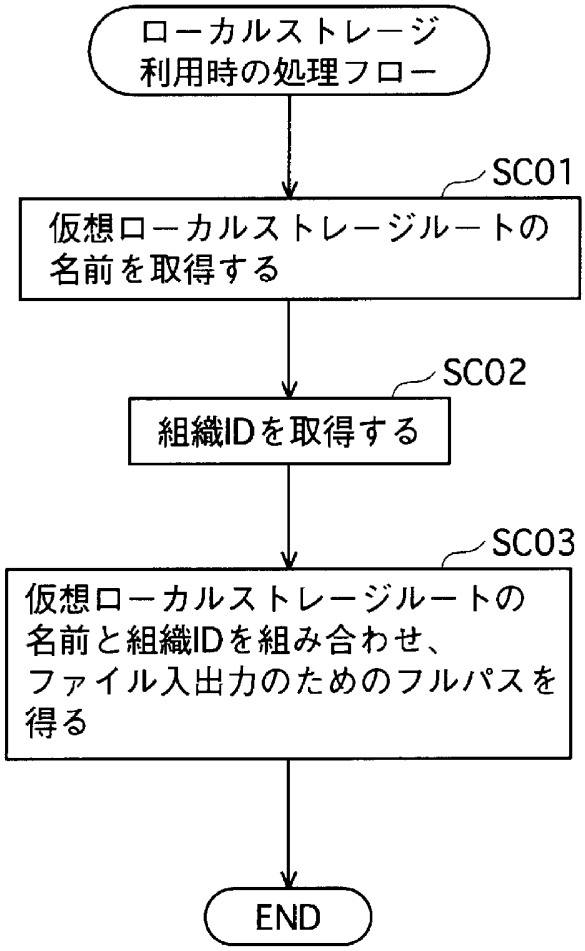
Credential list

[図10]

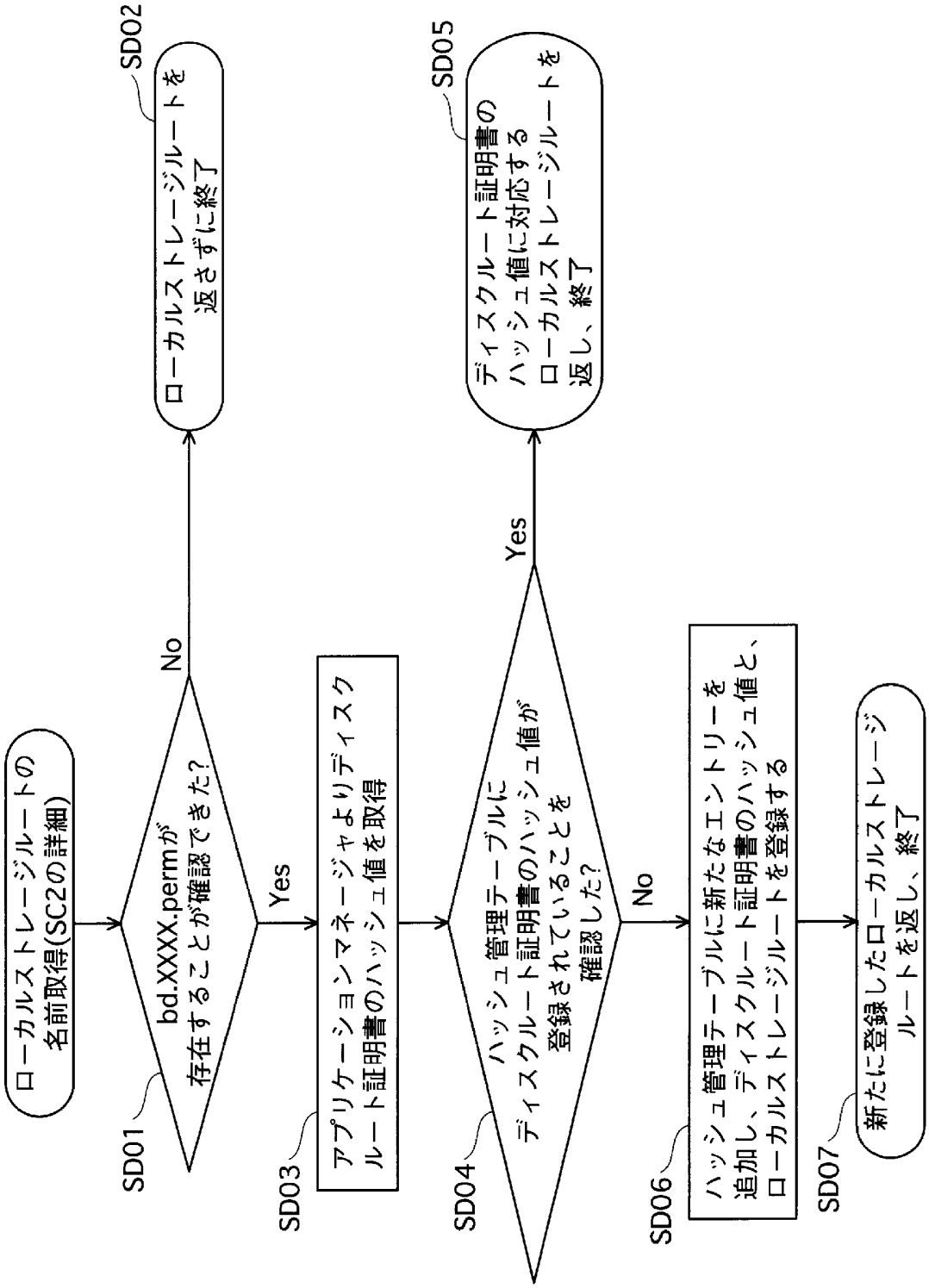
提供者ルート証明書ハッシュ値	96:9E:10:F7:38:53:51:E1 :BD:E8:A8:D1:BA:60:10:94	501
提供者組織ID	“4”	502
提供者ファイルリスト		506

提供ファイル名	“4/5/scores.txt”	“4/5/etc/settings.txt”	507
提供者アクセス方法	“read”	“resad” , “write”	508

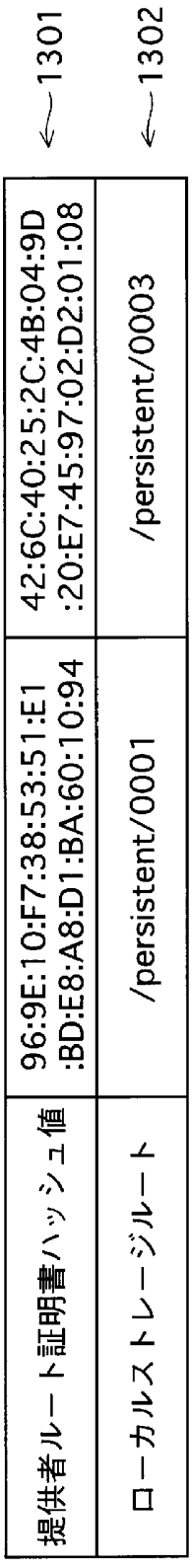
[図11]


ローカルストレージ
利用時の処理フロー
SC01
仮想ローカルストレージルートの
名前を取得する
SC02
組織IDを取得する
SC03
仮想ローカルストレージルートの
名前と組織IDを組み合わせ、
ファイル入出力のためのフルパスを
得る
END

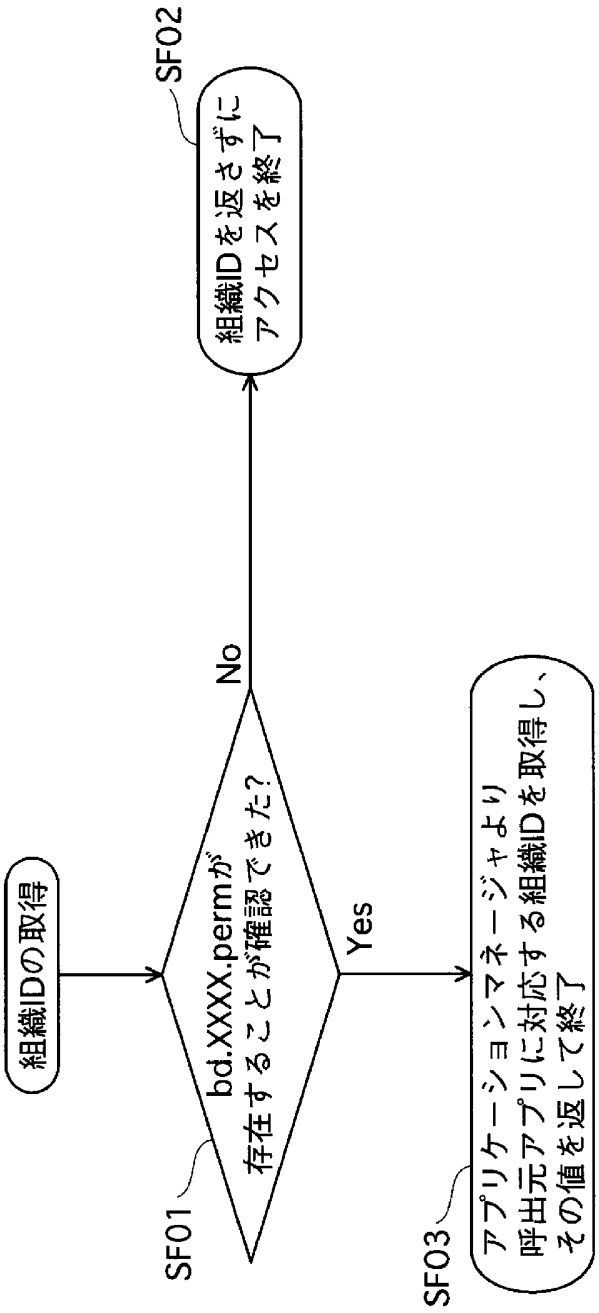
[図12]


ローカルストレージルートの
名前取得(SC2の詳細)
SD01
bd.XXXX.permが
存在することが確認できた?
No
SD02
ローカルストレージルートを
返さずに終了
Yes
SD03
アプリケーションマネージャよりディスク
ルート証明書のハッシュ値を取得
SD04
ハッシュ管理テーブルに
ディスクルート証明書のハッシュ値が
登録されていることを
確認した?
Yes
SD05
ディスクルート証明書の
ハッシュ値に対応する
ローカルストレージルートを
返し、終了
No
SD06
ハッシュ管理テーブルに新たなエントリーを
追加し、ディスクルート証明書のハッシュ値と、
ローカルストレージルートを登録する
SD07
新たに登録したローカルストレージ
ルートを返し、終了

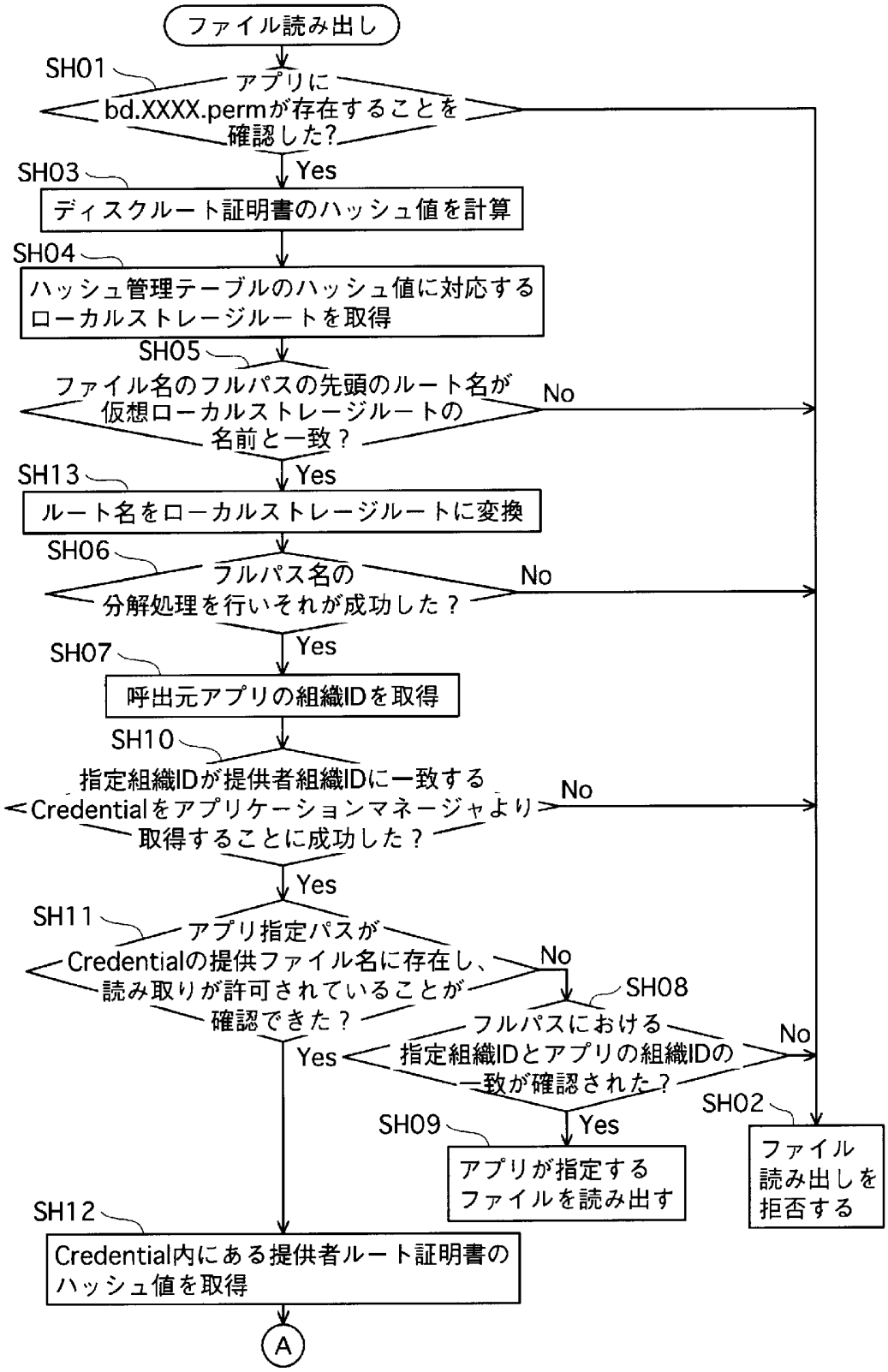
[図13]


セキュリティマネージャが保持するハッシュ管理テーブル
提供者ルート証明書ハッシュ値
ローカルストレージルート
96:9E:10:F7:38:53:51:E1
:BD:E8:A8:D1:BA:60:10:94
/persistent/0001
42:6C:40:25:2C:4B:04:9D
:20:E7:45:97:02:D2:01:08
/persistent/0003
1301
1302

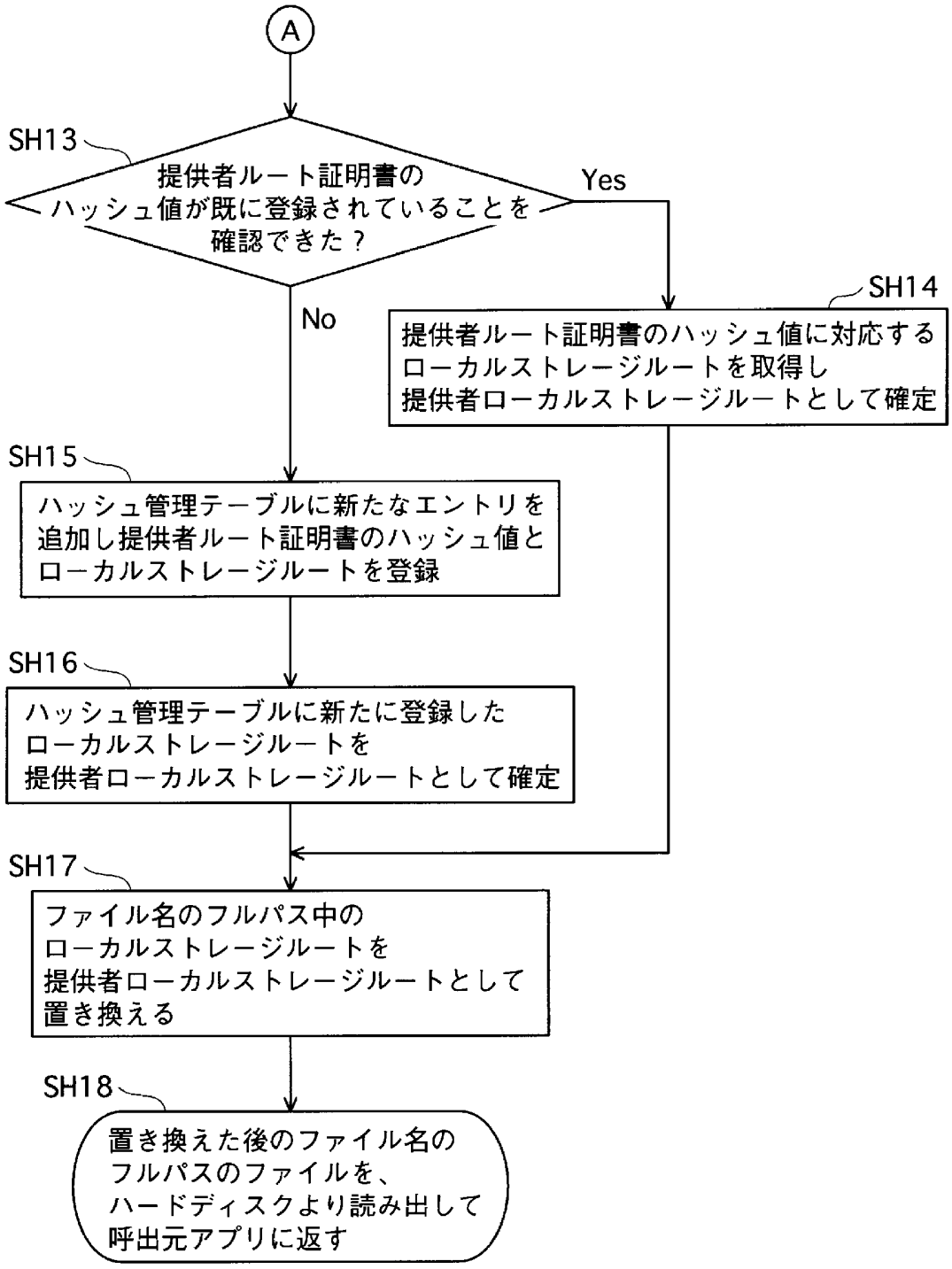
[図14]


組織IDの取得
SF01
bd.XXXX.permが
存在することが確認できた?
No
Yes
SF02
組織IDを返さずに
アクセスを終了
SF03
アプリケーションマネージャより
呼出元アプリに対応する組織IDを取得し、
その値を返して終了

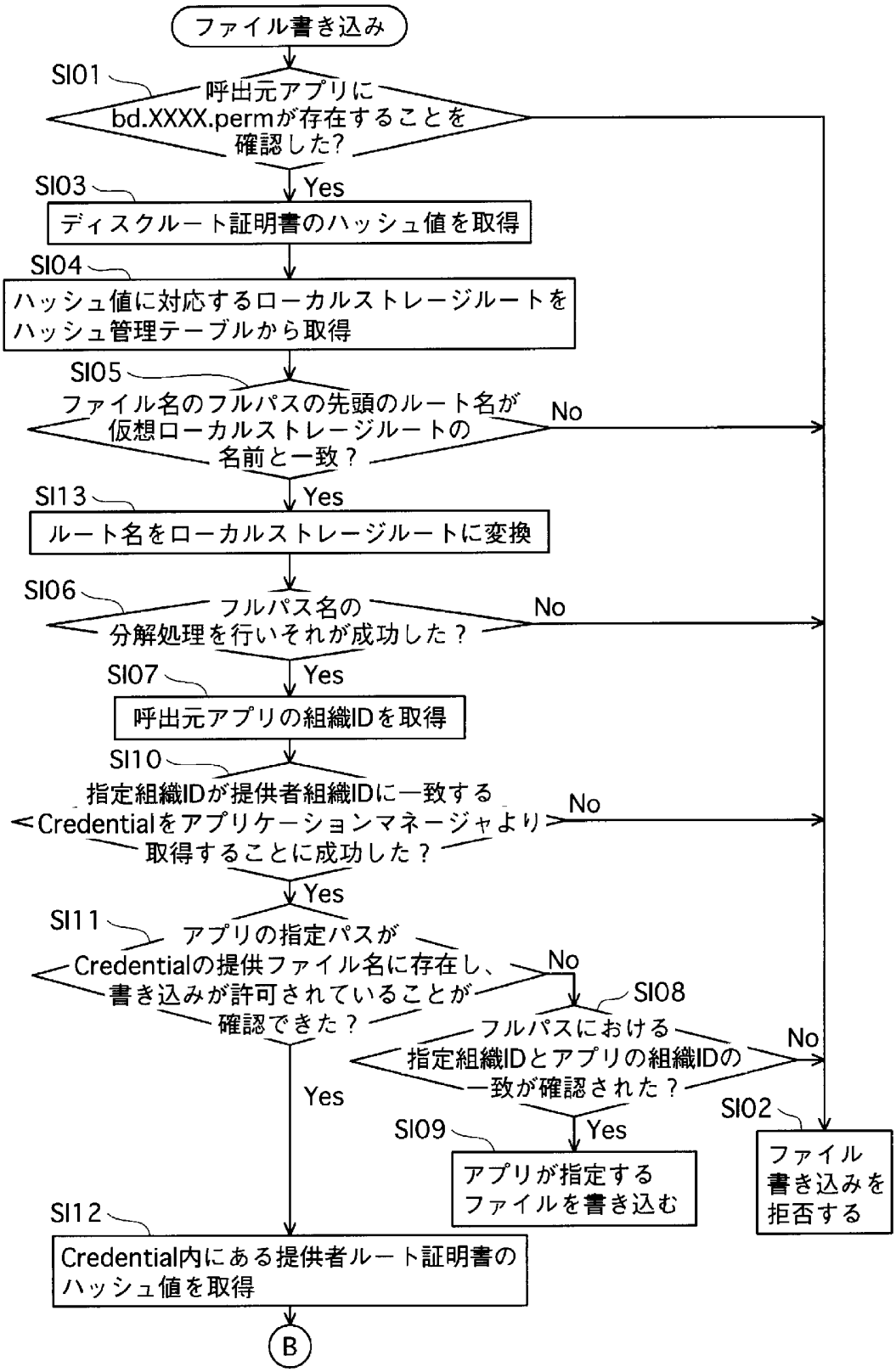
[図15]


ファイル読み出し
SH01
アプリに
bd.XXXX.permが存在することを
確認した?
Yes
SH03
ディスクルート証明書のハッシュ値を計算
SH04
ハッシュ管理テーブルのハッシュ値に対応する
ローカルストレージルートを取得
SH05
ファイル名のフルパスの先頭のルート名が
仮想ローカルストレージルートの
名前と一致?
No
Yes
SH13
ルート名をローカルストレージルートに変換
SH06
フルパス名の
分解処理を行いそれが成功した?
No
Yes
SH07
呼出元アプリの組織IDを取得
SH10
指定組織IDが提供者組織IDに一致する
Credentialをアプリケーションマネージャより
取得することに成功した?
No
Yes
SH11
アプリ指定パスが
Credentialの提供ファイル名に存在し、
読み取りが許可されていることが
確認できた?
No
SH08
フルパスにおける
指定組織IDとアプリの組織IDの
一致が確認された?
No
Yes
SH02
ファイル
読み出しを
拒否する
SH09
Yes
アプリが指定する
ファイルを読み出す
SH12
Credential内にある提供者ルート証明書の
ハッシュ値を取得
A

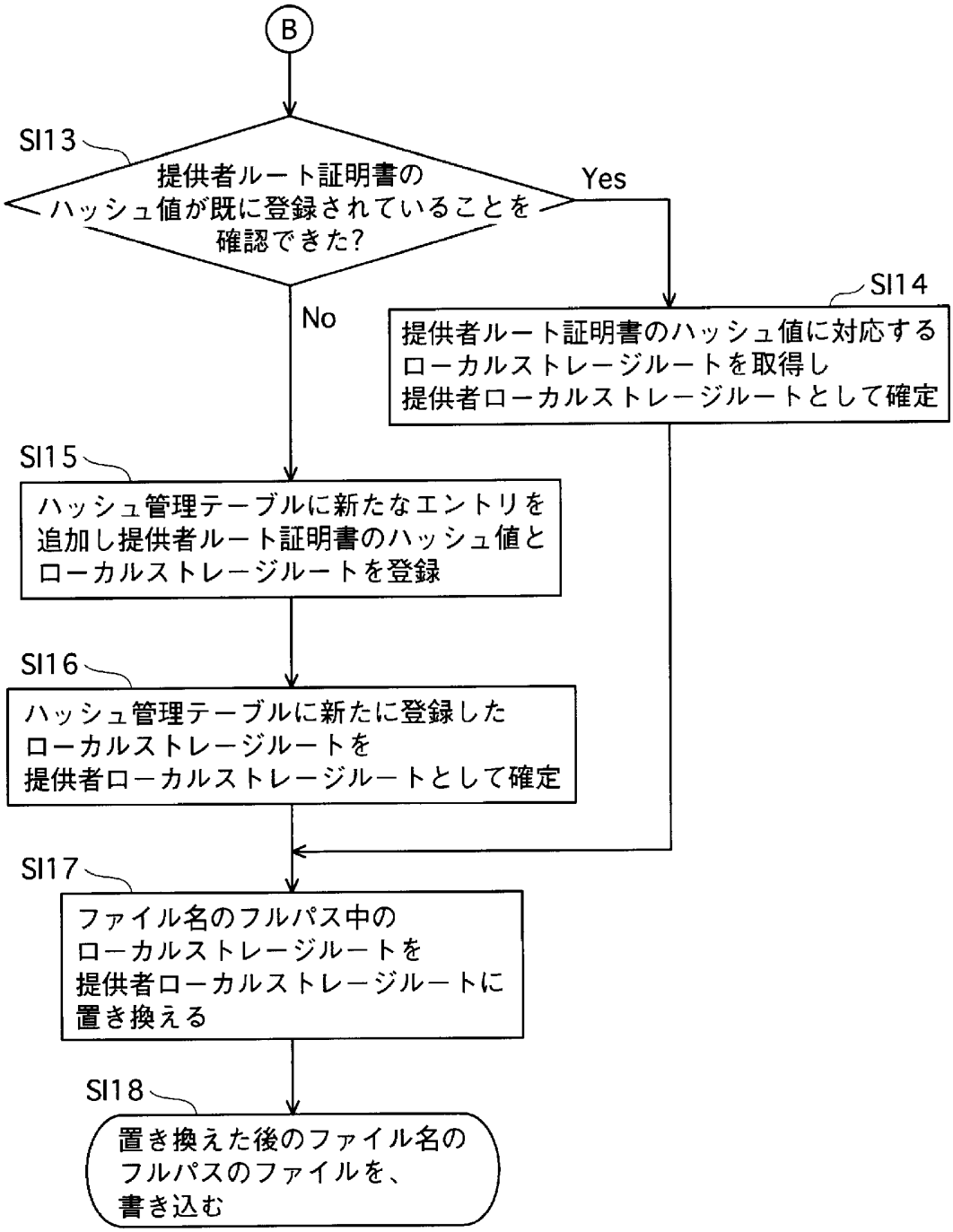
[図16]


A
SH13
提供者ルート証明書の
ハッシュ値が既に登録されていることを
確認できた？
Yes
No
SH14
提供者ルート証明書のハッシュ値に対応する
ローカルストレージルートを取得し
提供者ローカルストレージルートとして確定
SH15
ハッシュ管理テーブルに新たなエントリを
追加し提供者ルート証明書のハッシュ値と
ローカルストレージルートを登録
SH16
ハッシュ管理テーブルに新たに登録した
ローカルストレージルートを
提供者ローカルストレージルートとして確定
SH17
ファイル名のフルパス中の
ローカルストレージルートを
提供者ローカルストレージルートとして
置き換える
SH18
置き換えた後のファイル名の
フルパスのファイルを、
ハードディスクより読み出して
呼出元アプリに返す

[図17]


ファイル書き込み
SI01
呼出元アプリに
bd.XXXX.permが存在することを
確認した?
Yes
SI03
ディスクルート証明書のハッシュ値を取得
SI04
ハッシュ値に対応するローカルストレージルートを
ハッシュ管理テーブルから取得
SI05
ファイル名のフルパスの先頭のルート名が
仮想ローカルストレージルートの
名前と一致?
No
Yes
SI13
ルート名をローカルストレージルートに変換
SI06
フルパス名の
分解処理を行いそれが成功した?
No
Yes
SI07
呼出元アプリの組織IDを取得
SI10
指定組織IDが提供者組織IDに一致する
<Credentialをアプリケーションマネージャより
取得することに成功した?
No
Yes
SI11
アプリの指定パスが
Credentialの提供ファイル名に存在し、
書き込みが許可されていることが
確認できた?
No
SI08
フルパスにおける
指定組織IDとアプリの組織IDの
一致が確認された?
No
Yes
SI09
Yes
アプリが指定する
ファイルを書き込む
SI02
ファイル
書き込みを
拒否する
SI12
Credential内にある提供者ルート証明書の
ハッシュ値を取得
B

[図18]


B
SI13
提供者ルート証明書の
ハッシュ値が既に登録されていることを
確認できた?
Yes
No
SI14
提供者ルート証明書のハッシュ値に対応する
ローカルストレージルートを取得し
提供者ローカルストレージルートとして確定
SI15
ハッシュ管理テーブルに新たなエントリを
追加し提供者ルート証明書のハッシュ値と
ローカルストレージルートを登録
SI16
ハッシュ管理テーブルに新たに登録した
ローカルストレージルートを
提供者ローカルストレージルートとして確定
SI17
ファイル名のフルパス中の
ローカルストレージルートを
提供者ローカルストレージルートに
置き換える
SI18
置き換えた後のファイル名の
フルパスのファイルを、
書き込む

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/302448

A. CLASSIFICATION OF SUBJECT MATTER
G06F12/14(2006.01), ***G06F21/22***(2006.01), ***G06F21/24***(2006.01), ***G06Q10/00***(2006.01), ***G06Q30/00***(2006.01), ***G06Q50/00***(2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F12/14(2006.01), ***G06F21/22***(2006.01), ***G06F21/24***(2006.01), ***G06Q10/00***(2006.01), ***G06Q30/00***(2006.01), ***G06Q50/00***(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 10-83310 A (International Business Machines Corp.), 31 March, 1998 (31.03.98), Full text; all drawings & US 5825877 A1 & EP 813132 A2	1-10
A	JP 2004-302973 A (NTT Docomo Inc.), 28 October, 2004 (28.10.04), Full text; all drawings & US 2005/5099 A & EP 1465383 A1	1-10
A	JP 2005-524910 A (Sony Ericsson Mobile Communications Kabushiki Kaisha), 18 August, 2005 (18.08.05), Full text; all drawings (Family: none)	1-10

☐ 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
15 March, 2006 (15.03.06)	18 April, 2006 (18.04.06)
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／ＪＰ２００６／３０２４４８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*G06F12/14(2006.01)，G06F21/22(2006.01)，G06F21/24(2006.01)，G06Q10/00(2006.01)，G06Q30/00(2006.01)，G06Q50/00(2006.01)*

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　*G06F12/14(2006.01)，G06F21/22(2006.01)，G06F21/24(2006.01)，G06Q10/00(2006.01)，G06Q30/00(2006.01)，G06Q50/00(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 10-83310 A（インターナショナル・ビジネス・マシーンズ・コーポレイション）1998.03.31，全文全図 & US 5825877 A1 & EP 813132 A2	1-10
A	JP 2004-302973 A（株式会社エヌ・ティ・ティ・ドコモ）2004.10.28，全文全図 & US 2005/5099 A & EP 1465383 A1	1-10
A	JP 2005-524910 A（ソニー・エリクソン・モバイル・コミュニケーションズ）2005.08.18，全文全図　（ファミリ無し）	1-10

☐　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
１５．０３．２００６	１８．０４．２００６

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３３５０
永野　志保
電話番号　０３－３５８１－１１０１　内線　３５４６