(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
2023年12月28日(28.12.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/248474 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/60* (2013.01)
G06F 21/57 (2013.01)

(21) 国際出願番号： PCT/JP2022/025364

(22) 国際出願日： 2022年6月24日(24.06.2022)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

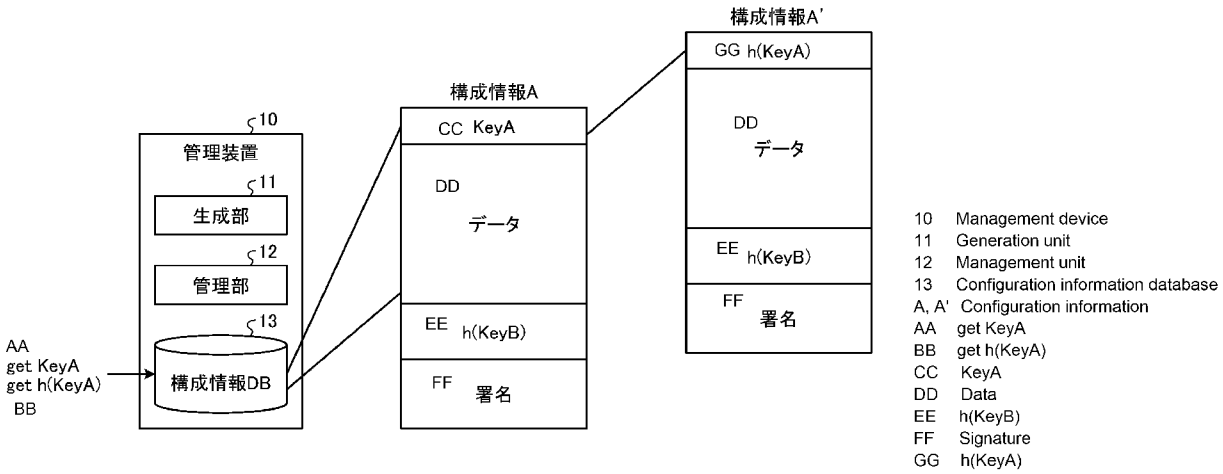
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 寺本 泰大 (**TERAMOTO, Yasuhiro**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 佐藤 亮太(**SATO, Ryota**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 和田 泰典(**WADA, Yasunori**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 伊藤 宏樹(**ITO, Hiroki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 中嶋 良彰(**NAKAJIMA, Yoshiaki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (**SAKAI INTERNATIONAL PATENT OFFICE**); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎の門三井ビルディング Tokyo (JP).

(54) **Title:** MANAGEMENT DEVICE, MANAGEMENT METHOD, AND MANAGEMENT PROGRAM

(54) 発明の名称： 管理装置、管理方法及び管理プログラム



(57) **Abstract:** A management device (10) comprises: a generation unit (11) that generates configuration information of a format obtained by adding, to data relating to first hardware or first software, a first identifier uniquely showing the first hardware or the first software, and a second identifier obtained by encoding a second identifier uniquely specifying another second hardware or second software constituting the first hardware or the first software by a one-way function, and an electronic signature to the data; and a management unit (12) that manages the configuration information.

(57) 要約：管理装置（１０）は、第１のハードウェアまたは第１のソフトウェアに関するデータに、第１のハードウェアまたは第１のソフトウェアを一意に示す第１の識別子と、第１のハードウェアまたは第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、データに対する電子署名と、を付加したフォーマットの構成情報を生成部（１１）と、構成情報を管理する管理部（１２）と、を有する。

WO 2023/248474 A1

［続葉有］

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

明　細　書

発明の名称 ： 管理装置、管理方法及び管理プログラム

技術分野

[0001] 本発明は、管理装置、管理方法及び管理プログラムに関する。

背景技術

[0002] サプライチェーンにおけるセキュリティリスクが高まっており、サプライチェーン全体の構成変化などの透明性を確保する必要がある。例えば、ライセンス管理や脆弱性管理のために、製品に含まれるソフトウェアコンポーネントや依存関係等を一覧化したSBoM（Software Bill of Materials）の普及が進んでおり、その重要性は高まっている。

[0003] SBoMの表現方法としては、SPDX、CycloneDX、SWIDなどのフォーマットなどが登場している。近年の製品開発は、単一のベンダーによって完結せず、複数のベンダーのサプライチェーンによって構成されることが多い。このため、SBoMには複数のベンダーによる構成情報が混在することになる。ここで、一つのSBoMファイルの中に全ての情報を記載することが多いが、CycloneDXなどは、外部のSBoM情報を参照するPedigreeなどの仕様を提供している。以降、SBoMのフォーマットを、総称して構成情報フォーマットと呼ぶ。

先行技術文献

非特許文献

[0004] 非特許文献1：日本電信電話株式会社及び日本電気株式会社, “NTTとNEC、情報通信インフラにおけるサプライチェーンセキュリティリスクへの対策技術を開発”, [online], [令和４年５月２７日検索], インターネット＜ＵＲＬ：https://group.ntt/jp/newsrelease/2021/10/27/211027b.html＞

発明の概要

発明が解決しようとする課題

[0005] この構成情報フォーマットの需要の高まりに反し、ソフトウェア構成情報などは、製造企業において最重要機密の一つでもあり、全てを納入先に開示

することは現実的ではない。

[0006] このため、例えば、納入先に情報の一部のみ開示する、納入先には情報を開示するがその納入先が製品を組み込んだ新たな製品を別企業に販売する時には情報を開示しない、などの、きめ細やかなアクセス制御が必要となる。しかしながら、従来のSBoM形式は、アクセス制御などの仕様を想定していないという問題があった。

[0007] これに類似する問題の解決として、Verifiable Credentialsのゼロ知識証明による署名が挙げられる。Verifiable Credentialsは、資格証明などの情報をデジタル化して第三者による検証を可能にしたものである。

[0008] Verifiable Credentialsでは、資格発行機関などが資格情報（電子ファイル）にデジタル署名した上でユーザーにファイルを渡し、ユーザーがその資格情報を証明したい時にはその電子ファイルを相手に提示する。この際、資格情報の中に相手に提示する必要のない情報が含まれていたとしても、署名付きのファイルを変更すると署名検証が不可能となるという問題があった。

[0009] この問題に対してゼロ知識証明（グループ署名）を用いて、ユーザーがフィールドの一部を除外したとしても、署名検証可能となる方式が存在する。しかしながら、この方式は、項目ごとに提示する、または、提示しない、の選択しかできないため、構成情報フォーマットには適していない。

[0010] 本発明は、上記に鑑みてなされたものであって、構成情報の円滑な署名検証を実現することができる管理装置、管理方法及び管理プログラムを提供することを目的とする。

課題を解決するための手段

[0011] 上述した課題を解決し、目的を達成するために、本発明に係る管理装置は、第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、前記第１のハードウェアまたは第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特

定する第２の識別子を一方向関数により符号化した第２の識別子と、前記データに対する電子署名と、を付加したフォーマットの構成情報を生成する生成部と、前記構成情報を管理する管理部と、を有することを特徴とする。

[0012] また、本発明に係る管理装置は、第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、前記第１のハードウェアまたは前記第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは前記第２のソフトウェアを一意に特定する第２の識別子と、構成情報全体の第１の電子署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する生成部と、前記構成情報を管理する管理部と、を有することを特徴とする。

[0013] また、本発明に係る管理装置は、第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、前記第１のハードウェアまたは第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、構成情報全体の第１の電子署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する生成部と、前記構成情報を管理する管理部と、を有することを特徴とする。

発明の効果

[0014] 本発明によれば、構成情報の円滑な署名検証を実現することができる。

図面の簡単な説明

[0015] [図1]図１は、構成情報の基本構造を説明する図である。

[図2]図２は、構成情報のフォーマットに求められる要件を説明する図である

。

[図3]図３は、従来の構成情報のフォーマットを説明する図である。

[図4]図４は、実施の形態に係る管理装置の構成の一例を模式的に示す図である。

[図5]図５は、生成部が生成する構成情報のフォーマットを説明する図である。

[図6]図６は、生成部が生成する構成情報のフォーマットを説明する図である。

[図7]図７は、生成部が生成する構成情報のフォーマットを説明する図である。

[図8]図８は、生成部が生成する構成情報のフォーマットを説明する図である。

[図9]図９は、実施の形態に係る管理処理の処理手順を示すフローチャートである。

[図10]図１０は、生成部が生成する構成情報のフォーマットの他の例を示す図である。

[図11]図１１は、生成部が生成する構成情報のフォーマットの他の例を示す図である。

[図12]図１２は、生成部が生成する構成情報のフォーマットの他の例を示す図である。

[図13]図１３は、プログラムが実行されることにより、管理装置が実現されるコンピュータの一例を示す図である。

発明を実施するための形態

[0016] 以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

[0017] ［実施の形態］

［構成情報の基本構造］

構成情報の基本構造について説明する。図１は、構成情報の基本構造を説明する図である。

[0018] 図１に示すように、構成情報には、キー（第１の識別子）と、データと、０個以上の外部キー（第２の識別子）と、署名情報とが含まれる。

[0019] キーは、この構成情報に対応する第１のハードウェアまたは第１のソフトウェアを一意に特定する識別子である。

[0020] 以降、自社製品、ソフトＡ，Ｂは、それぞれ別ファイルを想定する。ファイルは、提供時に全て渡すか、キーを指定すると構成情報をダウンロード可能なクラウドサービス等を想定する。

[0021] データ部分には、そのソフトに関する様々な情報が含まれる。例えば、データ部分には、ライセンス、リスク調査情報、動作仕様、等が含まれる。

[0022] 外部キーは、第１のハードウェアまたは第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを、一意に特定する識別子である。外部キーは、その製品（機器、ソフト）が組み込んでいる別の機器及び／またはソフトの構成情報の識別子であり、有向非巡回グラフを構成する。

[0023] ［要件］

次に、構成情報のフォーマットに求められる要件について説明する。図２は、構成情報のフォーマットに求められる要件を説明する図である。

[0024] サプライチェーンの透明性と機密性と完全性とを確保するために、構成情報のフォーマットに対して下記の要件を満たすことが求められる。

[0025] 必須要件は、署名で有効性を検証可能なこと（完全性）である。

[0026] 要件１は、依存先ライブラリ情報を秘匿可能なことである。要件１は、要件１－１，１－２を含む。

[0027] 要件１－１は、依存先ライブラリを秘匿したとしても、言い換えると、リンク情報を非開示としたとしても、リンク情報が失われないことである（図２の（１），（２））。

[0028] 要件１－２は、提供された構成情報（リンク）を秘匿可能なこと、言い換

えると、提供されたソフトＡ，Ｂの構成情報を署名の有効性を保ったまま一部秘匿可能なことである（図２の（３））。例えばライセンスで構成情報の再配布が禁止されている場合などが該当する。

[0029] 要件２は、構成情報のデータに開示可能なレベルを設定できること（オプション）である。要件２は、要件２－１．２－２を含む。

[0030] 要件２－１は、より高いレベルのデータが後から提供された時に、同じソフトウェアの構成情報であることを検証可能なことである。

[0031] 要件２－２は、提供された構成情報（データ）の秘匿レベルを上げられることである。

[0032] 要件１と要件２とは独立の要件である。

[0033] ［従来技術］

次に、従来技術について説明する。図３は、従来の構成情報のフォーマットを説明する図である。

[0034] 図３に示すように、従来の構成情報フォーマットの構成では、外部キーを削除した場合は依存先ソフトへのリンク情報そのものが欠落し（図３の（１））、要件１を満たすことができない。

[0035] 一般的な署名技術を利用する場合、提供された構成情報（リンクやデータ）を書き換えると署名の検証ができなくなり（図３の（２））、要件１，２を満たすことができない。この際、グループ署名を用いることによって、一部項目の削除は可能となるが、項目ごとに提示する、または、提示しない、の選択しかできないという問題が解決できなくなる。

[0036] ［実施の形態に係る管理装置］

本実施の形態に係る管理装置は、要件１及び／または要件２を満たす構成情報を生成し、管理する。

[0037] 実施の形態に係る管理装置について説明する。図４は、実施の形態に係る管理装置の構成の一例を模式的に示す図である。

[0038] 実施の形態に係る管理装置１０は、例えば、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、ＣＰＵ（Central Processing Un

it）等を含むコンピュータ等に所定のプログラムが読み込まれて、ＣＰＵが所定のプログラムを実行することで実現される。また、管理装置１０は、ネットワーク等を介して接続された他の装置との間で、各種情報を送受信する通信インタフェースを有する。管理装置１０は、ワークステーションやパソコン等の汎用コンピュータで実現される。管理装置１０は、図４に示すように、生成部１１と、管理部１２と、構成情報を記憶する構成情報データベース（ＤＢ）１３とを有する。

[0039] 生成部１１は、要件１及び／または要件２を満たすフォーマットの構成情報を生成し、構成情報ＤＢ１３に格納する。図５～図８は、生成部１１が生成する構成情報のフォーマットを説明する図である。

[0040] 図５に示すように、実施の形態では、まず、キーから、一方向関数により符号化した「h（キー）」を非開示キーとして生成し、キーを「h（キー）（h（外部キー）含む）」に変換した状態で署名する構成情報のフォーマットＦ１，Ｆ２を提案する。

[0041] 具体的には、生成部１１は、「外部キー」（第２の識別子）をハッシュ化し（図５の（１））、キー（第１の識別子）、ヘッダ、データ、「h（外部キー）」（符号化した第２の識別子）に、データに対する電子署名を付加したフォーマットＦ１で構成情報を生成する。

[0042] ここで、「ID」を保有していれば、「h（ID）」を生成可能だが、「h（ID）」のみからではIDは生成困難となるため、ハッシュ化することによってIDを秘匿することができる。したがって、フォーマットＦ１によれば、外部キーをハッシュ化することで、キーから外部キーへのリンク情報を保持かつ秘匿することを可能とする。

[0043] そして、生成部１１は、フォーマットＦ１の参照先の構成情報として、キーである「h（キー）」、ヘッダ、データ、「h（外部キー）」に、データに対する電子署名を付加したフォーマットＦ２で構成情報を生成する。すなわち、生成部１１は、キー（第１の識別子）に代えて、キーを一方向関数により符号化したキーを、データに付加したフォーマットＦ２の構成情報を生成

する。

[0044] したがって、フォーマットＦ２によれば、キー及び外部キーをハッシュ化することで、ハッシュ化前のキーと、外部キーへのリンク情報とを、保持かつ秘匿することを可能とする。なお、ハッシュ化は、符号化の一例であり、キーまたは外部キーを秘匿化することができれば、ハッシュ化以外の符号化を用いてもよい。

[0045] 例えば、図６に示すように、構成情報Ａ（KeyA）と構成情報Ｂ（KeyB）とがリンクし、構成情報Ｂと構成情報Ｃ（KeyC）とがリンクしている場合を例に説明する。

[0046] 構成情報Ａには、外部キーとして「h（KeyB）」が付されている。構成情報Ａからの構成情報Ｂのリンクを秘匿した場合であっても、構成情報Ｂの情報を後から入手した場合、「KeyB」から「h（KeyB）」の変換は可能となる（図６の（１））。構成情報Ａが、構成情報Ｂ´にリンクしていることを確認することができる（図６の矢印Ｙ１１）。

[0047] また、「h（KeyB）」をキーとして検索することで、構成情報Ｂの情報を秘匿したまま、構成情報Ａが、構成情報Ｂ´を介して、構成情報Ｃにリンクしていることを確認することができる。構成情報Ｂ´には、外部キーとして「KeyC」が記載されるため、構成情報Ａから、構成情報Ｂ´を介して、構成情報Ｃにリンクしていることを提示可能である（図６の矢印Ｙ１１，Ｙ１２）。例えば、脆弱性のソフトウェア検査の時に、該当するソフトウェアまでのリンクを秘匿したまま、そのソフトウェアが含まれることを提示できる。

[0048] このように、フォーマットＦ１，Ｆ２は、要件１を満たす。したがって、生成部１１は、フォーマットＦ１，Ｆ２を採用することで、リンク情報を失わず署名検証可能、かつ、後からキーを非開示化可能なリンク構造を有する構成情報を生成することができる。

[0049] 図５に戻り説明を続ける。生成部１１は、構成情報に対し、開示部署名（第２の電子署名）と非開示部署名（第１の電子署名）との２つの署名を生成し、生成した２つの署名を付与する署名方式を採用する。

[0050] 非開示部署名は、構成情報全体（キー、ヘッダ、データ、h（外部キー））の署名である（図５の矢印Ｙ１）。開示部署名は、一部の項目（例えば、データ全体）が秘匿された構成情報（例えば、キー、ヘッダ、外部キー）と、開示部署名とを基に、生成される（図５の矢印Ｙ２）。

[0051] このように、生成部１１は、一つの構成情報に対して、開示部署名と非開示部署名との２つの署名を生成する。このうち、開示部署名は、外部キー及び開示部署名を基に署名検証が可能であり（図５の（２））、データ部を必ずしも必要としない。このため、生成部１１は、フォーマットＦ１，Ｆ２を採用することによって、フォーマットＦ２に示すように、構成情報のデータ部を後から削除することも可能である。

[0052] 例えば、生成した構成情報（フォーマットＦ０）のキー及び外部キーを、ハッシュ化により秘匿化した「h（キー）」及び「h（外部キー）」に置換した場合であっても（図７の（１））、生成した構成情報（フォーマットＦ０）と、秘匿化後の構成情報（フォーマットＦ２）とは、開示部署名同士、及び／または、非開示部署名同士を検証することで、同一の署名で検証可能である（図７の（２））。したがって、単一の署名情報によって、秘匿されていない構成情報（フォーマットＦ０）と、秘匿された構成情報（フォーマットＦ２）との双方を検証可能となる。

[0053] このように、フォーマットＦ１，Ｆ２は、要件２を満たす。したがって、生成部１１は、フォーマットＦ１，Ｆ２を採用することで、一つの構成情報に、開示部署名と非開示部署名との２つを署名することで、データ部を後から削除することを可能とする。

[0054] また、このフォーマットＦ１，Ｆ２によれば、一定のルールに基づいて、データの一部のみの非開示化や、複数署名の付与による秘匿レベルのレベル分けも可能である。

[0055] 例えば、生成部１１は、データの一部項目のみを秘匿化する非開示部署名を、構成情報に付与してもよい。また、生成部１１は、例えば、データ全体を秘匿化する非開示部署名１と、データの一部項目を秘匿化する非開示部署

名２との２つの非開示部署名を構成情報に付与してもよい。

[0056] 管理装置１０では、各非開示部署名の秘匿化対象のデータの項目数をそれぞれ設定することで、構成情報のデータへの開示可能なレベルを設定することができる。言い換えると、生成部１１は、段階的に項目を削除した各構成情報から生成した複数の電子署名を付与することによって、データの段階的な項目の秘匿化が可能である。また、フォーマットＦ１，Ｆ２によれば、グループ署名との組み合わせも可能である。

[0057] なお、生成部１１は、構成情報のフォーマットとして、要件１を満たすフォーマットＦ１´，Ｆ２´、及び／または、要件２を満たすフォーマットＦ２´を採用してもよい（図８参照）。

[0058] フォーマットＦ１´は、構成情報の外部キーをハッシュ化により秘匿した構成であり、フォーマットＦ２´は、キーをハッシュ化により秘匿化した構成である。また、生成部１１は、構成情報のフォーマットとして、要件２を満たすフォーマットＦ０を採用してもよい（図７参照）。

[0059] このように、管理装置１０は、フォーマットＦ１，Ｆ１´，Ｆ２，Ｆ２´を採用することによって、秘匿した構成情報を開示せずに、他のハードウェアまたはソフトウェアが、さらに構成するハードウェアまたはソフトウェアへの情報を開示することが可能であり、事前に生成した電子署名により検証が可能である。また、管理装置１０は、フォーマットＦ１，Ｆ２を採用することによって、構成情報のデータに開示可能なレベルを設定できる。

[0060] 管理部１２は、構成情報ＤＢ１３に格納された構成情報を管理する。管理部１２は、Key、または、h（Key）をクエリのキーと受けると、キーに対応する構成情報を、構成情報ＤＢ１３から取得する。

[0061] 例えば、図４に示すように、管理部１２は、クエリのキーとして「KeyA」を受け付けた場合、「KeyA」をキーとして構成情報Ａを取得する。また、管理部１２は、クエリのキーとして「h（KeyA）」を受け付けた場合、「h（KeyA）」をキーとして構成情報Ａ´を取得する。管理部１２は、キーが不明である場合には、構成情報にアクセスできないように、各構成情報を管理してい

る。

[0062] 構成情報の要求元は、「KeyA」が分かれば、「h（KeyA）」をハッシュ化により生成可能なため、「h（KeyA）」の情報も取得することができるが、その逆は不可能である。

[0063] ［処理手順］

図９は、実施の形態に係る管理処理の処理手順を示すフローチャートである。

[0064] 図９に示すように、管理装置１０では、生成部１１が、フォーマットＦ１，Ｆ１´，Ｆ２，Ｆ２´の構成情報を生成し、生成した構成情報を構成情報ＤＢ１３に格納する生成処理を行う（ステップＳ１）。

[0065] 管理部１２は、構成情報ＤＢ１３に格納された構成情報を管理する管理処理を行う（ステップＳ２）。管理部１２は、「Key」、または、「h（Key）」をクエリのキーと受けると、キーに対応する構成情報を、構成情報ＤＢ１３から取得し、要求元に出力する。

[0066] ［実施の形態の効果］

実施の形態に係る管理装置１０は、「外部キー」をハッシュ化し、キー、ヘッダ、データ、「h（外部キー）」に、データに対する電子署名を付加したフォーマットの構成情報を生成することで、署名を用いて構成情報の有効性を検証可能とするとともに、リンク構造を維持したまま情報を秘匿可能とすることが可能となる。

[0067] また、管理装置１０は、構成情報に対し、開示部署名と非開示部署名との２つの署名を生成し、生成した２つの署名を付与する署名方式を採用することによって、署名を用いて構成情報の有効性を検証可能とするとともに、データ部に対する後からの削除や開示のレベル分けを可能とする。

[0068] したがって、管理装置１０によれば、サプライチェーンの透明性と機密性と完全性とを確保可能であるフォーマットの構成情報を生成及び管理することができる。

[0069] ［変形例１］

図１０は、生成部１１が生成する構成情報のフォーマットの他の例を示す図である。図１０に示すように、ハッシュ化の回数を１回、２回、２回以上のように変えることで秘匿レベルを複数段階で定義することも可能である。

[0070] 例えば、生成部１１は、図６でも例示したように、キーが「h（KeyB）」であり、外部キーとして「KeyC」を記載した構成情報Ｂ１を生成してもよい。この構成情報Ｂ１を介して、構成情報Ａから構成情報Ｃにリンクしていることを提示可能である（図１０の矢印Ｙ２１，Ｙ２２）。

[0071] さらに、生成部１１は、「KeyA」を１回ハッシュ化した「h（KeyA）」をキーとし、外部キーとして、「KeyB」を２回ハッシュ化した「h（h（KeyB））」を記載した構成情報Ａ１を生成する。生成部１１は、「KeyB」を２回ハッシュ化した「h（h（KeyB））」をキーとし、外部キーとして、「KeyC」を２回ハッシュ化した「h（h（KeyC））」を記載した構成情報Ｂ２を生成する。そして、生成部１１は、「KeyC」を２回ハッシュ化した「h（h（KeyC））」をキーとした構成情報Ｃ２を生成する。この場合には、構成情報Ｂ２を介して、構成情報Ａ１から構成情報Ｃ２にリンクしていることを提示できる（図１０の矢印Ｙ２３，Ｙ２４）。

[0072] このように、キー及び／または外部キーのハッシュ化の回数を多くすることで、構成情報の秘匿レベルを高くすることも可能である。したがって、キー及び／または外部キーのハッシュ化の回数を調整することで秘匿レベルも調整することができる。キー及び／または外部キーの秘匿レベル（ハッシュ化の回数）は、ユーザー自身が定義してもよいし、特定の共通仕様に応じて適宜定義してもよい。

[0073] ［変形例２］

図１１及び図１２は、生成部１１が生成する構成情報のフォーマットの他の例を示す図である。

[0074] 構成情報に、ライセンス情報や上位の秘匿レベルへのアップグレード手順（URL等）を内包することで、開示された情報に対して、後から、より秘匿レベルの高い情報を確認することが可能になる。

[0075] 例えば、図１１に示すように、構成情報Ａ３（第１の構成情報）が、ハッシュ化した外部キー「h（KeyB）」と、アップグレード手順（第３の構成情報から第２の構成情報を取得するための方法）とを含む。

[0076] この場合、構成情報Ａ３の外部キー「h（KeyB）」をクエリのキーとして、「h（KeyB）」をキーとして有する構成情報Ｂ３（第３の構成情報）を取得する（図１１の矢印Ｙ３１）。

[0077] この際、構成情報Ａ３から、外部キー「h（KeyB）」とともにアップグレード手順を取得できるため、「h（KeyB）」をアップグレードすることで（図１１の（１））、「KeyB」を取得できる。そして、「KeyB」をキーとすることで、構成情報Ｂ３より秘匿レベルの高い構成情報Ｂ（第２の構成情報）の取得が可能となる。

[0078] また、図１２に示すように、構成情報Ａ４（第１の構成情報）の参照先である構成情報Ｂ４（第３の構成情報）がアップグレード手順を含んでもよい。

[0079] この場合、構成情報Ａ４の外部キー「h（KeyB）」をクエリのキーとして、「h（KeyB）」をキーとして有する構成情報Ｂ４を取得する（図１２の矢印Ｙ４１）。この際、構成情報Ｂ４からアップグレード手順を取得できるため、「h（KeyB）」をアップグレードすることで（図１２の（１））、「KeyB」を取得できる。そして、「KeyB」をキーとすることで、構成情報Ｂ４より秘匿レベルの高い構成情報Ｂ（第２の構成情報）の取得が可能となる。

[0080] ［実施の形態のシステム構成について］

管理装置１０の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、管理装置１０の機能の分散及び統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散または統合して構成することができる。

[0081] また、管理装置１０においておこなわれる各処理は、全部または任意の一部が、ＣＰＵ、ＧＰＵ（Graphics Processing Unit）、及び、ＣＰＵ、Ｇ

ＰＵにより解析実行されるプログラムにて実現されてもよい。また、管理装置１０においておこなわれる各処理は、ワイヤードロジックによるハードウェアとして実現されてもよい。

[0082] また、実施の形態において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的に行うこともできる。もしくは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上述及び図示の処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて適宜変更することができる。

[0083] ［プログラム］

図１３は、プログラムが実行されることにより、管理装置１０が実現されるコンピュータの一例を示す図である。コンピュータ１０００は、例えば、メモリ１０１０、ＣＰＵ１０２０を有する。また、コンピュータ１０００は、ハードディスクドライブインタフェース１０３０、ディスクドライブインタフェース１０４０、シリアルポートインタフェース１０５０、ビデオアダプタ１０６０、ネットワークインタフェース１０７０を有する。これらの各部は、バス１０８０によって接続される。

[0084] メモリ１０１０は、ＲＯＭ１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、ハードディスクドライブ１０９０に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１１００に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ１１００に挿入される。シリアルポートインタフェース１０５０は、例えばマウス１１１０、キーボード１１２０に接続される。ビデオアダプタ１０６０は、例えばディスプレイ１１３０に接続される。

[0085] ハードディスクドライブ１０９０は、例えば、ＯＳ（Operating System）１０９１、アプリケーションプログラム１０９２、プログラムモジュール１

０９３、プログラムデータ１０９４を記憶する。すなわち、管理装置１０の各処理を規定するプログラムは、コンピュータ１０００により実行可能なコードが記述されたプログラムモジュール１０９３として実装される。プログラムモジュール１０９３は、例えばハードディスクドライブ１０９０に記憶される。例えば、管理装置１０における機能構成と同様の処理を実行するためのプログラムモジュール１０９３が、ハードディスクドライブ１０９０に記憶される。なお、ハードディスクドライブ１０９０は、ＳＳＤ（Solid State Drive）により代替されてもよい。

[0086] また、上述した実施の形態の処理で用いられる設定データは、プログラムデータ１０９４として、例えばメモリ１０１０やハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０が、メモリ１０１０やハードディスクドライブ１０９０に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出して実行する。

[0087] なお、プログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０９０に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ１１００等を介してCPU１０２０によって読み出されてもよい。あるいは、プログラムモジュール１０９３及びプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶されてもよい。そして、プログラムモジュール１０９３及びプログラムデータ１０９４は、他のコンピュータから、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

[0088] 以上、本発明者によってなされた発明を適用した実施の形態について説明したが、本実施の形態による本発明の開示の一部をなす記述及び図面により本発明は限定されることはない。すなわち、本実施の形態に基づいて当業者等によりなされる他の実施の形態、実施例及び運用技術等は全て本発明の範疇に含まれる。

符号の説明

[0089] １０　管理装置

１１　生成部

１２　管理部

１３　構成情報データベース（ＤＢ）

請求の範囲

[請求項1] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、

前記第１のハードウェアまたは第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、前記データに対する電子署名と、を付加したフォーマットの構成情報を生成する生成部と、

前記構成情報を管理する管理部と、

を有することを特徴とする管理装置。

[請求項2] 前記生成部は、前記第１の識別子に代えて、前記第１の識別子を一方向関数により符号化した第１の識別子を、前記データに付加したフォーマットの構成情報を生成することを特徴とする請求項１に記載の管理装置。

[請求項3] 前記生成部は、第１の構成情報の参照先の構成情報であって、第２の構成情報を基に秘匿化された構成情報である第３の構成情報から、前記第２の構成情報を取得するための方法を、前記第１の構成情報または前記第３の構成情報に含めることを特徴とする請求項１に記載の管理装置。

[請求項4] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、

前記第１のハードウェアまたは前記第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子と、構成情報全体の第１の電子

署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する生成部と、

前記構成情報を管理する管理部と、

を有することを特徴とする管理装置。

[請求項5] 前記生成部は、段階的に項目を削除した各構成情報から生成した複数の電子署名を付与することを特徴とする請求項４に記載の管理装置。

[請求項6] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置であって、

前記第１のハードウェアまたは第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、構成情報全体の第１の電子署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する生成部と、

前記構成情報を管理する管理部と、

を有することを特徴とする管理装置。

[請求項7] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置が実行する管理方法であって、

第１のハードウェアまたは第１のソフトウェアに関するデータに、第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、前記データに対する電子署名と、を付加したフォーマットの構成

情報を生成する工程と、

前記構成情報を管理する工程と、

を含んだことを特徴とする管理方法。

[請求項8] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置が実行する管理方法であって、

前記第１のハードウェアまたは前記第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子と、構成情報全体の第１の電子署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する工程と、

前記構成情報を管理する工程と、

を含んだことを特徴とする管理方法。

[請求項9] 第１のハードウェアまたは第１のソフトウェアの構成情報を管理する管理装置が実行する管理方法であって、

前記第１のハードウェアまたは第１のソフトウェアに関するデータに、前記第１のハードウェアまたは前記第１のソフトウェアを一意に示す第１の識別子と、前記第１のハードウェアまたは前記第１のソフトウェアを構成する他の第２のハードウェアまたは第２のソフトウェアを一意に特定する第２の識別子を一方向関数により符号化した第２の識別子と、構成情報全体の第１の電子署名と、一部の項目が秘匿された前記構成情報と前記第１の電子署名とを基に生成される第２の電子署名と、を付加したフォーマットの構成情報を生成する工程と、

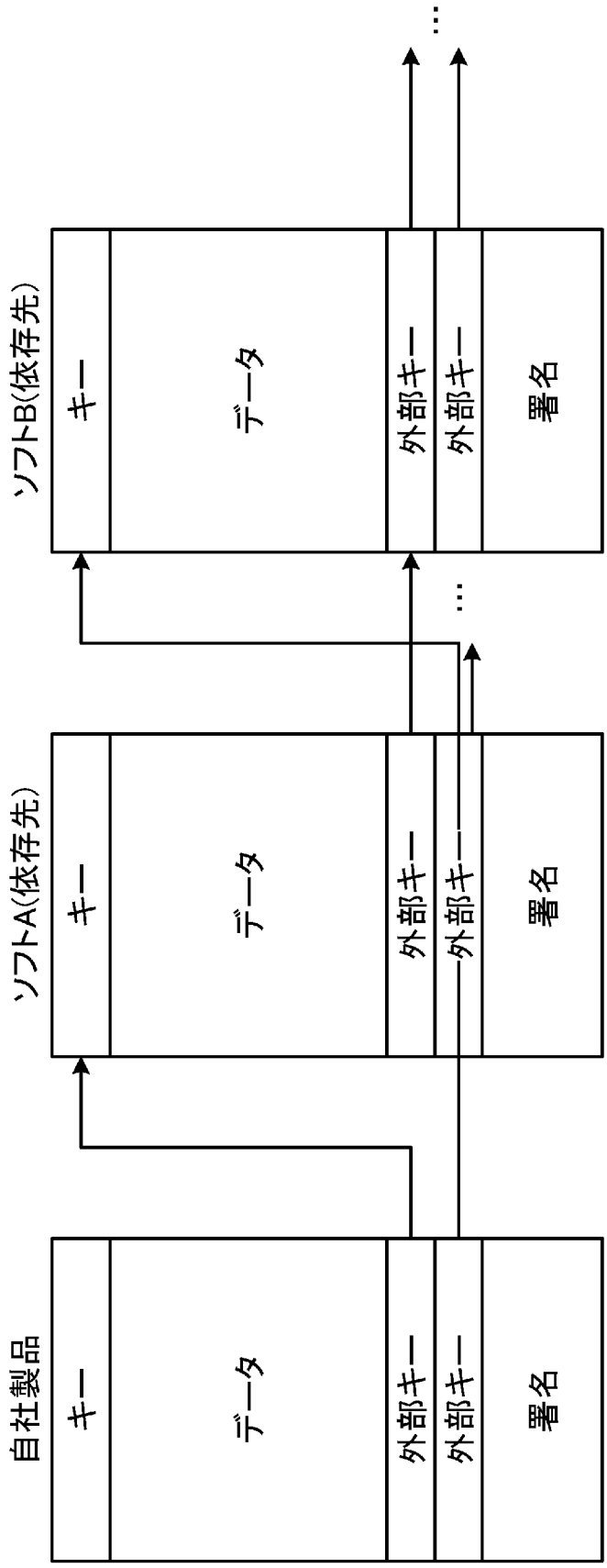
前記構成情報を管理する工程と、

を含んだことを特徴とする管理方法。

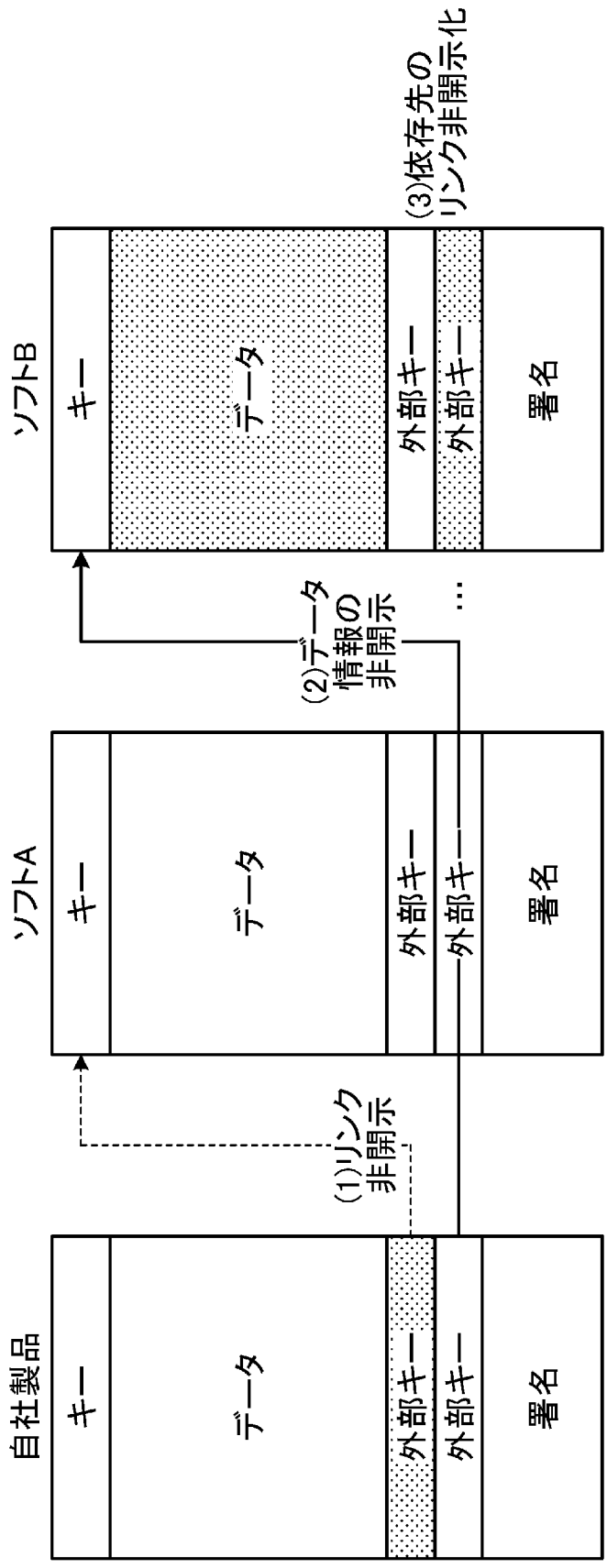
[請求項10] コンピュータを請求項１～６に記載の管理装置として機能させるた

めの管理プログラム。

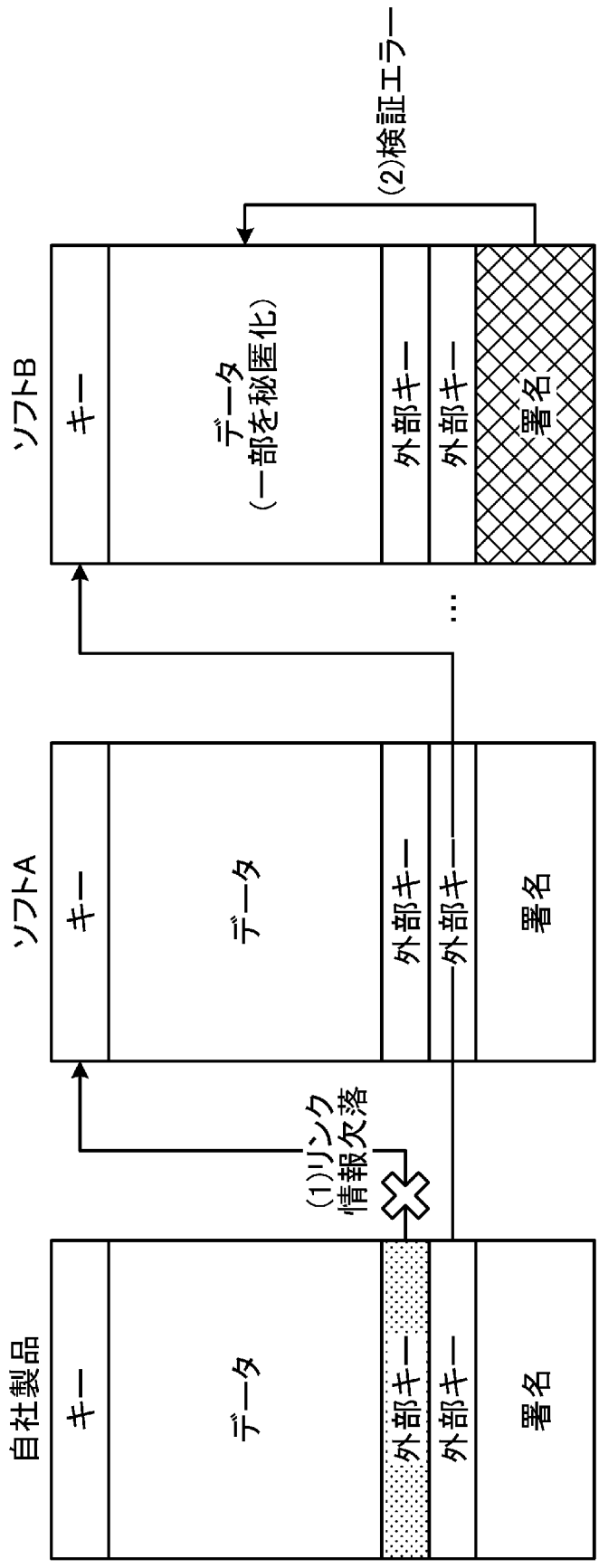
[図1]


自社製品
キー
データ
外部キー
外部キー
署名
ソフトA(依存先)
キー
データ
外部キー
外部キー
署名
ソフトB(依存先)
キー
データ
外部キー
外部キー
署名

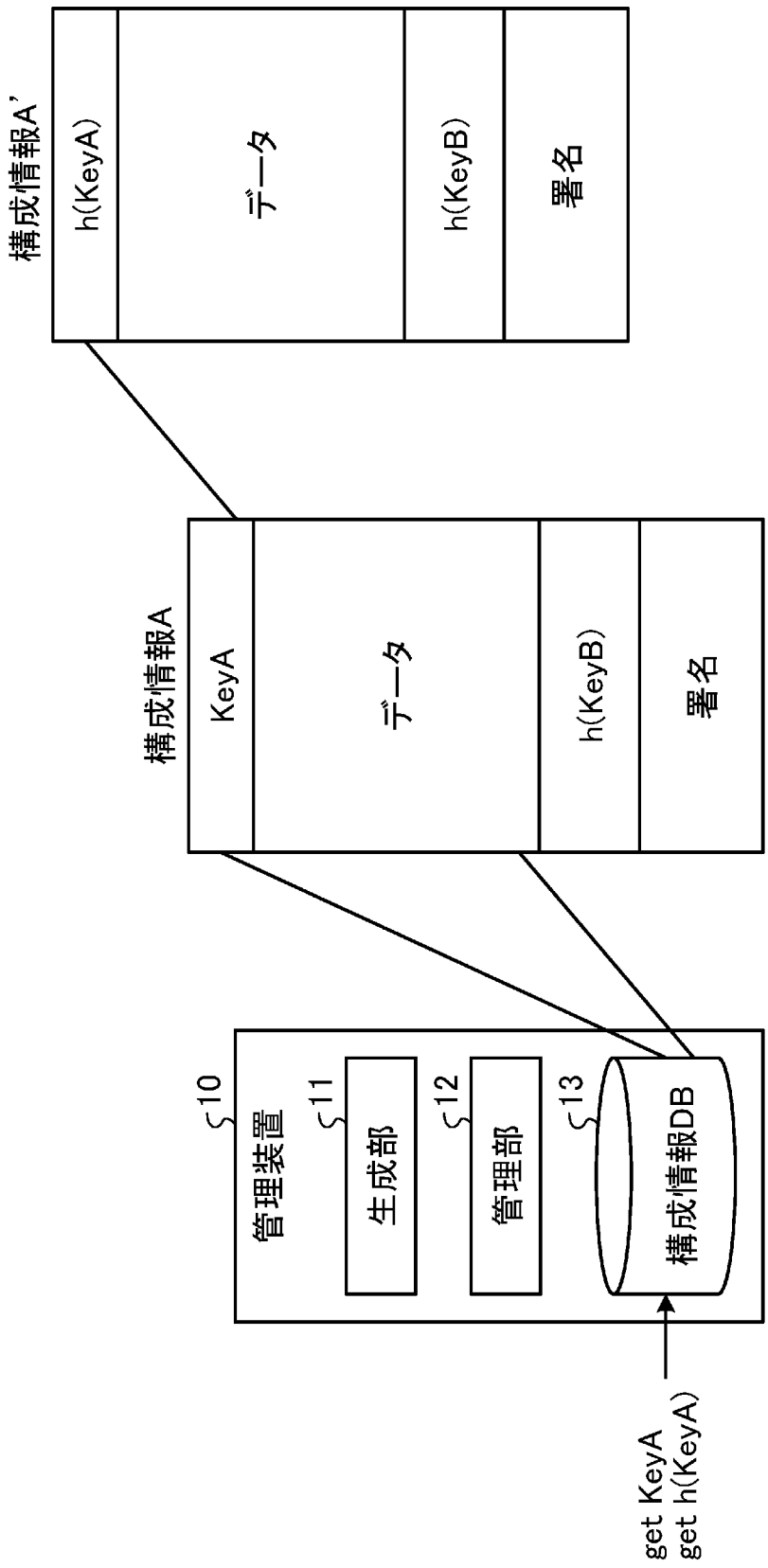
[図2]


自社製品
キー
データ
外部キー
外部キー
署名
(1)リンク
非開示
ソフトA
キー
データ
外部キー
外部キー
署名
(2)データ
情報の
非開示
ソフトB
キー
データ
外部キー
外部キー
署名
(3)依存先の
リンク非開示化

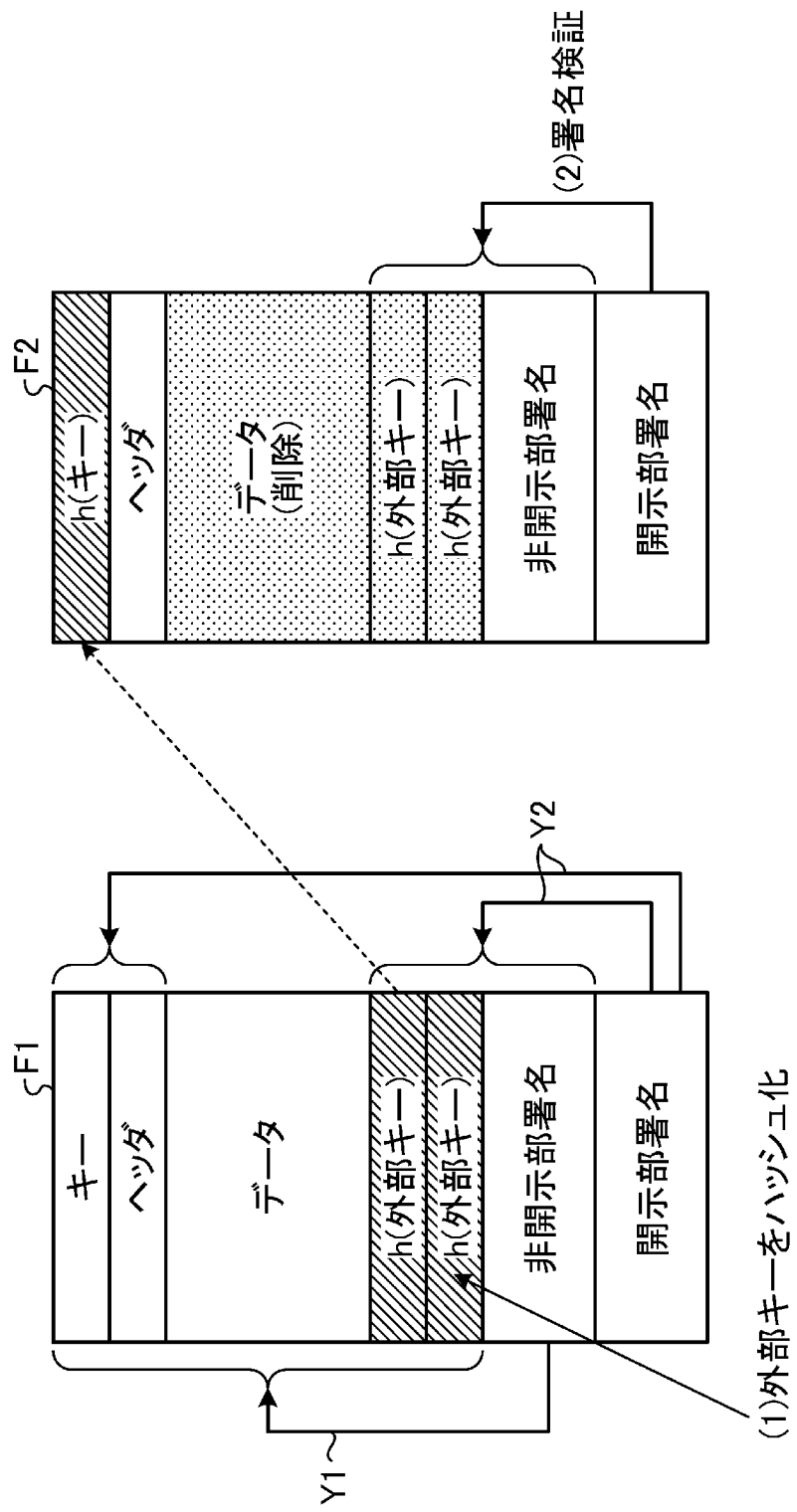
[図3]


(2)検証エラー
ソフトB
キー
データ
(一部を秘匿化)
外部キー
外部キー
署名
ソフトA
キー
データ
外部キー
外部キー
署名
(1)リンク
情報欠落
自社製品
キー
データ
外部キー
外部キー
署名

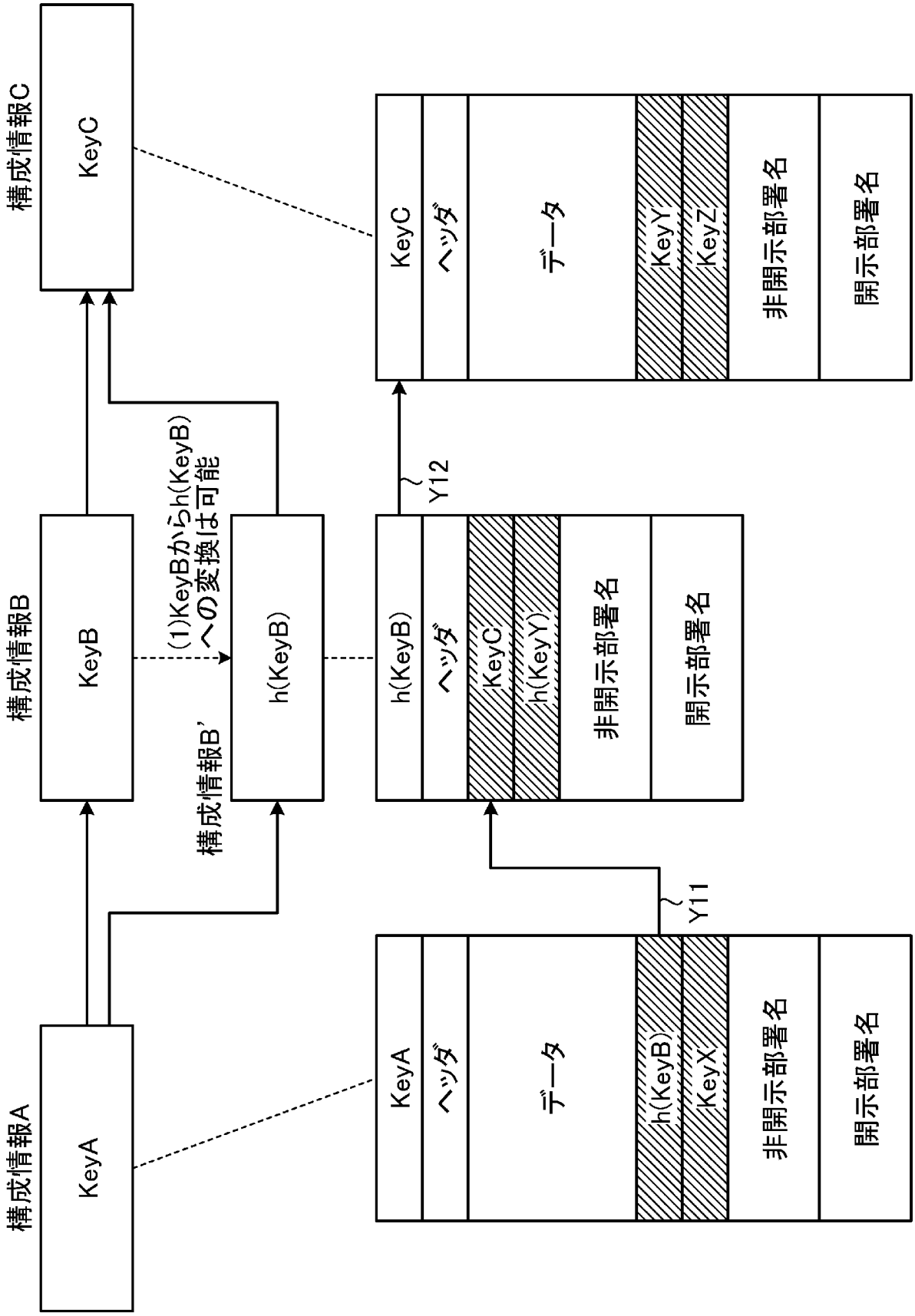
[図4]


構成情報A'
h(KeyA)
データ
h(KeyB)
署名
構成情報A
KeyA
データ
h(KeyB)
署名
10
管理装置
11
生成部
12
管理部
13
構成情報DB
get KeyA
get h(KeyA)

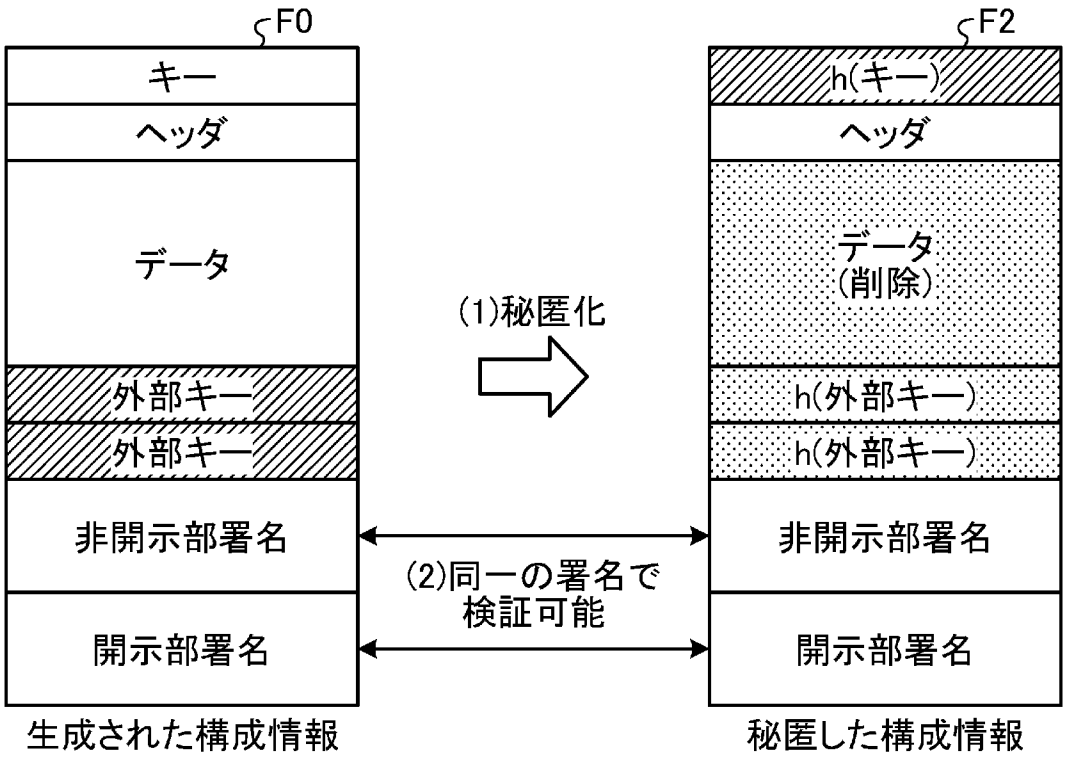
[図5]


(2)署名検証
F2
h(キー)
ヘッダ
データ
(削除)
h(外部キー)
h(外部キー)
非開示部署名
開示部署名
Y2
F1
キー
ヘッダ
データ
h(外部キー)
h(外部キー)
非開示部署名
開示部署名
(1)外部キーをハッシュ化
Y1

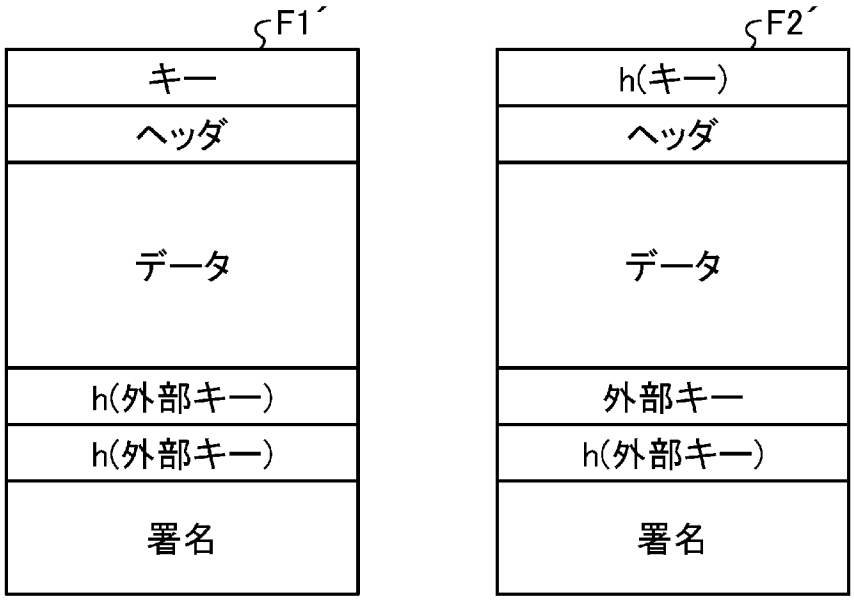
[図6]


構成情報C
KeyC
構成情報B
KeyB
(1)KeyBからh(KeyB)への変換は可能
構成情報B'
h(KeyB)
構成情報A
KeyA
KeyC
ヘッダ
データ
KeyY
KeyZ
非開示部署名
開示部署名
Y12
h(KeyB)
ヘッダ
KeyC
h(KeyY)
非開示部署名
開示部署名
Y11
KeyA
ヘッダ
データ
h(KeyB)'
KeyX
非開示部署名
開示部署名

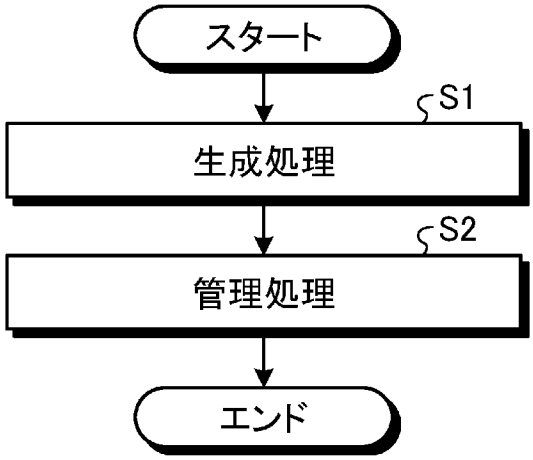
[図7]


F0
キー
ヘッダ
データ
外部キー
外部キー
非開示部署名
開示部署名
生成された構成情報
(1)秘匿化
(2)同一の署名で
検証可能
F2
h(キー)
ヘッダ
データ
(削除)
h(外部キー)
h(外部キー)
非開示部署名
開示部署名
秘匿した構成情報

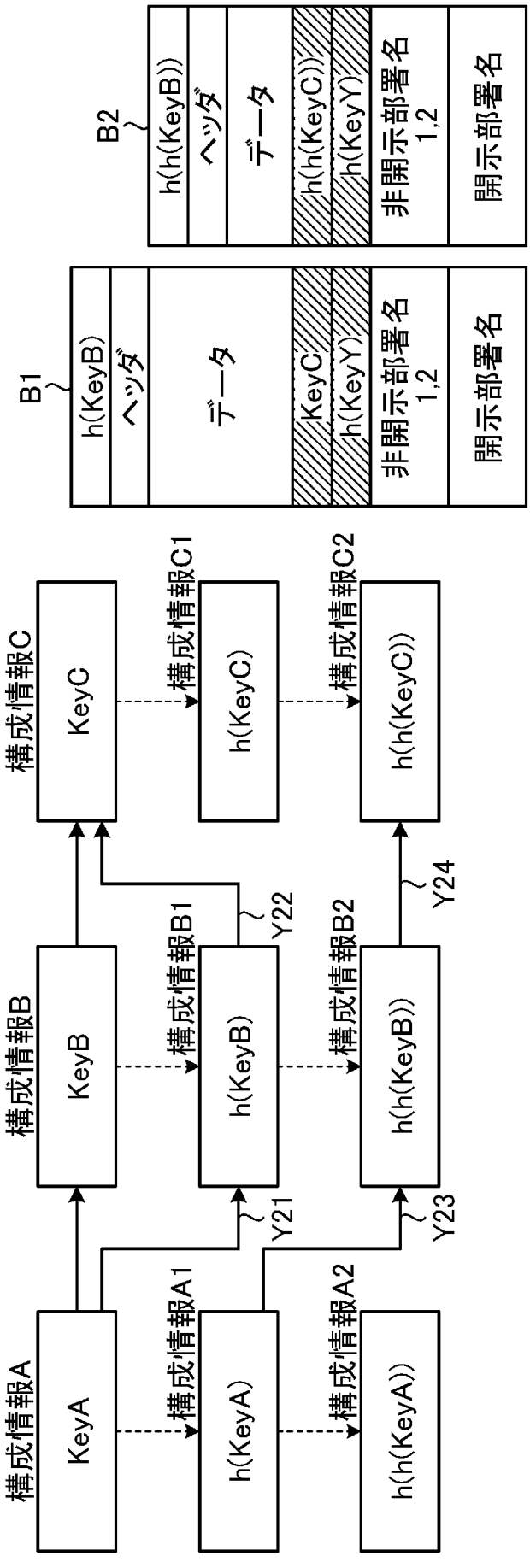
[図8]


F1´
キー
ヘッダ
データ
h(外部キー)
h(外部キー)
署名
F2´
h(キー)
ヘッダ
データ
外部キー
h(外部キー)
署名

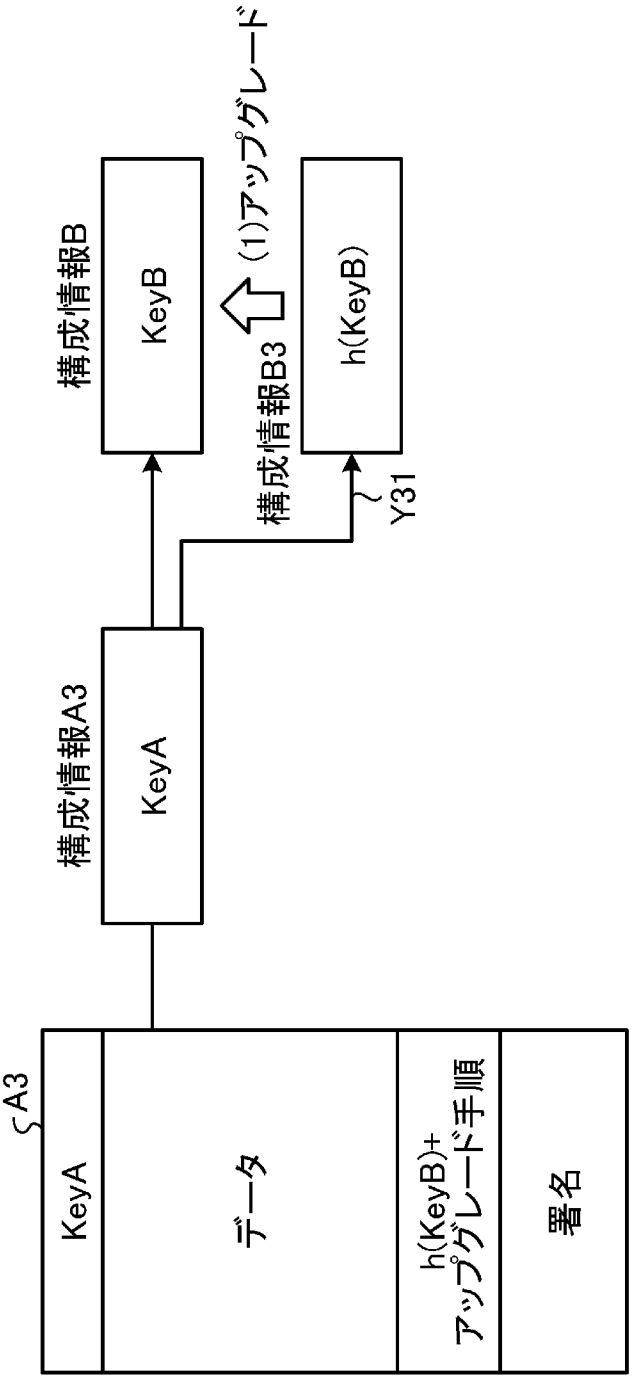
[図9]



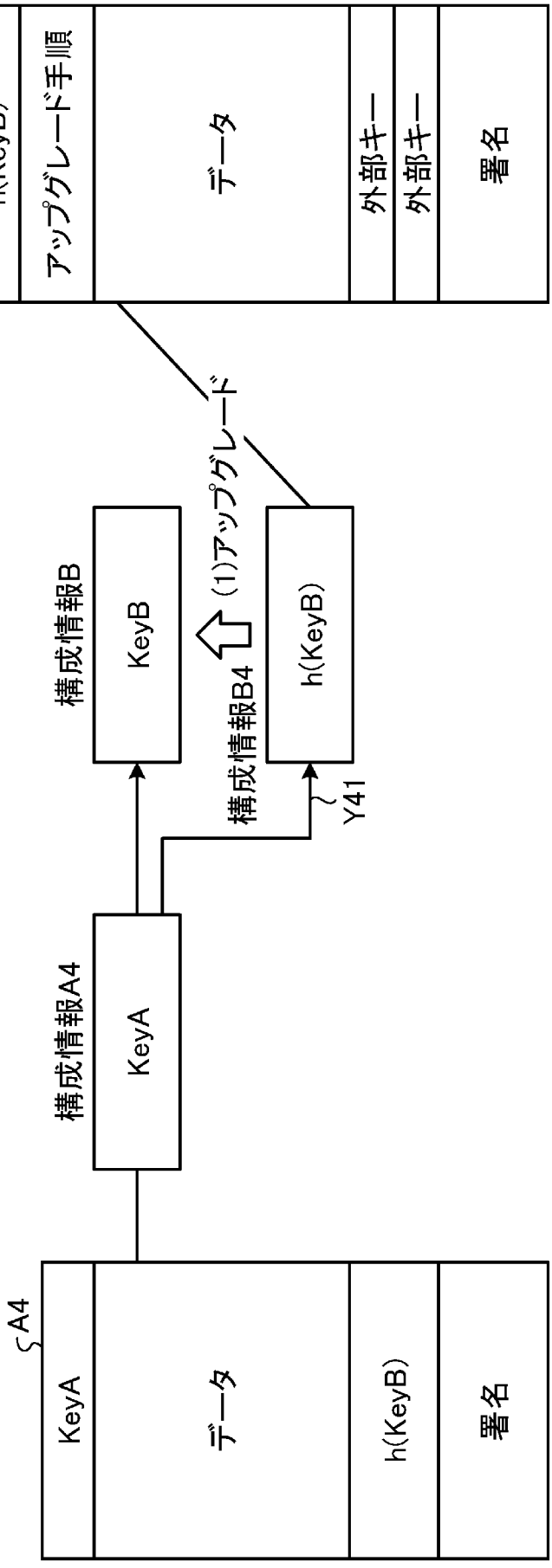
[図10]


B2
h(h(KeyB))
ヘッダ
データ
h(h(KeyC))
h(KeyY)
非開示部署名
1,2
開示部署名
B1
h(KeyB)
ヘッダ
データ
KeyC
h(KeyY)
非開示部署名
1,2
開示部署名
構成情報C
KeyC
構成情報C1
h(KeyC)
構成情報C2
h(h(KeyC))
構成情報B
KeyB
構成情報B1
h(KeyB)
構成情報B2
h(h(KeyB))
構成情報A
KeyA
構成情報A1
h(KeyA)
構成情報A2
h(h(KeyA))
Y21
Y22
Y23
Y24

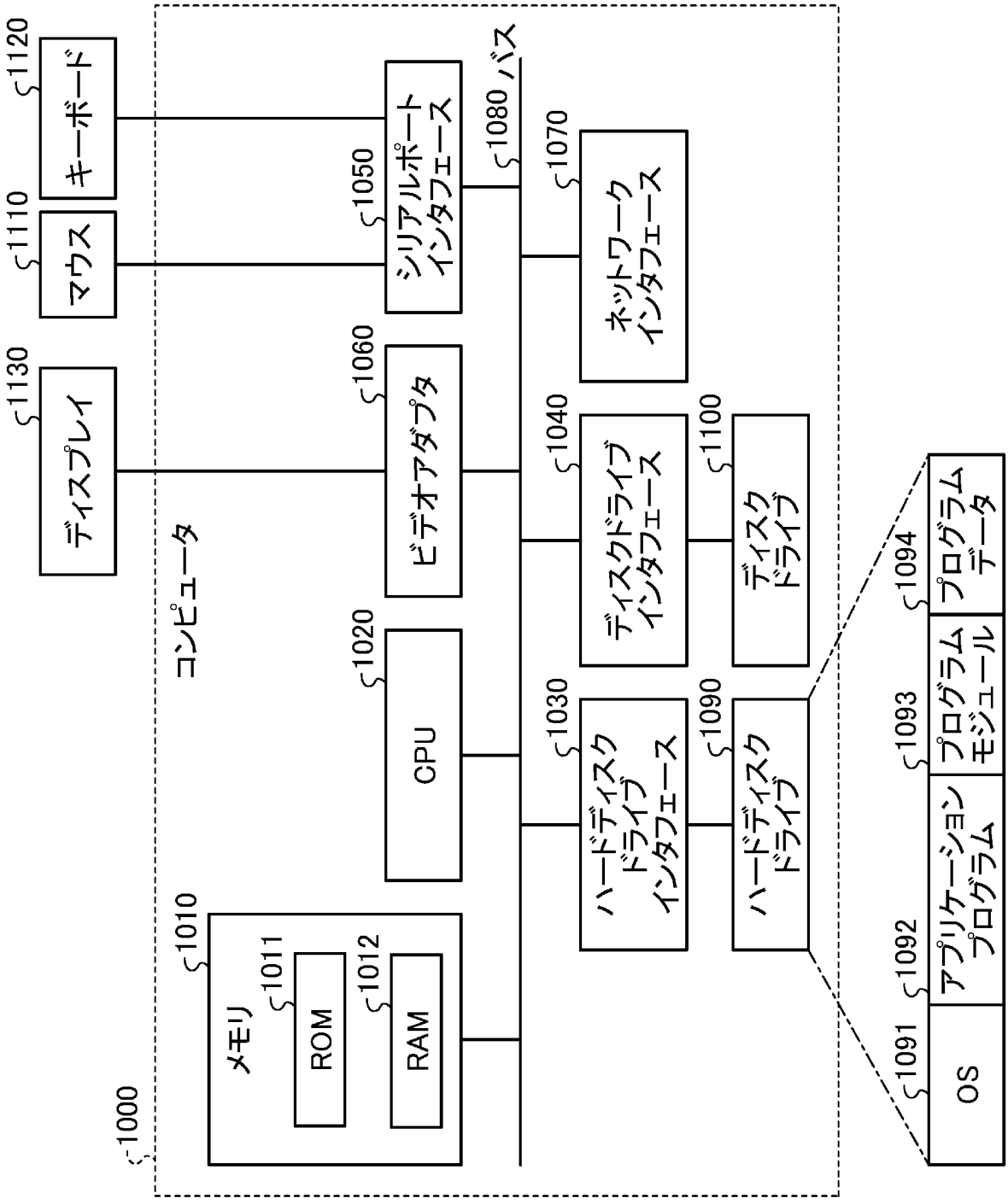
[図11]


A3
KeyA
データ
h(KeyB)+
アップグレード手順
署名
構成情報A3
KeyA
構成情報B3
(1)アップグレード
h(KeyB)
Y31
構成情報B
KeyB

[図12]


B4
h(KeyB)
アップグレード手順
データ
外部キー
外部キー
署名
(1)アップグレード
構成情報B
KeyB
構成情報B4
h(KeyB)
Y41
構成情報A4
KeyA
A4
KeyA
データ
h(KeyB)
署名

[図13]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
バス
1090
ハードディスクドライブ
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ
1100
ディスクドライブ
1110
マウス
1120
キーボード
1130
ディスプレイ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/025364

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; ***G06F 21/57***(2013.01)i; ***G06F 21/60***(2013.01)i
FI: H04L9/32 200E; G06F21/57; G06F21/60

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)

H04L9/32; G06F21/57; G06F21/60

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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 2021/220642 A1 (HITACHI LTD) 04 November 2021 (2021-11-04)	1-10
A	DIGLIO, Adrian. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft. Engineering@Microsoft [online]. 2021 [retrieved on 07 September 2022], Retrieved from the Internet: <URL https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/> entire text, all drawings	1-10
A	JP 2007-172450 A (NIPPON TELEGR & TELEPH CORP <NTT>) 05 July 2007 (2007-07-05)	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
07 September 2022	**20 September 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/025364

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2021/220642 A1	04 November 2021	(Family: none)	
JP 2007-172450 A	05 July 2007	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2022/025364

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i; G06F 21/57(2013.01)i; G06F 21/60(2013.01)i
FI: H04L9/32 200E; G06F21/57; G06F21/60

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））

H04L9/32; G06F21/57; G06F21/60

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	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２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 2021/220642 A1 (株式会社日立製作所) 04.11.2021 (2021-11-04)	1-10
A	DIGLIO, Adrian, Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft, Engineering@Microsoft [online], 2021 [retrieved on 2022.09.07], Retrieved from the Internet: <URL https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/> 全文、全図	1-10
A	JP 2007-172450 A (日本電信電話株式会社) 05.07.2007 (2007-07-05)	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抵触するものではなく、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
07.09.2022	20.09.2022

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
吉田　歩 5S 1206

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/025364

引用文献	公表日	パテントファミリー文献	公表日
WO 2021/220642 A1	04.11.2021	（ファミリーなし）	
JP 2007-172450 A	05.07.2007	（ファミリーなし）	