(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-46488
(P2019-46488A)
(43)公開日　平成31年3月22日(2019.3.22)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/62	354
G06F 16/00	(2019.01)	G06F	17/30	340B
		G06F	17/30	120A
		G06F	17/30	350C

審査請求 有　請求項の数 15　ＯＬ　（全 50 頁）

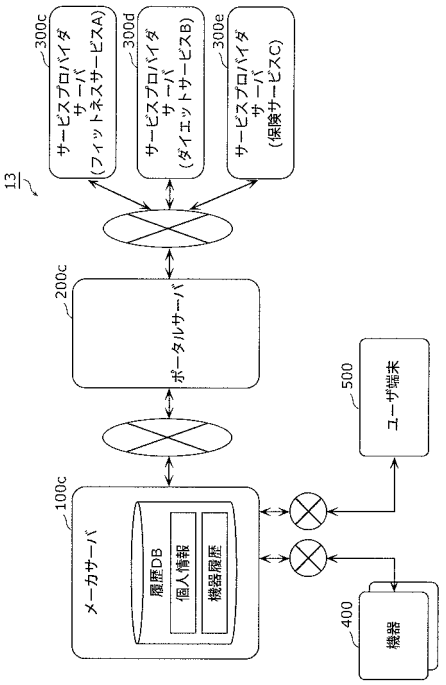
(21)出願番号　特願2018-201120 (P2018-201120)
(22)出願日　平成30年10月25日 (2018.10.25)
(62)分割の表示　特願2017-96338 (P2017-96338)の分割
原出願日　平成25年9月18日 (2013.9.18)
(31)優先権主張番号　61/706,910
(32)優先日　平成24年9月28日 (2012.9.28)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/720,429
(32)優先日　平成24年10月31日 (2012.10.31)
(33)優先権主張国　米国 (US)

(71)出願人　314012076
パナソニックＩＰマネジメント株式会社
大阪府大阪市中央区城見２丁目１番６１号
(74)代理人　100109210
弁理士　新居　広守
(74)代理人　100137235
弁理士　寺谷　英作
(74)代理人　100131417
弁理士　道坂　伸一
(72)発明者　海上　勇二
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　パナソニック株式会社内

最終頁に続く

(54)【発明の名称】情報管理方法および情報管理システム

(57)【要約】
【課題】ユーザの匿名性を確保しつつ、当該ユーザに適切なサービスを提供することができる情報管理方法を提供する。
【解決手段】ネットワークを介して、メーカサーバ（１００ｃ）から、第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、第１のユーザを特定可能な属性情報を含む第１のユーザ情報が所定ルールで匿名化された第１の匿名化ユーザ情報とを受信し、ネットワークを介して、メーカサーバ（１００ｃ）と異なるサービスプロバイダサーバ（３００ｃ等）から、第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、第２のユーザを特定可能な属性情報を含む第２のユーザ情報が上記所定ルールで匿名化された第２の匿名化ユーザ情報とを受信し、第１の匿名化ユーザ情報と第２の匿名化ユーザ情報とが同一または類似すると判断された場合に、受信した機器履歴情報とサービス履歴情報とを関連付けて複合情報として管理する。
【選択図】図１



【特許請求の範囲】
【請求項１】
情報を管理する情報管理装置における情報管理方法であって、
ユーザ情報の匿名化に用いられる匿名化ルールを生成し、
前記匿名化ルールを第１のサーバおよび第２のサーバに送信し、
前記第１のサーバから、第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、前記第１のユーザを特定可能な属性情報を含む第１のユーザ情報が前記匿名化ルールにより匿名化された第１の匿名化ユーザ情報とを受信し、
前記第２のサーバから、第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、前記第２のユーザを特定可能な属性情報を含む第２のユーザ情報が前記匿名化ルールで匿名化された第２の匿名化ユーザ情報とを受信する、
情報管理方法。
【請求項２】
前記第１の匿名化ユーザ情報と前記第２の匿名化ユーザ情報とが同一または類似すると判断された場合に、受信した前記機器履歴情報と前記サービス履歴情報とを関連付けて複合情報として管理する、
請求項１に記載の情報管理方法。
【請求項３】
前記匿名化ルールは、前記第１のサーバが記憶する前記機器履歴情報により示される動作の種類と前記第２のサーバが記憶する前記サービス履歴情報により示されるサービスの種類との組み合わせに基づいて決定される、
請求項１に記載の情報管理方法。
【請求項４】
前記匿名化ルールには、前記第１のユーザ情報および前記第２のユーザ情報に含まれる１以上の属性情報のうち、削除または抽象化すべき属性情報が規定されている、
請求項１～３のいずれか１項に記載の情報管理方法。
【請求項５】
前記第１の匿名化ユーザ情報および前記第２の匿名化ユーザ情報は、第１のユーザおよび第２のユーザにおける性別、年齢、年代、住所および職業のうち少なくとも一を属性情報として含む、
請求項１～４のいずれか１項に記載の情報管理方法。
【請求項６】
前記複合情報に基づいて、前記第１のユーザに対するサービス提案を示す提案情報を生成し、
生成した前記提案情報を前記第１のサーバを介して前記第１のユーザへ提供する、
請求項１～５のいずれか１項に記載の情報管理方法。
【請求項７】
前記提案情報は、前記機器を制御するための制御プログラムを含む情報である、
請求項６に記載の情報管理方法。
【請求項８】
前記複合情報に基づいて前記第２のユーザに対するサービス提案を示す提案情報を生成し、
生成した前記提案情報を前記第２のサーバを介して前記第２のユーザへ提供する、
請求項１～５のいずれか１項に記載の情報管理方法。
【請求項９】
前記第１のユーザと前記第２のユーザとは同一ユーザである、
請求項１～８のいずれか１項に記載の情報管理方法。
【請求項１０】
前記第１のユーザと前記第２のユーザとは異なるユーザである、
請求項１～８のいずれか１項に記載の情報管理方法。

【請求項１１】
前記サービス履歴情報は、前記第２のユーザが医療を含む健康管理に関するサービスを受けた履歴を含む情報である、
請求項１～１０のいずれか１項に記載の情報管理方法。
【請求項１２】
前記サービス履歴情報は、前記第２のユーザが教育サービスを受けた履歴を含む情報である、
請求項１～１０のいずれか１項に記載の情報管理方法。
【請求項１３】
前記サービス履歴情報は、前記第２のユーザが交通サービスを受けた履歴を含む情報である、
請求項１～１０のいずれか１項に記載の情報管理方法。
【請求項１４】
情報を管理する情報管理装置と、
第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、前記第１のユーザを特定可能な属性情報を含む第１のユーザ情報とを記憶する第１のサーバと、
第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、前記第２のユーザを特定可能な属性情報を含む第２のユーザ情報を記憶する第２のサーバと、を備え、
前記情報管理装置は、
ユーザ情報の匿名化に用いられる匿名化ルールを生成し、
前記匿名化ルールを前記第１のサーバおよび前記第２のサーバに送信し、
前記第１のサーバから、前記機器履歴情報と、前記第１のユーザ情報が前記匿名化ルールで匿名化された第１の匿名化ユーザ情報とを受信し、
前記第２のサーバから、前記サービス履歴情報と、前記第２のユーザ情報が前記匿名化ルールで匿名化された第２の匿名化ユーザ情報とを受信する、
情報管理システム。
【請求項１５】
前記情報管理装置は、
前記第１の匿名化ユーザ情報と前記第２の匿名化ユーザ情報とが同一または類似すると判断した場合に、受信した前記機器履歴情報と前記サービス履歴情報とを関連付けて複合情報として管理する、
請求項１４に記載の情報管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報管理方法および情報管理システムに関する。
【背景技術】
【０００２】
近年、家庭内の家電やＡＶ機器がネットワークに接続されており、そこからクラウドに各種履歴情報（ユーザの家電の使用履歴や、ＴＶの視聴履歴といった、いわゆる、ライフログ情報）が収集されている。そのため、クラウドに収集されたライフログ情報を用いたサービスの提供が期待されている。例えば、クラウドに収集したライフログ情報を活用し、さらにサービスプロバイダと連携することで、当該ユーザのライフスタイルに適した個人向けサービスの提供や統計情報を用いてマーケット分析を行うサービスの提供などが期待されている。
【０００３】
しかし、ライフログ情報は当該ユーザのプライバシに関連しているため、ライフログ情報に含まれる個人情報は当該ユーザの許可なく第三者には提供できない。
【０００４】
そのため、サービス提供者に対してユーザの匿名性を実現しつつ、サービスを提供する

方法が提案されている（例えば特許文献１）。特許文献１では、オンライン取引において、匿名の利用者にサービスを提供する方法が提案されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００９－１５９３１７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記従来の方法では、提供するサービスが当該ユーザに対するサービスであるか検証できないという問題がある。つまり、サービス提供者が、異なるユーザへのサービスを当該ユーザに提供しようとする場合であっても、提供しようとするユーザが当該ユーザであることを検証できない。そのため、当該ユーザに適切なサービスが提供できないことが生じうる。
【０００７】
本発明は、上述の事情を鑑みてなされたもので、ユーザの匿名性を確保しつつ、当該ユーザに適切なサービスを提供することができる情報管理方法および情報管理システムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
上記目的を達成するために、本発明の一態様に係る情報管理方法は、情報を管理する情報管理装置における情報管理方法であって、ユーザ情報の匿名化に用いられる匿名化ルールを生成し、前記匿名化ルールを第１のサーバおよび第２のサーバに送信し、前記第１のサーバから、第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、前記第１のユーザを特定可能な属性情報を含む第１のユーザ情報が前記匿名化ルールにより匿名化された第１の匿名化ユーザ情報とを受信し、前記第２のサーバから、第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、前記第２のユーザを特定可能な属性情報を含む第２のユーザ情報が前記匿名化ルールで匿名化された第２の匿名化ユーザ情報とを受信する。
【０００９】
なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。
【発明の効果】
【００１０】
本発明の情報管理方法等によれば、ユーザの匿名性を確保しつつ、当該ユーザに適切なサービスを提供することができる。
【図面の簡単な説明】
【００１１】
【図１】図１は、実施の形態１に係る情報管理システムの全体構成の一例を示す図である。
【図２】図２は、実施の形態１に係るメーカサーバの構成の一例を示すブロック図である。
【図３】図３は、実施の形態１に係る機器履歴証明書の構成の一例を示す図である。
【図４】図４は、実施の形態１に係るポータルサーバの構成の一例を示すブロック図である。
【図５】図５は、実施の形態１に係る匿名化ルールの一例を示す図である。
【図６】図６は、実施の形態１に係る提案情報証明書の構成の一例を示す図である。
【図７】図７は、実施の形態１に係るサービスプロバイダサーバの構成の一例を示すブロ

ック図である。
【図８】図８は、サービス履歴証明書の構成の一例を示す図である。
【図９】図９は、ポータルサーバからユーザに提案情報を提供する処理のシーケンス図である。
【図１０】図１０は、ポータルサーバからユーザに提案情報を提供する処理のシーケンス図である。
【図１１】図１１は、ポータルサーバからユーザに提案情報を提供する処理のシーケンス図である。
【図１２】図１２は、ポータルサーバからユーザに提案情報を提供する処理のシーケンス図である。
【図１３】図１３は、実施の形態２に係る情報管理システムの全体構成の一例を示す図である。
【図１４】図１４は、実施の形態２に係るメーカサーバの構成の一例を示すブロック図である。
【図１５】図１５は、実施の形態２に係る機器履歴証明書の構成の一例を示す図である。
【図１６】図１６は、実施の形態２に係る個人情報ＤＢの一例を示す図である。
【図１７】図１７は、実施の形態２に係る機器履歴ＤＢのＩＤリストの一例を示す図である。
【図１８】図１８は、実施の形態２に係る家電履歴ＤＢに記録されているデータの一例を示した図である。
【図１９】図１９は、実施の形態２に係るポータルサーバの構成の一例を示すブロック図である。
【図２０】図２０は、提案情報ＤＢの構成の一例を示す図である。
【図２１】図２１は、提案サービス情報ＤＢに記録されているデータの一例を示す図である。
【図２２】図２２は、実施の形態２に係る提案情報証明書の構成の一例を示す図である。
【図２３】図２３は、実施の形態２に係るサービスプロバイダサーバの構成の一例を示すブロック図である。
【図２４】図２４は、実施の形態２に係るサービス履歴ＤＢの一例を示す図である。
【図２５】図２５は、個人情報ＤＢの構成の一例を示した図である。
【図２６】図２６は、サービス情報ＤＢに記録されているデータの一例を示す図である。
【図２７】図２７は、ユーザがユーザ端末を用いてメーカサーバに登録するときのシーケンス図である。
【図２８】図２８は、ユーザがユーザ端末を用いて家電機器を登録するときのシーケンス図である。
【図２９】図２９は、機器が機器履歴情報をアップロードするときのシーケンス図である。
【図３０】図３０は、実施の形態２に係るポータルサーバからユーザに提案情報を提供するときのシーケンス図である。
【図３１】図３１は、実施の形態２に係るポータルサーバからユーザに提案情報を提供するときのシーケンス図である。
【図３２】図３２は、実施の形態２に係るポータルサーバからユーザに提案情報を提供するときのシーケンス図である。
【図３３】図３３は、実施の形態３に係る情報管理システムの全体構成の一例を示す図である。
【図３４】図３４は、実施の形態３に係るメーカサーバの構成の一例を示すブロック図である。
【図３５】図３５は、実施の形態３に係る個人情報ＤＢの一例を示す図である。
【図３６】図３６は、実施の形態３に係る機器履歴証明書の構成の一例を示す図である。
【図３７】図３７は、実施の形態３に係る提案情報証明書の構成の一例を示す図である。

【図３８】図３８は、実施の形態３に係るサービスプロバイダサーバの構成の一例を示すブロック図である。
【図３９】図３９は、実施の形態３に係るサービス履歴証明書の構成の一例図である。
【図４０】図４０は、実施の形態３に係るユーザの登録処理を示すシーケンス図である。
【図４１】図４１は、実施の形態３に係る提案情報提供処理のシーケンス図である。
【図４２】図４２は、実施の形態３に係る提案情報提供処理のシーケンス図である。
【図４３】図４３は、実施の形態３に係る提案情報提供処理のシーケンス図である。
【図４４】図４４は、実施の形態３に係る提案情報提供処理のシーケンス図である。
【図４５】図４５は、有効期限を含めた機器履歴証明書の構成の一例を示す図である。
【図４６】図４６は、機器履歴情報の提供データリストの一例を示す図である。
【図４７】図４７は、ポータルサーバからユーザへ提案情報を提供する処理のシーケンス図である。
【図４８】図４８は、ポータルサーバからユーザへ提案情報を提供する処理のシーケンス図である。
【図４９】図４９は、ポータルサーバからユーザへ提案情報を提供する処理のシーケンス図である。
【図５０】図５０は、提案情報証明書の構成の一例を示す図である。
【図５１】図５１は、情報管理システムの全体構成の一例を示す図である。
【図５２】図５２は、複数のユーザの機器履歴を含んだ機器履歴証明書の構成の一例を示す図である。
【発明を実施するための形態】
【００１２】
上記目的を達成するために、本発明の一態様に係る情報管理方法は、情報を管理する情報管理装置における情報管理方法であって、ネットワークを介して、第１のサーバから、第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、前記第１のユーザを特定可能な属性情報を含む第１のユーザ情報が所定ルールで匿名化された第１の匿名化ユーザ情報とを受信し、ネットワークを介して、前記第１のサーバと異なる第２のサーバから、第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、前記第２のユーザを特定可能な属性情報を含む第２のユーザ情報が前記所定ルールで匿名化された第２の匿名化ユーザ情報とを受信し、前記第１の匿名化ユーザ情報と前記第２の匿名化ユーザ情報とが同一または類似すると判断された場合に、受信した前記機器履歴情報と前記サービス履歴情報とを関連付けて複合情報として管理する。
【００１３】
この構成により、ユーザの匿名性を確保しつつ、当該ユーザに適切なサービスを提供することができる。
【００１４】
より具体的には、所定ルール（匿名化ルール）に従って匿名化されたユーザ情報を用いることで、第１のサーバと情報管理装置と第２のサーバとを連携させることができるので、情報管理装置は、ユーザの機器履歴と当該ユーザと同一または類似のサービス履歴とを復号情報として関係付けて管理することができる。それにより、情報管理装置は、複合情報を用いてサービスの提案情報を該当するユーザに提供することができる。なお、第１のサーバと第２のサーバは、情報管理装置に対して、ユーザが特定できない程度に匿名化されたユーザ情報を提供するに留まるので、情報管理装置は、ユーザのプライバシを保護しつつ、複合情報を用いて当該ユーザに対する提案情報などを生成することができる情報管理方法を実現することができる。
【００１５】
また、例えば、前記所定ルールは、前記第１のサーバが記憶する前記機器履歴情報により示される動作の種類と前記第２のサーバが記憶する前記サービス履歴情報により示されるサービスの種類との組み合わせに基づいて決定されるとしてもよい。ここで、例えば、前記所定ルールには、前記第１のユーザ情報および前記第２のユーザ情報に含まれる１以

上の属性情報のうち、削除または抽象化すべき属性情報が規定されている。
【００１６】
また、例えば前記第１の匿名化ユーザ情報および前記第２の匿名化ユーザ情報は、第１のユーザおよび第２のユーザにおける性別、年齢、年代、住所および職業のうち少なくとも一を属性情報として含むとしてもよい。
【００１７】
サービス履歴の内容やユーザが使用する機器に依存して、当該ユーザに対する提案情報も異なってくる。そのため、ユーザ情報に含まれる属性情報のうちユーザを特定できる属性情報は削除または抽象化するが、ユーザ情報に含まれる属性情報のうちユーザを特定できない属性情報は、サービスの種類や動作の種類の組み合わせにより削除または抽象化したりしなかったり決定することができる。それにより、複合情報を用いてより当該ユーザに適した提案情報を生成することができる情報管理方法を実現することができる。
【００１８】
また、例えば、前記複合情報に基づいて、前記第１のユーザに対するサービス提案を示す提案情報を生成し、生成した前記提案情報を前記第１のサーバを介して前記第１のユーザへ提供するとしてもよい。
【００１９】
また、例えば、前記提案情報は、前記機器を制御するための制御プログラムを含む情報であるとしてもよい。
【００２０】
また、例えば、前記複合情報に基づいて前記第２のユーザに対するサービス提案を示す提案情報を生成し、生成した前記提案情報を前記第２のサーバを介して前記第２のユーザへ提供するとしてもよい。
【００２１】
また、例えば、前記第１のユーザと前記第２のユーザとは同一ユーザであるとしてもよいし、前記第１のユーザと前記第２のユーザとは異なるユーザであるとしてもよい。
【００２２】
ここで、例えば、前記サービス履歴情報は、前記第２のユーザが医療を含む健康管理に関するサービスを受けた履歴を含む情報であるとしてもよい。
【００２３】
また、例えば、前記サービス履歴情報は、前記第２のユーザが教育サービスを受けた履歴を含む情報であるとしてもよい。
【００２４】
また、例えば、前記サービス履歴情報は、前記第２のユーザが交通サービスを受けた履歴を含む情報であるとしてもよい。
【００２５】
また、例えば、さらに、前記第１のサーバおよび前記第２のサーバに、ネットワークを介して、前記所定ルールを送信するとしてもよい。
【００２６】
また、上記目的を達成するために、本発明の一態様に係る情報管理システムは、情報を管理する情報管理装置と、第１のユーザが使用する機器の動作履歴を示す機器履歴情報と、前記第１のユーザを特定可能な属性情報を含む第１のユーザ情報とを記憶する第１のサーバと、第２のユーザが享受したサービスの履歴を示すサービス履歴情報と、前記第２のユーザを特定可能な属性情報を含む第２のユーザ情報を記憶する第２のサーバと、を備え、前記情報管理装置は、ネットワークを介して、前記第１のサーバから、前記機器履歴情報と、前記第１のユーザ情報が所定ルールで匿名化された第１の匿名化ユーザ情報とを受信し、ネットワークを介して、前記第２のサーバから、前記サービス履歴情報と、前記第２のユーザ情報が前記所定ルールで匿名化された第２の匿名化ユーザ情報とを受信し、前記第１の匿名化ユーザ情報と前記第２の匿名化ユーザ情報とが同一または類似すると判断した場合に、受信した前記機器履歴情報と前記サービス履歴情報とを関連付けて複合情報

として管理する。
【００２７】
ここで、例えば、前記情報管理装置は、さらに、ネットワークを介して、前記第１のサーバおよび前記第２のサーバに、前記所定ルールを送信し、前記第１のサーバは、記憶している前記第１のユーザ情報を前記所定ルールで匿名化することで前記第１のユーザ情報から前記第１の匿名化ユーザ情報を生成し、記憶している前記機器履歴情報と、生成した前記第１の匿名化ユーザ情報とを、前記情報管理装置に送信し、前記第２のサーバは、記憶している前記第２のユーザ情報を前記所定ルールで匿名化することで前記第２のユーザ情報から前記第２の匿名化ユーザ情報を生成し、記憶している前記サービス履歴情報と、生成した前記第２の匿名化ユーザ情報とを、前記情報管理装置に送信するとしてもよい。
【００２８】
なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なＣＤ－ＲＯＭなどの記録媒体記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。
【００２９】
以下、図面を参照しながら、本発明の一態様に係る情報管理方法および情報管理システムについて説明する。
【００３０】
なお、以下で説明する実施の形態は、いずれも本発明の一具体例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置および接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。
【００３１】
（実施の形態１）
１．システムの構成
以下、実施の形態１に係る情報管理システム１３について図面を参照しながら説明する。
【００３２】
１．１　情報管理システム１３の全体構成
図１は、実施の形態１に係る情報管理システムの全体構成の一例を示す図である。情報管理システム１３は、メーカサーバ１００ｃ、ポータルサーバ２００ｃ、サービスプロバイダサーバ３００ｃ～３００ｅ、機器４００、および、ユーザ端末５００から構成される。
【００３３】
ここで、機器４００は、例えばテレビや体組成計、ランニングマシン、エアロバイク（登録商標）、電動アシスト自転車などの機器である。機器４００は、メーカサーバ１００ｃを有するメーカで製造されており、機器履歴を収集する。ユーザ端末５００は、例えばパソコンや、携帯電話などの携帯端末である。
【００３４】
１．２　メーカサーバ１００ｃの構成
図２は、実施の形態１に係るメーカサーバ１００ｃの構成の一例を示すブロック図である。メーカサーバ１００ｃは、第１のサーバの一例であり、履歴ＤＢ制御部１０１、一時識別子生成部１０２、証明書生成部１０３、証明書検証部１０４、履歴ＤＢ１０５、機器制御指示部１０６、機器制御情報ＤＢ１０７、通信部１０８、および、匿名化部１２１を備える。
【００３５】
匿名化部１２１は、通信部１０８がポータルサーバ２００ｃから受信した匿名化ルール（所定ルール）に従って、個人情報ＤＢが格納するユーザ情報のうち該当するユーザ情報

を匿名化する。ここで、ユーザ情報とは、ユーザを特定可能なユーザの個人情報であり、ユーザを特定可能な属性情報を含む情報である。

【００３６】

履歴ＤＢ制御部１０１は、履歴ＤＢ１０５を制御し、ユーザの個人情報（ユーザ情報）と、ユーザが使用した機器４００の動作履歴を示す機器履歴（機器履歴情報）と、ユーザの個人情報（ユーザ情報）および機器履歴に対応する一時識別子と、機器履歴証明書とを管理する。

【００３７】

例えば、履歴ＤＢ制御部１０１は、ポータルサーバ２００ｃに機器履歴を提供（送信）するときに、ユーザＩＤに対応した一時識別子の生成を一時識別子生成部１０２へ依頼し、匿名化部１２１にポータルサーバ２００ｃから受信した匿名化ルール（所定ルール）に従って、個人情報ＤＢに格納されている該当ユーザ情報（該当ユーザの個人情報）の匿名化を依頼する。

【００３８】

また、履歴ＤＢ制御部１０１は、例えば、一時識別子生成部１０２からユーザＩＤと一時識別子とを受信し、匿名化部１２１から匿名化されたユーザ情報（匿名化ユーザ情報）を受信すると、履歴ＤＢ１０５内でユーザＩＤと一時識別子との紐付けを行い、一時識別子と匿名化ユーザ情報と機器履歴とを対応付ける署名生成を証明書生成部１０３に依頼する。

【００３９】

また、履歴ＤＢ制御部１０１は、例えば、証明書生成部１０３で受信した機器履歴証明書を、対応するユーザＩＤと一時識別子とを紐付けて管理する。履歴ＤＢ制御部１０１は、証明書検証部１０４で提案情報証明書の検証が成功すると、ユーザに対するサービス提案を示す提案情報を受信し、機器制御指示部１０６へ提案情報に基づいた機器の機器制御を依頼する。機器制御指示部１０６から機器制御情報を受信すると、一時識別子に紐付けられたユーザＩＤに基づいて、機器制御情報を該当ユーザに提供する。

【００４０】

一時識別子生成部１０２は、ユーザＩＤに対応した一時識別子を生成する。

【００４１】

例えば、一時識別子生成部１０２は、履歴ＤＢ制御部１０１から依頼を受信すると、ユーザＩＤから一時識別子を生成する。なお、一時識別子の生成方法は、ユーザＩＤと一意に紐付けできればよい。例えば、一時識別子をランダムに生成するとしてもよいし、ユーザＩＤに任意の暗号鍵を用いて暗号化した結果を一時識別子としてもよいし、ユーザＩＤに一方向性関数を用いて計算した結果を一時識別子としてもよい。また、一時識別子には、ユーザの個人情報が特定できない情報を含めてもよい。例えば、性別や年代などを含むとしてもよい。

【００４２】

証明書生成部１０３は、履歴ＤＢ制御部１０１から一時識別子と機器履歴と匿名化ユーザ情報を受信すると、機器履歴証明書を生成する。ここで、図３に実施の形態１に係る機器履歴証明書の構成の一例を示す。機器履歴証明書は、図３に示すように、一時識別子と匿名化ユーザ情報と機器履歴とに対し、証明書生成部１０３に保持する署名生成鍵（図示していない）で署名（メーカ署名）を生成し、一時識別子と匿名化ユーザ情報と機器履歴とを紐付けた上で署名（メーカ署名）を付与した証明書である。

【００４３】

証明書生成部１０３は、機器履歴証明書を生成後、機器履歴証明書と署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）とを送信する。ここで、公開鍵証明書は、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。なお、署名生成は、一時識別子と機器履歴を結合した値のハッシュ値に対して、署名を生成するとしてもよい。

【００４４】

証明書検証部１０４は、ポータルサーバ２００ｃから通信部１０８経由で提案情報証明書と署名検証鍵を含んだ公開鍵証明書とを受信し、署名の検証を行う。提案情報証明書の署名検証では、まず機器履歴証明書と提案情報とに対して、ポータルサーバ署名が正しいかを検証する。ポータルサーバ署名が正しい場合、機器履歴証明書のメーカサーバ署名が正しいかを検証する。メーカサーバ署名も正しい場合にのみ、提案情報証明書が正しいと判断する。提案情報証明書が正しい場合、一時識別子と匿名化ユーザ情報と提案情報とを履歴ＤＢ制御部１０１へ送信する。

【００４５】

履歴ＤＢ１０５は、個人情報ＤＢ、機器履歴ＤＢ、一時識別子および機器履歴証明書を記憶する。ここで、個人情報ＤＢは、ユーザの基本プロフィールデータである、氏名や住所などの情報を属性情報として含むユーザ情報を格納する。機器履歴ＤＢは、ユーザの保有する家電機器等の機器４００の操作履歴（例えばＴＶのチャンネル操作履歴）や、機器４００を用いたユーザの情報履歴（例えば体組成計を用いたユーザの体重の履歴）を格納する。

【００４６】

機器制御指示部１０６は、履歴ＤＢ制御部１０１から機器制御の依頼を受信すると、機器制御情報ＤＢ１０７で対応する機器４００の機器制御情報を検索し、機器制御情報を履歴ＤＢ制御部１０１へ送信する。ここで、機器制御情報とは、機器４００を制御するための制御プログラムを含む情報である。機器制御情報は、例えば、ランニングマシンでの動作速度と時間と制御する制御プログラムを含んでいたりしてもよいし、電動アシスト自転車のアシスト機能の強度を制御する制御プログラムを含んでいてもよい。つまり、機器制御情報は、機器の制御に関連する情報を含んでいればよい。

【００４７】

機器制御情報ＤＢ１０７は、機器４００の機器制御情報を記憶する。

【００４８】

通信部１０８は、ポータルサーバ２００ｃや機器４００、ユーザ端末５００との通信を行う。通信部１０８は、ポータルサーバ２００ｃやユーザ端末５００とのＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）通信を行う。ＳＳＬ通信に必要な証明書は通信部１０８で記憶する。また、通信部１０８は、ポータルサーバ２００ｃから匿名化のルール（所定ルール）を受信する。匿名化のルール（所定ルール）は、個人情報ＤＢが格納するユーザ情報に含まれる属性情報のうち、削除または抽象化すべき属性情報を規定するものである。

【００４９】

以上のように、メーカサーバ１００ｃは、第１のユーザが使用する機器４００の動作履歴を示す機器履歴と、第１のユーザを特定可能な属性情報を含む第１のユーザ情報とを記憶する。メーカサーバ１００ｃは、記憶している第１のユーザ情報を所定ルール（匿名化ルール）に従って匿名化することで第１の匿名化ユーザ情報を生成し、記憶している機器履歴と、生成した第１の匿名化ユーザ情報とを、ポータルサーバ２００ｃに送信する。

【００５０】

１．３　ポータルサーバ２００ｃの構成

図４は、実施の形態１に係るポータルサーバ２００ｃの構成の一例を示すブロック図である。ポータルサーバ２００ｃは、情報を管理する情報管理装置の一例であり、提案情報生成部２０１、提案情報ＤＢ２０２、証明書生成部２０３、証明書検証部２０４、通信部２０５、および、匿名化ルール生成部２１１を備える。

【００５１】

匿名化ルール生成部２１１は、ユーザに対するサービス提案を示す提案情報の生成に必要な情報を取得するため、メーカサーバ１００ｃやサービスプロバイダサーバ３００ｃ等が保持するユーザ情報（個人情報）を匿名化する匿名化ルール（所定ルール）を生成する。ここで、匿名化ルールには、上述したように、ユーザ情報（ユーザの個人情報）に含まれる属性情報のうち、削除または抽象化すべき属性情報が規定されている。また、匿名化

ルール生成部２１１は、メーカサーバ１００ｃが記憶する機器履歴により示される動作の種類とサービスプロバイダサーバ３００ｃ等が記憶するサービス履歴により示されるサービスの種類との組み合わせに基づいて決定する。これは、サービス履歴の内容やユーザが使用する機器に依存して、当該ユーザに対する提案情報も異なってからである。ユーザ情報に含まれる属性情報のうちユーザを特定できる属性情報は削除または抽象化する必要があるものの、ユーザ情報に含まれる属性情報のうちユーザを特定できない属性情報は、サービスの種類や動作の種類の組み合わせにより削除または抽象化するかしないかを決定すればよい。

【００５２】

図５は、実施の形態１に係る匿名化ルールの一例を示した図である。図５には、メーカサーバ１００ｃからの履歴情報とフィットネスサービスからのサービス履歴情報とから提案情報を生成する場合の匿名化ルールが示されている。

【００５３】

より具体的には、図５に示す匿名化ルールでは、名前の項目を削除し、住所の項目は市町村までの情報とし、市町村以下の番地などは削除する旨規定されている。また、生年月日は抽象化し、月や日は削除して年までとする旨規定されている。また、性別はそのまま提供し、メールや趣味は削除する旨規定されている。

【００５４】

つまり、匿名化ルールには、ユーザ情報（ユーザの個人情報）に含まれる属性情報のうち、削除または抽象化すべき属性情報が規定されているが、ユーザの性別、年齢、年代、住所およびまたは職業のうち少なくとも一の属性情報を匿名化ユーザ属性情報に含むように規定されている。このように、ユーザを特定できないものの提案情報の生成が可能な程度に、各サーバが保持するユーザ情報（個人情報）に含まれる属性情報のうちの一部の属性情報が削除または抽象化される。

【００５５】

提案情報生成部２０１は、複合情報として関連付けて管理されている機器履歴とサービス履歴とに基づいて、生成した第１のユーザに対するサービス提案を示す提案情報を生成する。そして、提案情報生成部２０１は、生成した提案情報を、メーカサーバ１００ｃを介してユーザへ提供する。

【００５６】

より具体的には、提案情報生成部２０１は、メーカサーバ１００ｃから受信した機器履歴証明書に含まれる機器履歴と、サービスプロバイダサーバ３００ｃ等から受信したサービス履歴と、提案情報ＤＢ２０２に記憶されている提案情報とに基づいて、ユーザへの提案情報を生成する。例えば、提案情報生成部２０１は、メーカサーバ１００ｃから受信した一時識別子と匿名化ユーザ情報と機器履歴と、サービスプロバイダサーバ３００ｃ等から受信した一時識別子と匿名化ユーザ情報とサービス情報とに基づいて、提案情報を生成する。なお、提案情報生成部２０１は、生成した提案情報は提案情報ＤＢへ記憶する。

【００５７】

また、提案情報生成部２０１は、提案情報を生成後、機器履歴証明書と提案情報とから提案情報証明書の生成を証明書生成部２０３へ依頼する。証明書生成部２０３から提案情報証明書を受信すると、メーカサーバ１００ｃに提案情報証明書を送信する。

【００５８】

提案情報ＤＢ２０２は、ユーザへ提案した提案情報を記憶する。

【００５９】

証明書生成部２０３は、提案情報生成部２０１から提案情報と機器履歴証明書を受信すると、提案情報証明書を生成する。図６に実施の形態１に係る提案情報証明書の構成の一例を示す。図６に示す提案情報証明書は、機器履歴証明書と提案情報とを紐付けた上で、証明書生成部２０３に保持する署名生成鍵（図示していない）で生成された署名（ポータルサーバ署名）を付与した証明書である。

【００６０】

証明書生成部２０３は、提案情報証明書を生成後、提案情報証明書と、署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）とを送信する。公開鍵証明書は、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。なお、署名生成は、機器履歴証明書と提案情報を結合した値のハッシュ値に対して、署名を生成するとしてもよい。

【００６１】

証明書検証部２０４は、メーカサーバ１００ｃから通信部２０５経由で機器履歴証明書と署名検証鍵を含んだ公開鍵証明書とを受信すると、署名の検証を行う。機器履歴証明書の署名検証では、機器履歴証明書に含まれる一時識別子と匿名化ユーザ情報と機器履歴とに対して、メーカサーバ署名が正しいかを検証する。メーカサーバ署名が正しい場合、一時識別子と匿名化ユーザ情報と機器履歴とを提案情報生成部２０１へ送信する。

【００６２】

通信部２０５は、メーカサーバ１００ｃやサービスプロバイダサーバ３００ｃ等との通信を行う。メーカサーバ１００ｃやサービスプロバイダサーバ３００ｃ等との通信ではＳＳＬ通信を行う。ＳＳＬ通信に必要な証明書は通信部２０５で記憶する。また、通信部２０５は、匿名化ルール生成部２１１により生成された匿名化ルール（所定ルール）を、ネットワークを介して、メーカサーバ１００ｃおよびサービスプロバイダサーバ３００ｃ等に送信する。

【００６３】

以上のように、ポータルサーバ２００ｃは、ネットワークを介して、メーカサーバ１００ｃから、機器履歴と、第１のユーザを特定可能な属性情報を含む第１のユーザ情報が匿名化ルールに従って匿名化された第１の匿名化ユーザ情報とを受信する。また、ポータルサーバ２００ｃは、ネットワークを介して、サービスプロバイダサーバ３００ｃから、サービス履歴と、第２のユーザを特定可能な属性情報を含む第２のユーザ情報が匿名化ルールに従って匿名化された第２の匿名化ユーザ情報とを受信する。そして、ポータルサーバ２００ｃは、第１の匿名化ユーザ情報と第２の匿名化ユーザ情報とが同一または類似すると判断した場合に、受信した第１のユーザの機器履歴と第１のユーザと同一または類似の第２のユーザのサービス履歴とを関連付けて複合情報として管理する。そして、ポータルサーバ２００ｃは、管理する複合情報データに基づいて、第１のユーザに対するサービス提案を示す提案情報を生成し、生成した提案情報を、メーカサーバ１００ｃを介して前記第１のユーザへ提供する。

【００６４】

なお、ポータルサーバ２００ｃは、提案情報を、メーカサーバ１００ｃを介して、ユーザに提供するとしたが、それに限らない。ユーザ端末５００が、メーカサーバ１００ｃではなくサービスプロバイダサーバ３００ｃとネットワークを介して接続されているとした場合には、サービスプロバイダサーバ３００ｃを介して、第２のユーザに対して提案情報を提供すればよい。

【００６５】

１．４　サービスプロバイダサーバ３００ｃの構成

図７は、実施の形態１に係るサービスプロバイダサーバ３００ｃの構成の一例を示すブロック図である。なお、サービスプロバイダサーバ３００ｄおよび３００ｅは、サービスプロバイダサーバ３００ｃと同様の構成であるため、ここではサービスプロバイダサーバ３００ｃについてのみ説明を行う。

【００６６】

サービスプロバイダサーバ３００ｃは、第２のサーバの一例であり、履歴ＤＢ制御部３０１、一時識別子生成部３０２、履歴ＤＢ３０３、通信部３０４、証明書検証部３１２、証明書生成部３１３、および、匿名化部３２１を備える。

【００６７】

匿名化部３２１は、通信部３０４がポータルサーバ２００ｃから受信した匿名化ルール（所定ルール）に従って、個人情報ＤＢ格納するユーザ情報のうち該当するユーザ情報を

匿名化する。

【００６８】

履歴ＤＢ制御部３０１は、履歴ＤＢ３０３を制御し、ユーザの個人情報（ユーザ情報）と、ユーザが享受したサービスの履歴を示すサービス履歴と、ユーザの個人情報（ユーザ情報）とサービス履歴とに対応する一時識別子とを管理する。ここで、サービス履歴は、フィットネスに関するサービスを受けた履歴を示す情報である。例えば、サービス履歴には、ＸＸＸ年Ｙ月Ｚ日に上級エアロ１セット、バイク３０分のトレーニングを受けた旨を示す履歴情報が記録されている。

【００６９】

履歴ＤＢ制御部３０１は、ポータルサーバ２００ｃにサービス履歴を提供（送信）するときに、ユーザＩＤに対応した一時識別子の生成を一時識別子生成部３０２へ依頼し、匿名化部３２１にポータルサーバ２００ｃから受信した匿名化ルール（所定ルール）に従って、個人情報ＤＢに格納される該当ユーザ情報（該当ユーザの個人情報）の匿名化を依頼する。

【００７０】

また、履歴ＤＢ制御部３０１は、例えば、一時識別子生成部３０２からユーザＩＤと一時識別子とを受信し、匿名化部３２１から匿名化されたユーザ情報（匿名化ユーザ情報）を受信すると、履歴ＤＢ３０３内でユーザＩＤと一時識別子との紐付けを行い、一時識別子と匿名化ユーザ情報とサービス履歴とを対応付けて管理する。履歴ＤＢ制御部３０１は、ポータルサーバ２００に、一時識別子と匿名化ユーザ情報とサービス履歴とをサービス履歴情報として送信する。

【００７１】

一時識別子生成部３０２は、ユーザＩＤに対応した一時識別子を生成する。例えば、一時識別子生成部３０２は、履歴ＤＢ制御部３０１から依頼を受信すると、ユーザＩＤから一時識別子を生成する。なお、一時識別子の生成方法は、ユーザＩＤと一意に紐付けできればよく、ランダムに生成してもよい。また、ユーザＩＤに任意の暗号鍵を用いて暗号化した結果を一時識別子としてもよいし、ユーザＩＤに一方向性関数を用いて計算した結果を一時識別子としてもよい。また、一時識別子には、ユーザの個人情報が特定できない情報を含めてもよい。例えば、性別や年代などを含むとしてもよい。

【００７２】

証明書生成部３１３は、履歴ＤＢ制御部３０１から一時識別子と機器履歴と匿名化ユーザ情報を受信すると、サービス履歴証明書を生成する。ここで、図８にサービス履歴証明書の構成の一例を示す。サービス履歴証明書は、一時識別子と匿名化ユーザ情報とサービス履歴とに対し、証明書生成部３１３に保持する署名生成鍵（図示していない）で署名を生成し、一時識別子と匿名化ユーザ情報とサービス履歴と紐付けた上で署名（サービスプロバイダ署名）を付与した証明書である。

【００７３】

証明書生成部３１３は、サービス履歴証明書を生成後、サービス履歴証明書と署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）とを送信する。

【００７４】

証明書検証部３１２は、ポータルサーバ２００ｃから通信部３０４経由で提案情報証明書と署名検証鍵を含んだ公開鍵証明書とを受信し、署名の検証を行う。上述した証明書検証部３１２は、証明書検証部１０４と同様であるため、説明を省略する。

【００７５】

履歴ＤＢ３０３は、個人情報ＤＢ、サービス履歴ＤＢ、および、一時識別子を記憶する。ここで、個人情報ＤＢは、ユーザの基本プロフィールデータである、氏名や住所などの情報をユーザ情報として格納する。サービス履歴ＤＢは、ユーザが享受したサービスの履歴を格納する。

【００７６】

通信部３０４は、ポータルサーバ２００ｃとの通信を行う。通信部３０４は、ポータル

サーバ２００ｃとの通信ではＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）通信を行う。ＳＳＬ通信に必要な証明書は通信部３０４で記憶する。また、通信部３０４は、ポータルサーバ２００ｃから匿名化のルール（所定ルール）を受信する。

【００７７】

以上のように、サービスプロバイダサーバ３００ｃは、第２のユーザが享受したサービスの履歴を示すサービス履歴と、第２のユーザを特定可能な属性情報を含む第２のユーザ情報を記憶する。サービスプロバイダサーバ３００ｃは、記憶している第２のユーザ情報に含まれる属性情報を上記匿名化ルールに従って匿名化することで第２のユーザ情報から第２の匿名化ユーザ情報を生成し、記憶しているサービス履歴と、生成した第２の匿名化ユーザ情報とを、ポータルサーバ２００ｃに送信する。

【００７８】

１．５　情報管理システム１３の動作

情報管理システム１３の動作には、以下のものがある。

【００７９】

（１）ユーザがユーザ端末５００を用いて、メーカサーバ１００ｃに登録するときの処理

（２）ユーザがメーカサーバ１００ｃに家電機器を登録するときの処理

（３）ユーザの機器４００から家電履歴情報を機器履歴ＤＢにアップロードするときの処理

（４）ポータルサーバ２００からユーザに提案情報を提供する処理

【００８０】

なお、（１）から（３）の処理は実施の形態２で説明することとし、本実施の形態での説明を省略する。

【００８１】

１．５．１　ポータルサーバ２００からユーザに提案情報を提供するときの処理

図９から図１２は、ポータルサーバ２００ｃからユーザに提案情報を提供する処理のシーケンス図である。なお、この提案情報の提供は、定期的または不定期に行われる。

【００８２】

Ｓ４０１において、メーカサーバ１００ｃとポータルサーバ２００ｃとの間でＳＳＬ認証を行い、暗号通信路を確立する。

【００８３】

次に、Ｓ４０２において、ポータルサーバ２００ｃは、匿名化ルールを生成し、メーカサーバ１００ｃに匿名化ルールを送信する。

【００８４】

次に、Ｓ４０３において、メーカサーバ１００ｃは、受信した匿名化ルールに基づき、ユーザの個人情報（ユーザ情報）を匿名化し、ユーザＩＤから一時識別子を生成する。

【００８５】

次に、Ｓ４０４において、メーカサーバ１００ｃは一時識別子と匿名化ユーザ情報と機器履歴とに対して署名（メーカ署名）を生成し、図３に示すような機器履歴証明書を生成する。そして、メーカサーバ１００ｃは、生成した機器履歴証明書と公開鍵証明書とをポータルサーバ２００ｃに送信する。

【００８６】

次に、Ｓ４０５において、ポータルサーバ２００ｃは、メーカサーバ１００ｃから機器履歴証明書と公開鍵証明書とを受信し、これら証明書の検証を行う。これら証明書の検証が失敗した場合、メーカサーバ１００ｃにエラーを通知する。

【００８７】

次に、Ｓ４０６において、ポータルサーバ２００ｃは、機器履歴証明書の検証が成功した場合、例えばサービスプロバイダサーバ３００ｃとの間でＳＳＬ認証を行い、暗号化通信路を確立する。

【００８８】

次に、Ｓ４０７において、ポータルサーバ２００ｃは、サービスプロバイダサーバ３００ｃに受信した機器履歴情報に関連するサービス履歴の取得依頼を匿名化ルールとともに送信する。

【００８９】

次に、Ｓ４０８において、サービスプロバイダサーバ３００ｃは、ポータルサーバ２００ｃからサービス情報取得依頼と匿名化ルールとを受信すると、匿名化ルールに基づき、ユーザの個人情報（ユーザ情報）を匿名化し、ユーザＩＤから一時識別子を生成する。

【００９０】

次に、Ｓ４０９において、サービスプロバイダサーバ３００ｃは、一時識別子と匿名化ユーザ情報とサービス履歴とに対して署名を生成し、図８に示すようなサービス履歴証明書を生成する。そして、サービスプロバイダサーバ３００ｃは、ポータルサーバ２００ｃにサービス履歴証明書と公開鍵証明書とを送信する。

【００９１】

次に、Ｓ４１０において、ポータルサーバ２００ｃは、サービスプロバイダサーバ３００ｃからサービス履歴証明書と公開鍵証明書とを受信し、これら証明書の検証を行う。これら証明書の検証が失敗した場合、サービスプロバイダサーバ３００ｃにエラーを通知する。

【００９２】

また、ポータルサーバ２００は、受信した機器履歴証明書とサービス履歴証明書とが、匿名化ルールに従って匿名化されているかを確認する。なお、匿名化されたユーザ情報が同一でもなく類似でもない場合、メーカサーバ１００ｃとサービスプロバイダサーバ３００ｃにエラーを通知する。

【００９３】

次に、Ｓ４１１において、ポータルサーバ２００ｃは、メーカサーバ１００ｃから受信した機器履歴証明書と、サービスプロバイダサーバ３００ｃから受信したサービス履歴証明書とを記録する。

【００９４】

次に、Ｓ４１２において、ポータルサーバ２００ｃは、機器履歴証明書の機器履歴とサービス履歴証明書のサービス履歴と匿名化ユーザ情報とに基づいて、提案情報を生成する。

【００９５】

次に、Ｓ４１３において、ポータルサーバ２００ｃは、生成した提案情報と機器履歴証明書とに対して署名を生成し、図６に示したような提案情報証明書を生成する。

【００９６】

次に、Ｓ４１４において、ポータルサーバ２００ｃは生成した提案情報証明書をメーカサーバ１００ｃに送信する。

【００９７】

次に、Ｓ４１５において、メーカサーバ１００ｃは、受信した提案情報証明書を検証する。メーカサーバ１００ｃは、提案情報証明書の検証が失敗した場合、ポータルサーバ２００ｃにエラーを通知する。

【００９８】

次に、Ｓ４１６において、メーカサーバ１００ｃが提案情報証明書の検証が成功した場合、メーカサーバ１００ｃは、提案情報証明書に含まれる機器履歴証明書から履歴ＤＢ１０５内の機器履歴証明書を検索する。検索した機器履歴証明書に含まれる一時識別子と対応するユーザＩＤを検索し、提案情報を提供すべきユーザＩＤを特定する。

【００９９】

次に、Ｓ４１７において、メーカサーバ１００ｃは、特定したユーザＩＤへ提案情報を提供する。このとき、提案情報が機器４００の制御情報を含む場合、メーカサーバ１００ｃは、ユーザ端末５００へ機器制御情報がある旨の通知を行い、ユーザ端末５００からＯＫとの通知が来た場合、制御情報を送信する。なお、提案情報が機器４００の制御情報を

含まない場合、ユーザ端末５００に提案情報を送信する。
【０１００】
１．６　効果
以上、実施の形態１によれば、ポータルサーバ２００ｃが提供する匿名化ルールに従って匿名化されたユーザ情報を用いることで、メーカサーバ１００ｃとポータルサーバ２００ｃとサービスプロバイダサーバ３００ｃ等とを連携させることができるので、ポータルサーバ２００ｃは、ユーザの機器履歴と当該ユーザと同一または類似のサービス履歴とを用いてサービスの提案情報を当該ユーザに提供することができる。なお、メーカサーバ１００ｃとサービスプロバイダサーバ３００ｃ等は、ポータルサーバ２００ｃに対して、ユーザが特定できないもののサービスの提案情報を作成できる程度に匿名化されたユーザ情報を提供するに留まる。つまり、メーカサーバ１００ｃとサービスプロバイダサーバ３００ｃ等は、ポータルサーバ２００ｃに対してユーザの個人情報を提供しない。このようにして、ユーザのプライバシを保護しつつ、提案情報を生成することができる情報管理方法および情報管理システムを実現することができる。
【０１０１】
それにより、ユーザはメーカサーバ１００ｃやサービスプロバイダサーバ３００ｃに登録するときにのみ、ユーザの個人情報（ユーザ情報）の登録を行えばよい。つまり、ユーザは、ポータルサーバ２００ｃは、個人情報（ユーザ情報）を提供しなくても、ポータルサーバ２００ｃから提案情報を取得することができる。
【０１０２】
また、メーカサーバ１００ｃは、メーカサーバ１００ｃが提供する機器履歴証明書に対して、提案情報証明書を生成することで、提供した機器履歴証明書が改ざんされたり、別のユーザの機器履歴情報に対する提案情報にすり替わっていたりすることを検証することができる。
【０１０３】
なお、上記では、フィットネスサービスＡを提供するサービスプロバイダサーバ３００ｃとポータルサーバ２００ｃとが連携する場合の例について説明したため、サービス履歴は、フィットネスに関するサービスを受けた履歴を示す情報であるとして説明したが、それに限らない。例えば、ダイエットサービスＢを提供するサービスプロバイダサーバ３００ｄや保険サービスＣを提供するサービスプロバイダサーバ３００ｅと、ポータルサーバ２００ｃとが連携する場合には、サービス履歴は、ダイエットサービスＢや保険サービスＣに関するサービスを受けた履歴を示す。
【０１０４】
さらに、サービス履歴は、上記の例に限定されず、医療を含む健康管理に関するサービスを受けた履歴を示す情報であってもよいし、教育サービスを受けた履歴を示す情報であってもよいし、交通サービスを受けた履歴を示す情報であってもよい。
【０１０５】
なお、サービス履歴が教育サービスを受けた履歴を示す情報である場合、サービス履歴には、例えば通信教育サービスを受けた日時や通信教育サービスの内容を示す履歴情報が記録される。
【０１０６】
この場合、たとえば、通信教育サービスを提供するサービスプロバイダは、当該ユーザと同一または類似のユーザが通信教育サービスを受けた日時や内容を示す履歴情報が記録されているサービス履歴をポータルサーバ２００ｃに送信（提供）する。メーカサーバ１００ｃは、ポータルサーバ２００ｃに例えば当該ユーザが視聴したテレビの内容等を示す視聴履歴が記録されている機器履歴を生成した第１の匿名化ユーザとともに送信する。それにより、ポータルサーバ２００ｃは、受信したサービス履歴や機器履歴等に基づいて、当該ユーザの興味のある事象に関する教育サービスを提案する提案情報を当該ユーザに提供することができる。
【０１０７】

（実施の形態２）
２．システムの構成
以下、実施の形態２に係る情報管理システム１０について、図面を参照しながら説明する。
【０１０８】
２．１　情報管理システム１０の全体構成
図１３は、実施の形態２に係る情報管理システムの全体構成の一例を示す図である。情報管理システム１１は、メーカサーバ１００、ポータルサーバ２００、サービスプロバイダサーバ３００、機器４００、および、ユーザ端末５００を備える。なお、実施の形態１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。
【０１０９】
２．２　メーカサーバ１００の構成
図１４は、実施の形態２に係るメーカサーバ１００の構成の一例を示すブロック図である。図１４に示すメーカサーバ１００は、履歴ＤＢ制御部１０１Ａ、一時識別子生成部１０２、証明書生成部１０３Ａ、証明書検証部１０４、履歴ＤＢ１０５、機器制御指示部１０６、機器制御情報ＤＢ１０７、通信部１０８から構成される。このメーカサーバ１００は、実施の形態１のメーカサーバ１００ｃに対して、匿名化部１２１がない点で構成が異なる。
【０１１０】
履歴ＤＢ制御部１０１Ａは、履歴ＤＢ１０５を制御し、ユーザの個人情報（ユーザ情報）と、ユーザが使用した機器４００の動作履歴を示す機器履歴（機器履歴情報）と、ユーザの個人情報（ユーザ情報）と機器履歴に対応する一時識別子と、機器履歴証明書とを管理する。
【０１１１】
例えば、履歴ＤＢ制御部１０１Ａは、ポータルサーバ２００に機器履歴情報を提供するときに、ユーザＩＤに対応した一時識別子の生成を一時識別子生成部１０２へ依頼する。また、履歴ＤＢ制御部１０１Ａは、例えば、一時識別子生成部１０２からユーザＩＤと一時識別子とを受信すると、履歴ＤＢ１０５内でユーザＩＤと一時識別子との紐付けを行い、一時識別子と機器履歴とを対応付ける署名生成を証明書生成部１０３Ａに依頼する。履歴ＤＢ制御部１０１Ａは、証明書生成部１０３Ａで受信した機器履歴証明書を対応するユーザＩＤと一時識別子と紐付けて管理する。履歴ＤＢ制御部１０１Ａは、証明書検証部１０４で提案情報証明書の検証が成功後、ユーザに対するサービス提案を示す提案情報を受信し、機器制御指示部１０６へ提案情報に基づいた家電機器の機器制御を依頼する。また、履歴ＤＢ制御部１０１Ａは、機器制御指示部１０６から機器制御情報を受信すると、ユーザＩＤに基づいて、機器制御情報を該当ユーザに提供する。
【０１１２】
一時識別子生成部１０２は、ユーザＩＤに対応した一時識別子を生成する。履歴ＤＢ制御部１０１Ａから依頼を受信し、ユーザＩＤから一時識別子を生成する。このとき、一時識別子の生成方法は、実施の形態１で説明したとおりであるため、説明を省略する。
【０１１３】
証明書生成部１０３Ａは、履歴ＤＢ制御部１０１Ａから一時識別子と機器履歴とを受信した場合に、機器履歴証明書を生成する。ここで、図１５に実施の形態２に係る機器履歴証明書の構成の一例を示す。図１５に示すように、機器履歴証明書は、一時識別子と機器履歴とに対し、証明書生成部１０３Ａに保持する署名生成鍵（図示していない）で生成された署名（メーカ署名）を、一時識別子と機器履歴とを紐付けた上で付与した証明書である。証明書生成部１０３Ａは、機器履歴証明書を生成後、機器履歴証明書と署名生成鍵とに対応する署名検証鍵を含んだ公開鍵証明書（図示していない）を送信する。ここで、公開鍵証明書は、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。なお、署名生成は、一時識別子と機器履歴とを結合した値のハッシュ値に対して、署名を生成するとしてもよい。

【０１１４】
証明書検証部１０４は、ポータルサーバ２００から通信部１０８経由で提案情報証明書と署名検証鍵を含んだ公開鍵証明書を受信し、署名の検証を行う。提案情報証明書の署名検証は、実施の形態１で説明したとおりであるため、説明を省略する。証明書検証部１０４は、提案情報証明書が正しい場合、一時識別子と提案情報を履歴ＤＢ制御部１０１Ａへ送信する。
【０１１５】
履歴ＤＢ１０５は、個人情報ＤＢ、機器履歴ＤＢ、一時識別子および機器履歴証明書を記憶する。
【０１１６】
ここで、個人情報ＤＢは、実施の形態１と同様に、ユーザの基本プロフィールデータである、氏名や住所などの情報を属性情報として含むユーザ情報を格納する。図１６は実施の形態２に係る個人情報ＤＢの構成の一例を示した図である。図１６に示す例では、ユーザ情報は、ユーザの氏名、住所、生年月日、性別および趣味を項目（属性情報の項目）として含んでいる。これら項目の設定はシステムで種々設定すればよい。図１６に示す例では、ＩＤ１１のユーザ情報の属性情報として、氏名：山田美紀、住所：大阪市福島区３丁目１０、生年月日：１９８０年１０月５日、性別：女、趣味：　エアロビクスが登録されている。また、ＩＤ１２のユーザ情報の属性情報としては、氏名：佐藤次郎、住所：東京都港区１丁目１９、生年月日：１９９０年３月３日、性別：　男、趣味：　読書が登録されている。これらユーザ情報に含まれる属性情報（共通する属性情報の項目）は、ユーザがメーカサーバ１００に始めて登録するときに、ユーザが入力する属性情報である。
【０１１７】
また、機器履歴ＤＢは、ユーザの保有する家電機器等の機器４００の操作履歴（例えばＴＶのチャンネル操作履歴）や、機器４００を用いたユーザの機器履歴（例えば体組成計を用いたユーザの体重の履歴）を格納する。図１７は、実施の形態２に係る機器履歴ＤＢのＩＤリストの一例を示した図である。図１７に示す例では、機器４００は、例えば体組成計とＴＶと活動量計とであり、体組成計の機器履歴は、ＩＤＡ１のデータベースに格納され、ＴＶの機器履歴はＩＤＡ２のデータベースに格納され、活動量計の機器履歴はＩＤＡ３のデータベースに格納されていることを示している。
【０１１８】
図１８は、実施の形態２に係る家電履歴ＤＢに記録されているデータの一例を示した図である。図１８に示す例では、各家電履歴ＤＢは家電機器（機器４００）の種類ごとに構成され、それぞれユーザＩＤごとにその機器履歴（家電履歴情報）が記録される。より具体的には、ＩＤＡ１のデータベース、つまり体組成計のＤＢには、ユーザＩＤがＩＤ１１の家電履歴情報として、「２０１２．１．１　体重５５キログラム、体脂肪率１８％、２０１２．１．３　体重５６キログラム、体脂肪率１９％」と記録されている。これは２０１２．１．１に計測したときに、体重が５５キログラム、体脂肪率が１８％であったことを示し、また、２０１２．１．３には、体重５６キログラム、体脂肪率１９％であったことを示す。また、ユーザＩＤがユーザＩＤ１２の情報は、「２０１１．１２．３０　体重８０キログラム、体脂肪率２２％、２０１２．１．３　体重８２キログラム、体脂肪率２２％」と記録されている。一方、ＩＤＡ２のデータベース、ＴＶのＤＢには、ユーザＩＤがＩＤ１１の家電履歴情報として、「２０１２．１．１　１８：００　ドラマ、２０：００　ニュース、２０１２．１．３　１０：００　アニメ、１３：００　ドラマ」といったＴＶで視聴した番組の履歴が記録されている。なお、上記のような家電履歴情報（機器４００の機器履歴）は、ユーザが登録した家電からメーカサーバに定期的または不定期に情報がアップロードされる。
【０１１９】
機器制御指示部１０６は、履歴ＤＢ制御部１０１Ａから機器制御の依頼を受信すると、機器制御情報ＤＢ１０７から対応する家電機器（機器４００）の機器制御情報を検索し、機器制御情報を履歴ＤＢ制御部１０１Ａへ送信する。なお、機器制御情報は、実施の形態

１で説明したとおりであるため、説明を省略する。
【０１２０】
機器制御情報ＤＢ１０７は、機器４００の機器制御情報を記憶する。
【０１２１】
通信部１０８Ａは、ポータルサーバ２００や機器４００、ユーザ端末５００との通信を行う。ポータルサーバ２００やユーザ端末５００とのＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）通信を行う。ＳＳＬ通信に必要な証明書は通信部１０８で記憶する。
【０１２２】
以上のように、メーカサーバ１００は、ユーザが使用する機器４００の動作履歴を示す機器履歴と、ユーザを特定可能な属性情報を含むユーザ情報とを記憶している。メーカサーバ１００は、記憶しているユーザ情報に対応する一時識別子を生成し、記憶している機器履歴と、生成した一時識別子とを、ポータルサーバ２００に送信する。
【０１２３】
２．３　ポータルサーバ２００の構成
図１９は、実施の形態２に係るポータルサーバ２００の構成の一例を示すブロック図である。ポータルサーバ２００は、提案情報生成部２０１Ａ、提案情報ＤＢ２０２、証明書生成部２０３Ａ、証明書検証部２０４Ａ、および、通信部２０５を備える。ポータルサーバ２００は、実施の形態１のメーカサーバ１００ｃと比較して、匿名化ルール生成部２１１がない点で構成が異なる。
【０１２４】
提案情報生成部２０１Ａは、メーカサーバ１００から受信した機器履歴証明書に含まれる機器履歴とサービスプロバイダサーバ３００から受信したサービス履歴証明書に含まれるサービス履歴と提案情報ＤＢ２０２に記憶されている提案情報とに基づいて、ユーザに対する提案情報を生成する。提案情報の生成方法の詳細は後述する。提案情報生成部２０１Ａは、生成した提案情報は提案情報ＤＢへ記憶する。また、提案情報生成部２０１Ａは、提案情報を生成後、機器履歴証明書と提案情報から提案情報証明書の生成を証明書生成部２０３Ａへ依頼する。証明書生成部２０３Ａから提案情報証明書を受信すると、メーカサーバ１００へ提案情報証明書を送信する。
【０１２５】
提案情報ＤＢ２０２は、ユーザへ提案した提案情報を格納（記憶）する。
【０１２６】
ここで、図２０は、提案情報ＤＢ２０２の構成の一例を示す図である。図２０に示すように、格納されている提案情報は、提案情報のジャンルとサービス情報ＤＢとの項目から構成されている。より具体的には、ダイエットや番組おすすめのジャンルでは、ダイエットの提案サービス情報ＤＢがＩＤＳ１のデータベースに格納されていることが示されている。番組おすすめのジャンルでは、提案サービス情報ＤＢはＩＤＡ２のデータベースに格納されていることが示されている。
【０１２７】
図２１は、提案サービス情報ＤＢに記録されているデータの一例を示す図である。図２１に示す例では、提案サービス履歴ＤＢは、提案情報の種類ごとに構成され、提案サービス情報のＩＤごとにその提案情報が記録されている。例えば、ＩＤＳ１の提案情報では、ダイエットの提案情報として、３０代男性向けのダイエットプログラムや３０代女性向けのダイエットプログラムなどが記憶されている。なお、３０代女性向けのダイエットプログラムでは、例えばランニングマシンを３０分、エアロバイク（登録商標）を３０分などのプログラムを記憶する。また、ＩＤ２の提案情報では、番組おすすめの提案情報として、アニメ好きおすすめ番組やスポーツ好きおすすめ番組などが記憶されている。
【０１２８】
証明書生成部２０３Ａは、提案情報生成部２０１から提案情報と機器履歴証明書を受信すると、提案情報証明書を生成する。図２２に実施の形態２に係る提案情報証明書の構成

の一例を示す。図２２に示す提案情報証明書は、機器履歴証明書と提案情報とを紐付けた上で、証明書生成部２０３Ａに保持する署名生成鍵（図示していない）で生成された署名（ポータルサーバ署名）を付与した証明書である。証明書生成部２０３Ａは、提案情報証明書を生成後、提案情報証明書と署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）とを送信する。なお、公開鍵証明書は、実施の形態１と同様に、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。また、署名生成は、機器履歴証明書と提案情報を結合した値のハッシュ値に対して、署名を生成するとしてもよい。

【０１２９】

証明書検証部２０４Ａは、メーカサーバ１００から通信部２０５経由で機器履歴証明書と署名検証鍵を含んだ公開鍵証明書とを受信すると、署名の検証を行う。機器履歴証明書の署名検証では、機器履歴証明書に含まれる一時識別子と機器履歴とに対して、メーカサーバ署名が正しいかを検証する。メーカサーバ署名が正しい場合、一時識別子と機器履歴を提案情報生成部２０１へ送信する。

【０１３０】

通信部２０５Ａは、メーカサーバ１００やサービスプロバイダサーバ３００との通信を行う。メーカサーバ１００やサービスプロバイダサーバ３００との通信ではＳＳＬ通信を行う。ＳＳＬ通信に必要な証明書は通信部２０５で記憶する。

【０１３１】

２．３．１　提案情報の生成方法

提案情報生成部２０１Ａは、メーカサーバ１００から受信した一時識別子と機器履歴と、サービスプロバイダから受信した一時識別子とサービス情報とに基づいて、提案情報を生成する。以下では、ダイエットプログラムを提案情報として生成する場合の例を説明する。

【０１３２】

まず、提案情報生成部２０１Ａは、メーカサーバ１００から受信した機器履歴証明書に含まれる一時識別子を取得し、機器履歴の利用履歴すなわち体組成計である機器４００を利用したユーザの年代や体組成情報などを取得することができる。

【０１３３】

次に、提案情報生成部２０１Ａは、サービスプロバイダサーバ３００からユーザが享受したサービスの履歴を示すサービス履歴を取得する。ここでは、サービスプロバイダサーバ３００は、フィットネスクラブが有するものであり、提案情報生成部２０１Ａは、一時識別子とともにサービス履歴として、サービスプロバイダサーバ３００からフィットネスクラブの提供しているサービスプログラムを取得する。また、提案情報生成部２０１Ａは、サービスプロバイダサーバ３００から取得した一時識別子に基づき、提案情報を提供すべきユーザと同年代のサービス履歴を参照し、一時識別子に対応するユーザに対する提案情報を決定する。

【０１３４】

例えば、提案情報生成部２０１は、メーカサーバ１００から受信した一時識別子に対応するユーザが３０代女性であることがわかった場合、サービスプロバイダサーバ３００から受信した一時識別子に対応するユーザのうち３０代女性に紐付けられたサービス履歴を参照することで３０代女性向けの提供したサービスを検索する。提案情報生成部２０１は、検索結果したダイエットプログラムを、メーカサーバ１００から受信した一時識別子に対応するユーザに対する提案情報として決定する。ここで、ユーザが電動アシスト自転車を持っていた場合、ダイエットプログラムをエアロバイク（登録商標）で実行した場合と同様の負荷をかけるように、電動アシスト自転車に対して負荷をかける時間を決定して提案情報として提供する。つまり、このときの提案情報は、例えば、電動アシスト自転車で６０分間負荷をかけるといったことになる。このようにして、提案情報生成部２０１は、３０代女性向けのダイエットプログラムを提案情報として生成することができる。そして、ポータルサーバ２００は、この提案情報をメーカサーバ１００に提供することで、メー

カサーバ１００から電動アシスト自転車への制御情報をユーザに提供することができる。
【０１３５】
以上のように、ポータルサーバ２００は、ネットワークを介して、メーカサーバ１００から、機器履歴と一時識別子とを受信する。また、ポータルサーバ２００は、ネットワークを介して、サービスプロバイダサーバ３００から、サービス履歴と一時識別子とを受信する。そして、ポータルサーバ２００は、一時識別子に対応づけられたユーザ情報と機器履歴とサービス履歴とに基づいて、ユーザに対するサービス提案を示す提案情報を生成し、生成した提案情報を、メーカサーバ１００を介してユーザに提供する。
【０１３６】
２．４　サービスプロバイダサーバ３００の構成
図２３は、実施の形態２に係るサービスプロバイダサーバ３００の構成の一例を示すブロック図である。サービスプロバイダサーバ３００は、履歴ＤＢ制御部３０１Ａ、一時識別子生成部３０２、履歴ＤＢ３０３、および、通信部３０４Ａを備える。サービスプロバイダサーバ３００は、実施の形態１のサービスプロバイダサーバ３００ｃ等と比較して、匿名化部３２１がない点で構成が異なる。
【０１３７】
履歴ＤＢ制御部３０１Ａは、履歴ＤＢ３０３を制御し、ユーザの個人情報（ユーザ情報）と、ユーザが享受したサービスの履歴を示すサービス履歴と、ユーザの個人情報（ユーザ情報）とサービス履歴とに対応する一時識別子とを管理する。
【０１３８】
例えば、履歴ＤＢ制御部３０１Ａは、ポータルサーバ２００にサービス履歴情報を提供するときに、ユーザＩＤに対応した一時識別子の生成を一時識別子生成部３０２へ依頼する。また、履歴ＤＢ制御部３０１Ａは、例えば、一時識別子生成部３０２からユーザＩＤと一時識別子とを受信すると、履歴ＤＢ３０３内でユーザＩＤと一時識別子との紐付けを行い、一時識別子とサービス履歴とを対応付けて管理する。履歴ＤＢ制御部３０１Ａは、ポータルサーバ２００へ一時識別子とサービス履歴とをサービス履歴情報として送信する。図２４は、実施の形態２に係るサービス履歴情報の構成の一例を示した図である。
【０１３９】
一時識別子生成部３０２は、ユーザＩＤに対応した一時識別子を生成する。例えば、一時識別子生成部３０２は、履歴ＤＢ制御部３０１から依頼を受信すると、ユーザＩＤから一時識別子を生成する。なお、一時識別子の生成方法は、実施の形態１で説明したとおりであるため、説明を省略する。
【０１４０】
履歴ＤＢ３０３は、個人情報ＤＢ、サービス履歴ＤＢ、および一時識別子を記憶する。
【０１４１】
ここで、個人情報ＤＢは、ユーザの基本プロフィールデータである、氏名や住所などの情報を属性情報として含むユーザ情報として格納する。図２５は、本開示に係る個人情報ＤＢの構成の一例を示した図である。図２５に示す例では、ユーザ情報は、ユーザの氏名、住所、生年月日、性別および趣味を項目（属性情報の項目）として含んでいる。これら項目の設定はシステムで種々設定すればよい。図２５に示す例では、ＩＤ２１のユーザ情報の属性情報として、氏名：山田美紀、住所：大阪市福島区３丁目１０、生年月日：１９８０年１０月５日、性別：女、趣味：　エアロビクスが登録されている。また、ＩＤ２２のユーザ情報の属性情報としては、氏名：加藤五郎、住所：千葉市中央区１丁目１９、生年月日：１９７５年６月１日、性別：　男、趣味：　マラソンが登録されている。これらユーザ情報に含まれる属性情報（共通する属性情報の項目）は、ユーザがサービスプロバイダサーバ３００に始めて登録するときに、ユーザが入力する属性情報である。
【０１４２】
図２６は、サービス情報ＤＢに記録されているデータの一例を示す図である。図２６に示す例では、サービス履歴ＤＢは、提案サービスの履歴情報としてＩＤごとにそのサービス履歴が記録されている。例えば、ＩＤ２１の提供サービスの履歴情報には、「２０１１

．１２．２８　走らないエアロ２セット、ラン３０分、アドバイス、２０１２．１．３　上級エアロ１セット、バイク３０分」と記録されている。これは、２０１１．１２．２８には、走らないエアロ２セット、ラン３０分のトレーニングを受け、さらにトレーニングに関するアドバイスを受けたことを示す。同様にして、ＩＤ２２の提供サービスの履歴情報には、２０１２．１．３には、上級エアロ１セット、バイク３０分のトレーニングを受けたことが示されている。

【０１４３】

通信部３０４Ａは、ポータルサーバ２００との通信を行う。通信部３０４Ａは、ポータルサーバ２００ｃとの通信ではＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）通信を行う。ＳＳＬ通信に必要な証明書は通信部３０４Ａで記憶する。

【０１４４】

以上のように、サービスプロバイダサーバ３００は、ユーザが享受したサービスの履歴を示すサービス履歴と、ユーザを特定可能なユーザ情報とを記憶する。サービスプロバイダサーバ３００は、記憶しているユーザ情報に対応する一時識別子を生成し、記憶しているサービス履歴と、生成した一時識別子とを、ポータルサーバ２００に送信する。

【０１４５】

２．５　情報管理システム１０の動作

情報管理システム１０の動作には、以下のものがある。

【０１４６】

（１）ユーザがユーザ端末５００を用いて、メーカサーバ１００に登録するときの処理

（２）ユーザがメーカサーバ１００に家電機器を登録するときの処理

（３）ユーザの機器４００から家電履歴情報を機器履歴ＤＢにアップロードするときの処理

（４）ポータルサーバ２００からユーザに提案情報を提供する処理

【０１４７】

なお、ユーザがユーザ端末を用いて、サービスプロバイダサーバ３００に登録する処理は（１）の処理と同様のため、ここでは説明を省略する。また、ユーザのサービス履歴をサービスプロバイダサーバ３００へ登録する処理は、サービスプロバイダによって異なる。すなわち、ユーザがサービス履歴を登録してもよいし、サービスプロバイダ側で提供したサービス履歴を登録するとしてもよい。

【０１４８】

以下、それぞれについて図を用いて説明する。

【０１４９】

２．５．１　ユーザの登録処理時の動作

図２７は、ユーザがユーザ端末５００を用いてメーカサーバ１００に登録するときのシーケンス図である。

【０１５０】

まず、Ｓ１０１において、メーカサーバ１００とユーザ端末５００との間でＳＳＬ認証を行い、暗号通信路を確立する。ＳＳＬ認証およびＳＳＬ通信路については、ここでは詳しくは述べない。

【０１５１】

次に、Ｓ１０２において、ユーザ端末５００は、ユーザＩＤをメーカサーバ１００に送信する。メーカサーバ１００は、送信されたユーザＩＤがすでに登録されている場合にはその旨をユーザ端末５００に通知し、登録処理を終了する。一方、送信されたユーザＩＤが未登録である場合は、新規登録が可能である旨をユーザ端末５００に送信する。

【０１５２】

次に、Ｓ１０３において、ユーザはユーザ端末５００を介し、パスワード（以下、ＰＷとする）および個人情報を、所定の書式に従って入力する。なお、これらの情報は、上述したように、メーカサーバ１００における履歴ＤＢ１０５が有する個人情報ＤＢに記録される。また、ＰＷは、次回以降ユーザがメーカサーバ１００に接続する際に用いる。メー

カサーバ１００は、入力されたＰＷを例えば図１４におけるユーザ端末５００と通信する通信部１０８に記録し、次回以降の接続時に、ユーザＩＤおよび記録したＰＷと、ユーザからの入力されたユーザＩＤおよびＰＷとを比較して、一致するときに、接続を許可する。

【０１５３】

２．５．２　機器４００の登録処理時の動作

図２８は、ユーザがユーザ端末５００を用いて自身の家電機器４００を登録するときのシーケンス図である。ここで、ユーザは、ユーザ端末５００において、例えば、メーカアプリ（図示しない）を起動して登録処理を行うとして説明する。なお、ユーザは、ユーザ端末５００を用いてメーカサーバ１００に接続して登録するとしてもよい。

【０１５４】

まず、Ｓ１１１において、メーカサーバ１００とユーザ端末５００間でＳＳＬ認証を行い、暗号通信路を確立する。

【０１５５】

次に、Ｓ１１２において、ユーザは初期登録の際に設定したＰＷを入力する。メーカサーバ１００は、ユーザＩＤに対応して記録しているＰＷと比較し、一致していれば、認証成功とする。なお、認証失敗の場合、ユーザに認証失敗を通知する。

【０１５６】

次に、Ｓ１１３において、ユーザは、アプリの家電登録メニューから登録する機器ＩＤをユーザ端末５００に入力し、ユーザ端末５００から送信する。ここで、機器ＩＤとは機器４００を識別するＩＤである。機器ＩＤは、機器４００の筐体や同梱の印刷物に印刷されていてもよく、この場合、ユーザは、印刷されている機器ＩＤを入力する。また、ユーザ端末５００が機器ＩＤを機器４００から取得するとしてもよい。この場合、例えば、ユーザ端末５００と機器４００との間で通信することで、機器ＩＤを取得し、ユーザ端末５００からメーカサーバ１００に送信するとしてもよい。

【０１５７】

次に、Ｓ１１４において、メーカサーバ１００は、機器ＩＤをユーザＩＤに関連づけて登録する。

【０１５８】

２．５．３　機器４００からの機器履歴のアップロード処理時の動作

図２９は、機器４００が機器履歴情報をアップロードするときのシーケンス図である。なお、アップロードは、定期的または不定期に行われる。

【０１５９】

まず、Ｓ１２１において、機器４００は、蓄積した機器履歴を、機器ＩＤとともにメーカサーバ１００にアップロードする。

【０１６０】

次に、Ｓ１２２において、メーカサーバ１００は、機器ＩＤとその機器履歴とを受信し、機器ＩＤを用いて機器ＩＤに対応する機器履歴ＤＢを検索し、対応するユーザＩＤの領域に受信した機器履歴を追加する。

【０１６１】

２．５．４　ポータルサーバ２００からユーザに提案情報を提供するときの処理動作

図３０～図３２は、実施の形態２に係るポータルサーバ２００からユーザに提案情報を提供するときのシーケンス図である。なお、この提案情報の提供は、定期的または不定期に行われる。

【０１６２】

まず、Ｓ１３１において、メーカサーバ１００とポータルサーバ２００との間でＳＳＬ認証を行い、暗号通信路を確立する。

【０１６３】

次に、Ｓ１３２において、メーカサーバ１００は、サービスを提供したいユーザを選択し、ユーザＩＤから一時識別子を生成する。

【０１６４】
次に、Ｓ１３３において、メーカサーバ１００は一時識別子と機器履歴とに対して署名を生成し、機器履歴証明書を生成する。メーカサーバ１００は、生成した機器履歴証明書と公開鍵証明書とをポータルサーバ２００に送信する。
【０１６５】
次に、Ｓ１３４において、ポータルサーバ２００は、メーカサーバ１００から機器履歴証明書と公開鍵証明書を受信し、これら証明書の検証を行う。証明書の検証が失敗した場合、メーカサーバ１００にエラーを通知する。
【０１６６】
次に、Ｓ１３５において、ポータルサーバ２００は、機器履歴証明書の検証が成功した場合、サービスプロバイダサーバ３００との間でＳＳＬ認証を行い、暗号化通信路を確立する。
【０１６７】
次に、Ｓ１３６において、ポータルサーバ２００は、サービスプロバイダサーバ３００に、機器履歴情報に関連するサービス履歴の取得依頼を送信する。
【０１６８】
次に、Ｓ１３７において、サービスプロバイダサーバ３００は、ポータルサーバ２００からサービス情報取得依頼を受信すると、ユーザＩＤから一時識別子を生成し、ポータルサーバ２００に一時識別子とサービス履歴とを送信する。
【０１６９】
次に、Ｓ１３８において、ポータルサーバ２００は、サービスプロバイダサーバ３００からサービス履歴を受信すると、機器履歴とサービス履歴とに基づいて、提案情報を生成する。
【０１７０】
次に、Ｓ１３９において、ポータルサーバ２００は、生成した提案情報と機器履歴証明書とに対して署名を生成し、提案情報証明書を生成する。
【０１７１】
次に、Ｓ１４０において、ポータルサーバ２００は、生成した提案情報証明書をメーカサーバ１００に送信する。
【０１７２】
次に、Ｓ１４１において、メーカサーバ１００は、受信した提案情報証明書を検証する。提案情報証明書の検証が失敗した場合、ポータルサーバ２００にエラーを通知する。
【０１７３】
次に、Ｓ１４２において、メーカサーバ１００は、提案情報証明書の検証が成功した場合、提案情報証明書に含まれる機器履歴証明書から履歴ＤＢ内の機器履歴証明書を検索する。また、メーカサーバ１００は、検索した機器履歴証明書に含まれる一時識別子と対応するユーザＩＤを検索し、提案情報を提供すべきユーザＩＤを特定する。
【０１７４】
次に、Ｓ１４３において、メーカサーバ１００は、特定したユーザＩＤへ提案情報を提供する。このとき、提案情報が機器４００の制御情報を含む場合、ユーザ端末５００に対して提案情報に制御情報が含まれる旨の通知を行い、ユーザ端末５００からＯＫとの通知が来た場合、制御情報を送信する。なお、提案情報が機器４００の制御情報を含まない場合、上記の通知は行わず、ユーザ端末５００に提案情報を送信する。
【０１７５】
２．６　効果
以上、実施の形態２によれば、一時識別子を用いることで、メーカサーバ１００、ポータルサーバ２００、および、サービスプロバイダサーバ３００を連携させることができるので、ポータルサーバ２００は、ユーザにサービスの提案情報を提供することができる。
【０１７６】
より具体的には、メーカサーバ１００と連携するポータルサーバ２００には、個人情報

を提供せずに、一時識別子を用いて機器履歴を提供することで、ポータルサーバ２００は、ユーザのプライバシを保護しつつ、提案情報を生成することができる。また、メーカサーバ１００は、メーカサーバ１００が提供する機器履歴証明書に対して、提案情報証明書を生成することで、提供した機器履歴証明書が改ざんされたり、別のユーザの機器履歴情報に対する提案情報にすり替わっていたりすることをメーカサーバ１００が検証することができる。また、ユーザはメーカサーバ１００以外に個人情報を登録しなくとも、サービスプロバイダサーバ３００と連携したポータルサーバ２００からの提案情報を受けることができる。

【０１７７】

以上のように、実施の形態２でも、ユーザはメーカサーバ１００に登録するときにのみ、個人情報の登録を行い、サービスごとに登録する必要がない。また、メーカサーバ１００は、ポータルサーバ２００に機器履歴とともに一時識別子を提供するが、一時識別子はメーカサーバ１００以外に特定のユーザと紐付けることができない（つまり、ユーザを特定できない）ことから、プライバシへの配慮も実現している。また、メーカサーバ１００では、ユーザ情報と一時識別子とを紐付けて管理し、一時識別子に署名をつけて、ポータルサーバに提供することで、提案情報がユーザに適するものであることも検証することが可能となる。

【０１７８】

（実施の形態３）

３．システムの構成

以下、実施の形態３に係る情報管理システム１２について、図面を参照しながら説明する。

【０１７９】

実施の形態３では、メーカサーバとサービスプロバイダサーバとに同一のユーザが存在する場合、ユーザの許可のもとユーザの機器履歴とサービス履歴とを紐付けて、ポータルサーバから提案情報を提供する場合について説明する。

【０１８０】

３．１　情報管理システム１２の全体構成

図３３は、実施の形態３に係る情報管理システムの全体構成の一例を示す図である。情報管理システム１２は、メーカサーバ１００ｂ、ポータルサーバ２００ｂ、サービスプロバイダサーバ３００ｂ、機器４００、および、ユーザ端末５００を備える。なお、実施の形態１および２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。

【０１８１】

３．２　メーカサーバ１００ｂの構成

図３４は、実施の形態３に係るメーカサーバ１００ｂの構成の一例を示すブロック図である。図３４に示すメーカサーバ１００は、履歴ＤＢ制御部１０１Ｂ、一時識別子生成部１０２、証明書生成部１０３Ｂ、証明書検証部１０４、履歴ＤＢ１０５、機器制御指示部１０６、機器制御情報ＤＢ１０７、通信部１０８Ａ、および暗号処理部１１１から構成される。このメーカサーバ１００ｂは、実施の形態２のメーカサーバ１００の構成に加えて、暗号処理部１１１を備える。

【０１８２】

履歴ＤＢ制御部１０１Ｂは、実施の形態１の履歴ＤＢ制御部１０１Ａの機能に加え、ユーザ端末５００を用いるユーザに対し、サービスプロバイダサーバ３００ｂに個人情報付で機器履歴を提供してもよいか否かの問い合わせ機能を有する。履歴ＤＢ制御部１０１Ｂは、ユーザ端末５００から個人情報付の機器履歴の提供可否を受信すると、履歴ＤＢ１０５内の個人情報ＤＢを更新する。ここで、個人情報とは実施の形態１および２でのユーザ情報に対応する。

【０１８３】

図３５は、実施の形態３に係る個人情報ＤＢの構成の一例を示した図である。図３５に示すように、個人情報ＤＢには、ユーザの個人情報と、個人情報付で機器履歴を提供可能

なサービスプロバイダＩＤとが記憶される。例えば、履歴ＤＢ制御部１０１Ｂは、ポータルサーバ２００ｂから提案情報を取得するときに、機器履歴を提供する。より具体的には、履歴ＤＢ制御部１０１Ｂは、提案情報を提供するユーザが個人情報付で機器履歴を提供することが可能となっている場合、当該サービスプロバイダＩＤとともに、ユーザＩＤに対応した個人情報の暗号化処理を暗号処理部１１１へ依頼する。履歴ＤＢ制御部１０１Ｂは、暗号処理部１１１から暗号化個人情報を受信すると、一時識別子とサービスプロバイダＩＤと暗号化個人情報と機器履歴とを対応付ける署名生成を証明書生成部１０３に依頼する。そして、証明書生成部１０３から機器履歴証明書を受信すると、受信した機器履歴証明書をポータルサーバ２００ｂに送信する。

【０１８４】

証明書生成部１０３Ｂは、履歴ＤＢ制御部１０１Ｂから一時識別子とサービスプロバイダＩＤと暗号化個人情報と機器履歴とを受信した場合に機器履歴証明書を生成する。

【０１８５】

図３６に実施の形態３に係る機器履歴証明書の構成の一例を示す。図３６に示す機器履歴証明書は、一時識別子とサービスプロバイダＩＤと暗号化個人情報と機器履歴とに対し、証明書生成部１０３Ｂに保持する署名生成鍵（図示していない）で生成された署名（メーカ署名）を、一時識別子とサービスプロバイダＩＤと暗号化個人情報と機器履歴とを紐付けた上で付与した証明書である。機器履歴証明書を生成後、機器履歴証明書と署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）を送信する。公開鍵証明書は、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。

【０１８６】

暗号処理部１１１は、サービスプロバイダの公開鍵を保持し、履歴ＤＢ制御部１０１Ｂから暗号化処理の依頼とサービスプロバイダＩＤとを受信すると、サービスプロバイダＩＤに対応した公開鍵で個人情報を暗号化し、暗号化個人情報を履歴ＤＢ制御部１０１Ｂに送信する。

【０１８７】

３．３　ポータルサーバ２００ｂの構成

ポータルサーバ２００ｂは、実施の形態２のポータルサーバ２００と同様の構成である。すなわち、ポータルサーバ２００ｂは、提案情報生成部２０１Ｂ、提案情報ＤＢ２０２、証明書生成部２０３Ｂ、証明書検証部２０４Ａ、および、通信部２０５を備える。

【０１８８】

以下では、実施の形態２と異なる機能を含む構成について説明する。

【０１８９】

提案情報生成部２０１Ｂは、メーカサーバ１００ｂから受信した機器履歴証明書に含まれる機器履歴と、サービスプロバイダサーバ３００ｂから受信したサービス履歴証明書に含まれるサービス履歴と、提案情報ＤＢ２０２に記憶されている提案情報とに基づいて、ユーザに対する提案情報を生成する。より具体的には、提案情報生成部２０１Ｂは、メーカサーバ１００ｂから機器履歴証明書を受信すると、サービスプロバイダＩＤの基づき、対応するサービスプロバイダにサービス履歴証明書の取得依頼を送付する。サービスプロバイダサーバ３００ｂからサービス履歴証明書を受信すると、機器履歴証明書に含まれる機器履歴とサービス履歴証明書に含まれるサービス履歴とを用いて提案情報を生成する。なお、本実施の形態では、機器履歴証明書に対応するユーザとサービス履歴証明書に対応するユーザとは同一である。

【０１９０】

以下では、ダイエットプログラムを提案情報として生成する場合の例を説明する。

【０１９１】

まず、提案情報生成部２０１Ｂは、メーカサーバ１００ｂから受信したユーザの機器履歴証明書にある一時識別子を取得し、機器履歴の利用履歴すなわち体組成計である機器４００を利用したユーザの年代や体組成情報などを取得することできる。

【０１９２】
次に、提案情報生成部２０１Ｂは、サービスプロバイダサーバ３００ｂから当該ユーザが享受したサービスの履歴を示すサービス履歴を取得する。ここでは、サービスプロバイダサーバ３００ｂは、フィットネスクラブが有するものであり、提案情報生成部２０１Ｂは、一時識別子とともにサービス履歴として、サービスプロバイダサーバ３００ｂからフィットネスクラブで当該ユーザに提供しているサービスプログラムを取得する。また、提案情報生成部２０１Ｂは、サービスプロバイダサーバ３００ｂから取得した当該ユーザと同年代のサービス履歴を参照し、ダイエットに成功している他のユーザのサービス履歴などに基づいて、当該ユーザに対する提案情報を生成する。ここで、当該ユーザに対する提案情報とは、例えば、フィットネスクラブでのメニューや自宅でできる運動メニュー、さらにダイエット向けの料理レシピなどである。

【０１９３】
証明書生成部２０３Ｂは、提案情報と機器履歴証明書とに加えサービス履歴証明書を含めた提案情報証明書を生成する。図３７に実施の形態３に係る提案情報証明書の構成の一例を示す。図３７に示す提案情報証明書は、機器履歴証明書とサービス履歴証明書と提案情報とを紐付けた上で、証明書生成部２０３Ｂに保持する署名生成鍵（図示していない）で生成された署名（ポータルサーバ署名）を付与した証明書である。証明書生成部２０３Ｂは、提案情報証明書を生成後、提案情報証明書と署名生成鍵に対応する署名検証鍵を含んだ公開鍵証明書（図示していない）とを送信する。なお、公開鍵証明書は、実施の形態１および２と同様に、署名検証鍵に対し、（全体構成には記述されていない）証明書発行センターが署名を施したものである。また、署名生成は、機器履歴証明書と提案情報を結合した値のハッシュ値に対して、署名を生成するとしてもよい。

【０１９４】
３．４　サービスプロバイダサーバ３００ｂの構成
図３８は、実施の形態３に係るサービスプロバイダサーバ３００ｂの構成の一例を示すブロック図である。サービスプロバイダサーバ３００ｂは、履歴ＤＢ制御部３０１Ｂ、一時識別子生成部３０２、履歴ＤＢ３０３、通信部３０４Ａ、暗号処理部３１１、証明書検証部３１２および証明書生成部３１３を備える。なお、図７および図２３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。

【０１９５】
サービスプロバイダサーバ３００ｂは、実施の形態２のサービスプロバイダサーバ３００と比較して、暗号処理部３１１、証明書検証部３１２および証明書生成部３１３の構成が追加されている上、履歴ＤＢ制御部３０１Ｂの構成が異なる。また、サービスプロバイダサーバ３００ｂは、実施の形態１のサービスプロバイダサーバ３００ｃと比較して、履歴ＤＢ制御部３０１Ｂの構成が異なる。

【０１９６】
以下では、実施の形態１および２と異なる部分を中心に説明する。

【０１９７】
履歴ＤＢ制御部３０１Ｂは、ポータルサーバ２００ｂから受信した機器履歴証明書を暗号処理部３１１に送信する。履歴ＤＢ制御部３０１Ｂは、暗号処理部３１１から復号した個人情報を受信すると、それを証明書検証部３１２に送信する。また、履歴ＤＢ制御部３０１Ｂは、証明書検証部３１２で証明書の検証が成功すると、個人情報から履歴ＤＢ３０３の個人情報ＤＢから復号した個人情報と一致するユーザを特定する。履歴ＤＢ制御部３０１Ｂは、特定したユーザのサービス履歴を抽出すると、証明書生成部３１３に一時識別子と機器履歴証明書とサービス履歴とに対するサービス履歴証明書の生成を依頼する。履歴ＤＢ制御部３０１Ｂは、証明書生成部３１３からサービス履歴証明書を受信すると、ポータルサーバ２００ｂへ送信する。ここで、図３９は、実施の形態３に係るサービス履歴証明書の構成の一例を示す図である。

【０１９８】
３．５　情報管理システム１２の動作

情報管理システム１２の動作には、以下のものがある。

【０１９９】

（１）ユーザがユーザ端末５００を用いて、メーカサーバ１００ｂに登録するときの処理

（２）ユーザがメーカサーバ１００ｂに家電機器を登録するときの処理

（３）ユーザの機器４００から家電履歴情報を機器履歴ＤＢにアップロードするときの処理

（４）ポータルサーバ２００からユーザに提案情報を提供する処理

【０２００】

なお、（２）から（３）の処理は実施の形態２で説明した通りであるため、ここでは説明を省略する。

【０２０１】

３．５．１　ユーザの登録処理時の動作

図４０は、実施の形態３に係るユーザの登録処理を示すシーケンスである。

【０２０２】

まず、Ｓ３０１において、メーカサーバ１００ｂとユーザ端末５００との間で、ＳＳＬ認証を行い、暗号通信路を確立する。なお、ＳＳＬ認証およびＳＳＬ通信路については、ここでは詳しくは述べない。

【０２０３】

次に、Ｓ３０２において、ユーザ端末５００は、ユーザＩＤをメーカサーバ１００ｂに送信する。メーカサーバ１００ｂは、送信されたユーザＩＤがすでに登録されている場合にはその旨をユーザ端末５００に通知し、登録処理を終了する。一方、送信されたユーザＩＤが未登録である場合は、新規登録が可能である旨をユーザ端末５００に送信する。

【０２０４】

次に、Ｓ３０３において、ユーザはユーザ端末５００を介し、パスワード（ＰＷ）および個人情報を所定の書式に従って入力する。

【０２０５】

次に、Ｓ３０４において、メーカサーバ１００ｂは、個人情報を提供可能なサービスプロバイダのリストをユーザに提示する。ユーザは、ユーザ端末５００を介し、個人情報を提供してもよいと考えるサービスプロバイダを選択する。なお、ユーザの個人情報と選択したサービスプロバイダとは、メーカサーバ１００ｂの履歴ＤＢ１０５が有する個人情報ＤＢに記録される。

【０２０６】

３．５．２　ポータルサーバ２００ｂからユーザに提案情報を提供するときの処理動作

図４１～図４４は、実施の形態３に係る提案情報提供処理のシーケンス図である。なお、この提案情報の提供は、定期的または不定期に行われる。

【０２０７】

まず、Ｓ３１１において、メーカサーバ１００ｂとポータルサーバ２００ｂとの間でＳＳＬ認証を行い、暗号通信路を確立する。

【０２０８】

次に、Ｓ３１２において、メーカサーバ１００ｂは、サービスを提供したいユーザを選択し、ユーザＩＤから一時識別子を生成する。

【０２０９】

次に、Ｓ３１３において、メーカサーバ１００ｂは、ユーザがサービスプロバイダに個人情報を提供してもよいと許可している場合、個人情報をサービスプロバイダの暗号鍵で暗号化する。

【０２１０】

次に、Ｓ３１４において、メーカサーバ１００ｂは、一時識別子と暗号化個人情報と機器履歴とに対して署名を生成し、機器履歴証明書を生成する。メーカサーバ１００ｂから機器履歴証明書と公開鍵証明書とをポータルサーバ２００ｂに送信する。

【０２１１】
次に、Ｓ３１５において、ポータルサーバ２００ｂは、メーカサーバ１００ｂから機器履歴証明書と公開鍵証明書とを受信し、機器履歴証明書の検証を行う。機器履歴証明書の検証が失敗した場合、メーカサーバ１００ｂにエラーを通知する。
【０２１２】
次に、Ｓ３１６において、ポータルサーバ２００ｂは、機器履歴証明書の検証が成功した場合、機器履歴証明書に記載のサービスプロバイダＩＤに対応したサービスプロバイダサーバ３００ｂとの間でとＳＳＬ認証を行い、暗号化通信路を確立する。
【０２１３】
次に、Ｓ３１７において、ポータルサーバ２００ｂは、サービスプロバイダサーバ３００ｂに、機器履歴証明書と公開鍵証明書とともに、機器履歴証明書に関連するサービス履歴証明書の取得依頼を送信する。
【０２１４】
次に、Ｓ３１８において、サービスプロバイダサーバ３００ｂは、ポータルサーバ２００ｂから機器履歴証明書と公開鍵証明書を受信し、機器履歴証明書の検証を行う。機器履歴証明書の検証が失敗した場合、ポータルサーバ２００ｂにエラーを通知する。
【０２１５】
次に、Ｓ３１９において、サービスプロバイダサーバ３００ｂは、機器履歴証明書の検証が成功した場合、機器履歴証明書の暗号化個人情報を復号する。復号した個人情報から個人情報ＤＢに登録されている個人情報と一致するユーザを特定する。
【０２１６】
次に、Ｓ３２０において、サービスプロバイダサーバ３００ｂは、特定したユーザのユーザＩＤから一時識別子を生成する。
【０２１７】
次に、Ｓ３２１において、サービスプロバイダサーバ３００ｂは、特定したユーザの一時識別子とサービス履歴と機器履歴証明書とに対して、署名を生成し、サービス履歴証明書を生成する。サービスプロバイダサーバ３００ｂは、ポータルサーバ２００ｂにサービス履歴証明書と公開鍵証明書とを送信する。
【０２１８】
次に、Ｓ３２２において、ポータルサーバ２００ｂは、サービスプロバイダサーバ３００ｂからサービス履歴証明書と公開鍵証明書とを受信し、サービス履歴証明書の検証を行う。サービス履歴証明書の検証が失敗した場合、サービスプロバイダサーバ３００ｂにエラーを通知する。
【０２１９】
次に、Ｓ３２３において、ポータルサーバ２００ｂは、サービス履歴証明書の検証が成功した場合、機器履歴とサービス履歴とに基づいて、提案情報を生成する。
【０２２０】
次に、Ｓ３２５において、ポータルサーバ２００ｂは、生成した提案情報と機器履歴証明書とに対して署名を生成し、提案情報証明書を生成する。
【０２２１】
次に、Ｓ３２５において、ポータルサーバ２００ｂは、生成した提案情報証明書をメーカサーバへ送信する。
【０２２２】
次に、Ｓ３２６において、メーカサーバ１００ｂは、受信した提案情報証明書を検証する。提案情報証明書の検証が失敗した場合、ポータルサーバ２００ｂへエラーを通知する。
【０２２３】
次に、Ｓ３２７において、メーカサーバ１００ｂは、提案情報証明書の検証が成功した場合、提案情報証明書に含まれる機器履歴証明書から履歴ＤＢ内の機器履歴証明書を検索する。そして、メーカサーバ１００ｂは、検索した機器履歴証明書に含まれる一時識別子

と対応するユーザＩＤを検索し、提案情報を提供するユーザＩＤを特定する。
【０２２４】
次に、Ｓ３２８において、メーカサーバ１００ｂは、特定したユーザＩＤへ提案情報を提供する。このとき、提案情報が機器４００の制御情報を含む場合、ユーザ端末５００に対して提案情報に機器制御情報が含まれる旨の通知を行い、ユーザ端末５００からＯＫとの通知が来た場合、制御情報を送信する。なお、提案情報が機器４００の制御情報を含まない場合、上記の通知は行わず、ユーザ端末５００に提案情報を送信する。
【０２２５】
３．６　効果
以上、実施の形態３によれば、同一ユーザの機器履歴とサービス履歴とを用いることができるので、メーカサーバ１００ｂ、ポータルサーバ２００ｂ、および、サービスプロバイダサーバ３００を連携させて、当該ユーザに提案情報を提供することができる。
【０２２６】
より具体的には、メーカサーバ１００ｂとサービスプロバイダサーバ３００ｂとが連携するポータルサーバ２００ｂへは、個人情報を提供しないが、ユーザの許可の下、メーカサーバ１００ｂとサービスプロバイダサーバ３００ｂとには個人情報が提供される。そのため、メーカサーバ１００ｂとサービスプロバイダサーバ３００ｂとは、同一ユーザの機器履歴とサービス履歴とをポータルサーバ２００に提供することができる。
【０２２７】
つまり、メーカサーバ１００ｂは、ポータルサーバ２００ｂに、ユーザが利用した機器４００の機器履歴とユーザ情報とを提供する際、機器履歴に対するユーザ情報（個人情報）をサービスプロバイダサーバ３００ｂのみが復号できるように暗号化して送付することで、ポータルサーバ２００ｂへの匿名性を実現している。また、サービスプロバイダサーバ３００ｂでは、復号した個人情報（ユーザ情報）に対するサービス履歴をポータルサーバ２００ｂに提供することが可能となり、ポータルサーバ２００ｂでは当該ユーザの機器履歴とサービス履歴から提案情報が生成できる。
【０２２８】
それにより、ポータルサーバ２００ｂは、ユーザのプライバシを保護しつつ、提案情報を生成することができる。
【０２２９】
以上のように、実施の形態３では、ユーザはメーカサーバ１００ｂやサービスプロバイダサーバ３００ｂに登録するときにのみユーザの個人情報の登録を行い、ポータルサーバ２００ｂへは個人情報を提供せずとも、ユーザの機器履歴とサービス履歴とを紐付けた情報をもとにポータルサーバ２００ｂから提案情報を取得することができる。
【０２３０】
以上、本発明の一つまたは複数の態様に係る情報管理方法および情報管理システムについて、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、本発明の一つまたは複数の態様の範囲内に含まれてもよい。
【０２３１】
例えば、以下のような場合も本発明に含まれる。
【０２３２】
（１）実施の形態２では、機器履歴証明書は、一時識別子と機器履歴とメーカ署名とから構成されているとして説明したが、これに限定されない。例えば図４５に示すように有効期限を含めるとしてもよい。図４５は、有効期限を含めた機器履歴証明書の構成の一例を示す図である。例えば機器履歴の情報が古い場合、ユーザに適した提案情報とならない場合が考えられるからである。図４５に示すように機器履歴証明書に有効期限を含めることで、有効期限切れの機器履歴を用いた提案情報をユーザに提供することがなく、ユーザにとって新しい機器履歴を用いた提案情報を受けることができる。

【０２３３】
（２）実施の形態１～３では、機器４００からメーカサーバ１００等に直接機器履歴情報をアップロードしているが、ユーザ端末５００を介してアップロードするとしてもよい。この場合、機器４００とユーザ端末５００とは、ローカル通信路やＮＦＣ（Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）などの近接通信路で接続されるとしてもよい。
【０２３４】
（３）実施の形態２では、メーカサーバ１００がポータルサーバ２００へ機器履歴証明書を提供するごとに一時識別子を生成しているが、これに限定されない。例えば、一定期間経過後に変えるとしてもよいし、機器履歴証明書を送る回数が所定のしきい値を越えた時点で変えるとしてもよい。これにより、複数回の機器履歴情報を組み合わせて、提案情報が提供することができる。
【０２３５】
以下、より具体的に説明する。図４６は、機器履歴情報の提供データリストの一例を示す図である。すなわち、メーカサーバ１００は、図４６に示す提供データリストに従って、ユーザの過去の機器履歴のうち、どの期間の機器履歴情報を提供するかを判断する。例えば、体組成計の機器履歴を提供する場合、図４６に示すように、メーカサーバ１００は、機器履歴証明書には１週間分の機器履歴が含めて提供することを判断する。なお、図４６には、同じ一時識別子を用いて、機器履歴証明書を生成する場合、２回までが許容されることを示している。この履歴期間や送信許容回数は、メーカサーバ１００が決定するとしてもよいし、ユーザやポータルサーバ２００のリクエストに対応して決定するとしてもよい。また、決定後であっても、変更できるとしてもよい。
【０２３６】
これにより、複数回の機器履歴情報を組み合わせるだけでなく、履歴期間や送信許容回数を決定することができる。それにより、ユーザが機器履歴すべてを提供したくない場合にも、機器の履歴期間や送信許容回数を適切に変更することができる。
【０２３７】
（４）実施の形態１～３では、ポータルサーバ２００等がサービスプロバイダサーバ３００等からサービス履歴を取得しているが、これ例に限定されない。例えば、メーカサーバ１００等がサービスプロバイダサーバ３００等からサービス履歴を取得するとしてもよい。このときのポータルサーバ２００等から提案情報を提供する処理を以下に示す。
【０２３８】
図４７から図４９は、ポータルサーバ２００からユーザへ提案情報を提供する処理のシーケンス図である。
【０２３９】
まず、Ｓ２０１において、メーカサーバ１００とサービスプロバイダサーバ３００との間でＳＳＬ認証を行い、暗号通信路を確立する。
【０２４０】
次に、Ｓ２０２において、メーカサーバ１００は、サービスを提供したいユーザを選択し、サービスプロバイダサーバ３００にサービスを提供したいユーザが保有する機器に関連するサービス履歴の取得依頼を送信する。
【０２４１】
次に、Ｓ２０３において、サービスプロバイダサーバ３００は、メーカサーバ１００からサービス情報取得依頼を受信すると、ユーザＩＤから一時識別子を生成し、メーカサーバ１００へ一時識別子とサービス履歴を送信する。
【０２４２】
次に、Ｓ２０４において、メーカサーバ１００とポータルサーバ２００との間でＳＳＬ認証を行い、暗号通信路を確立する。
【０２４３】
次に、Ｓ２０５において、メーカサーバ１００は、選択したユーザのユーザＩＤから一

時識別子を生成する。

【０２４４】

次に、Ｓ２０６において、メーカサーバ１００は、一時識別子と機器履歴とに対して署名を生成し、機器履歴証明書を生成する。メーカサーバ１００は、生成した機器履歴証明書および公開鍵証明書とともにサービス履歴をポータルサーバ２００に送信する。

【０２４５】

次に、Ｓ２０７において、ポータルサーバ２００は、メーカサーバ１００から機器履歴証明書と公開鍵証明書とサービス履歴とを受信し、機器履歴証明書の検証を行う。機器履歴証明書の検証が失敗した場合、メーカサーバ１００にエラーを通知する。

【０２４６】

次に、Ｓ２０８において、ポータルサーバ２００は、機器履歴とサービス履歴とに基づいて、提案情報を生成する。

【０２４７】

次に、Ｓ２０９において、ポータルサーバ２００は、生成した提案情報と、機器履歴証明書およびサービス履歴とに対して署名を生成し、提案情報証明書を生成する。図５０は、提案情報証明書の構成の一例を示す図である。図５０に示す提案情報証明書は、機器履歴証明書とサービス履歴と提案情報とを紐付けた上、証明書生成部２０３に保持する署名生成鍵で生成した署名（ポータルサーバ署名）を付与した証明書である。

【０２４８】

次に、Ｓ２１０において、ポータルサーバ２００は、生成した提案情報証明書をメーカサーバ１００へ送信する。

【０２４９】

次に、Ｓ２１１において、メーカサーバ１００は、受信した提案情報証明書を検証する。提案情報証明書の検証が失敗した場合、ポータルサーバ２００へエラーを通知する。

【０２５０】

次に、Ｓ２１２において、メーカサーバ１００は、提案情報証明書の検証が成功した場合、提案情報証明書に含まれる機器履歴証明書を用いて履歴ＤＢ内の機器履歴証明書を検索する。メーカサーバ１００は、検索した機器履歴証明書に含まれる一時識別子と対応するユーザＩＤを検索し、提案情報を提供するユーザＩＤを特定する。

【０２５１】

次に、Ｓ２１３において、メーカサーバ１００は、特定したユーザＩＤへ提案情報を提供する。このとき、提案情報が機器４００の制御情報を含む場合、ユーザ端末５００に対して提案情報に機器制御情報が含まれる旨の通知を行い、ユーザ端末５００からＯＫとの通知が来た場合、制御情報を送信する。また、提案情報が機器４００の制御情報を含まない場合、上記の通知は行わず、ユーザ端末５００へ提案情報を送信する。

【０２５２】

これにより、メーカサーバ１００は、ポータルサーバ２００に機器履歴に関連するサービス履歴のみを提供することで、ユーザに提案情報を取得することができる。

【０２５３】

（５）実施の形態２では、Ｓ１３４において、証明書の検証処理が成功した場合に、ポータルサーバ２００からサービスプロバイダサーバ３００にサービス情報取得依頼をしているが、この例に限定されない。例えば定期的または不定期にポータルサーバ２００からサービスプロバイダサーバ３００へサービス情報取得依頼を行い、ポータルサーバ２００でサービス情報を蓄積しておくとしてもよい。

【０２５４】

（６）実施の形態２では、サービスプロバイダサーバ３００から提供されるサービス履歴は、一時識別子とサービス履歴とで構成されるとしているが、これに限定するわけではない。例えば、一時識別子とサービス履歴とに対し、署名を生成し、一時識別子とサービス履歴と署名とを含むサービス履歴証明書としてもよい。さらに、サービスプロバイダサーバ３００がポータルサーバ２００からサービス履歴と機器履歴に基づいた提案情報と、

サービス履歴証明書を含む提案情報証明書とを取得するとしてもよい。このとき、サービスプロバイダサーバ３００は、証明書生成部と証明書検証部とを含むとしてもよい。これにより、メーカサーバ１００だけでなく、サービスプロバイダサーバ３００も提案情報を取得でき、ユーザに提案情報を提供することができる。

【０２５５】

（７）実施の形態１～３では、機器履歴やサービス履歴は、履歴ＤＢ１０５に格納するすべての情報を提供するとしているが、これに限定されない。例えば、最新の１日や１回分の履歴を提供するとしてもよいし、最新の数日や数回の履歴を提供するとしてもよい。

【０２５６】

（８）実施の形態１～３では、ポータルサーバ２００等から機器４００へ機器制御情報を提供するとして説明したが、ポータルサーバ２００等は、機器制御情報の署名を生成し、機器４００で検証するとしてもよい。

【０２５７】

（９）実施の形態１～３では、ポータルサーバ２００等が提案情報を生成しているが、これに限定されない。例えば、メーカサーバ１００がサービスプロバイダサーバ３００からサービス履歴を取得し、ユーザへの提案情報を生成するとしてもよい。図５１は、情報管理システム１１Ａの全体構成の一例を示す図である。図５１に示す情報管理システム１１Ａは、メーカサーバ１００ａ、サービスプロバイダサーバ３００、機器４００、および、ユーザ端末５００を備える。メーカサーバ１００ａは、実施の形態２のメーカサーバ１００の機能構成に加え、ポータルサーバ２００の提案情報生成部２０１、提案情報ＤＢ２０２と同様の機能をもつ提案情報生成部と提案情報ＤＢとを備えるとすればよい。

【０２５８】

（１０）実施の形態１～３では、機器履歴は、１人のユーザ（１ユーザ）を選択して、履歴ＤＢ１０５に格納するすべての情報を提供するとしているが、これに限定するわけではない。例えば、複数のユーザの機器履歴を提供するとしてもよい。図５２は、複数のユーザの機器履歴を含んだ機器履歴証明書の構成の一例を示す図である。

【０２５９】

以下、図５２を用いて、２ユーザの機器履歴を含んだ機器履歴証明書を例に説明する。すなわち、例えばメーカサーバ１００は、１ユーザ分の機器履歴証明書を結合し、２ユーザ分の機器履歴証明書に対して、さらに署名を生成する。このとき、署名の方法としては、２ユーザ分の機器履歴証明書それぞれのハッシュ値に対して、ハッシュ値を結合し、結合したハッシュ値に署名をするとしてもよい。具体的には、一時識別子１と機器履歴１とメーカ署名１のそれぞれのハッシュ値をまたはそれぞれを結合したハッシュ値と、一時識別子２と機器履歴２とメーカ署名２のそれぞれのハッシュ値をまたはそれぞれを結合したハッシュ値を結合して、結合したハッシュ値に署名を行う。また、ハッシュ値ではなく、暗号結果や一方向性関数の演算結果とするとしてもよい。これにより、ポータルサーバ２００が１ユーザ分の機器履歴証明書のみを取り出して、他の機器履歴証明書と組み合わせて、提案情報を生成した場合、メーカサーバ１００は提案情報を検証することで、検出することができる。

【０２６０】

（１１）なお、上記（１０）では、複数のユーザの機器履歴から機器履歴証明書を生成するとして説明したがそれに限らない。複数のユーザのうち、提案情報を提供しないユーザの機器履歴をハッシュ値として、ポータルサーバ２００に提供しないとしてもよい。例えば、図５２において、メーカサーバ１００で機器履歴２のユーザには提案情報を提供しないため、ポータルサーバ２００には機器履歴を提供しないと判断した場合、機器履歴２の領域に機器履歴２のハッシュ値を置き換えるとしてもよい。それにより、ポータルサーバ２００では機器履歴２を取得することはできない。さらに、メーカ署名は一時識別子１と機器履歴１とメーカ署名１のハッシュ値と、一時識別子２と機器履歴２とメーカ署名２のハッシュ値からメーカ署名を生成しているため、機器履歴２をポータルサーバ２００に提供しなくとも、署名の生成ができる。さらに、提案情報証明書の検証も同様に検証でき

る。
【０２６１】
（１２）実施の形態２では、ポータルサーバ２００は一時識別子で識別する一ユーザに対して提案情報を生成しているが、これに限定するわけではない。例えば、複数の機器履歴証明書の一時識別子における属性情報が同じユーザに対して提案情報を生成するとしてもよい。
【０２６２】
より具体的には、ポータルサーバ２００は、複数の機器履歴証明書の一時識別子から、属性情報が同じ３０代女性となっているユーザにダイエットプログラムを生成し、同じ提案情報を各機器履歴証明書の一時識別子に対応するユーザに対して、提案情報である３０代女性向けダイエットプログラムを提供するとしてもよい。これにより、一ユーザに対してだけでなく、複数のユーザ向けに一斉に提案情報を提供することで、より多くのユーザに提案情報を提供することができる。
【０２６３】
（１３）実施の形態２では、ポータルサーバ２００は、提案情報と機器履歴証明書とに対して署名を生成し、提案情報証明書を生成しているが、これに限定するわけではない。例えば、機器履歴証明書に含まれる一時識別子と提案情報とに対して署名を生成し、提案情報証明書とするとしてもよい。
【０２６４】
（１４）実施の形態３では、ポータルサーバ２００ｂで個人情報を暗号化し、サービスプロバイダサーバ３００ｂで暗号化個人情報を復号して、ユーザを特定しているが、これに限定するわけではない。例えばサービスプロバイダサーバ３００ｂに登録されているユーザの個人情報を暗号化し、ポータルサーバ２００ｂで復号するとしてもよい。
【０２６５】
（１５）実施の形態１では、匿名化ルールをポータルサーバ２００ｃが生成して、メーカサーバ１００ｃやサービスプロバイダサーバ３００ｃ等へ送信して、匿名化を行っているが、これに限定するわけではない。例えば、メーカサーバ１００ｃやサービスプロバイダサーバ３００ｃ等が匿名化ルールを生成するとしてもよい。
【０２６６】
（１６）なお、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。
【０２６７】
（１７）また、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。
【０２６８】
また、上記の各装置を構成する構成要素の各部は、個別に１チップ化されていても良いし、一部又はすべてを含むように１チップ化されてもよい。
【０２６９】
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良い。

【０２７０】

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。

【０２７１】

（１８）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。

【０２７２】

（１９）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。

【０２７３】

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（登録商標） 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。

【０２７４】

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。

【０２７５】

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。

【０２７６】

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。

【０２７７】

（２０）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。

【０２７８】

（２１）例えば、本開示の一態様である情報管理システムは、機器履歴を収集して管理する第１の管理サーバと、サービス履歴を収集して管理する第２の管理サーバと、前記機器履歴と前記サービス履歴を利用する第３の管理サーバと、前記機器履歴を前記第１の管理サーバへ送信する機器とからなる情報管理システムであって、前記第１の管理サーバは、前記機器履歴と前記機器履歴に関連するユーザ情報を格納する第１の履歴ＤＢと、前記ユーザ情報を暗号化して暗号化ユーザ情報を算出する第１の暗号処理部と、前記暗号化ユーザ情報と前記機器履歴とに対する第１の署名を生成する第１の署名生成部と前記暗号化ユーザ情報と前記機器履歴と前記第１の署名とを含む機器履歴情報を第２の管理サーバへ提供する第１の提供部とを備え、前記第２の管理サーバは、前記サービス履歴と前記サー

ビス履歴に関連するユーザ情報を格納する第２の履歴ＤＢと、前記暗号化ユーザ情報を復号して、ユーザ情報を取得する第２の暗号処理部と、前記ユーザ情報に基づいて、前記履歴ＤＢのサービス履歴を検索し、前記第３のサーバへ提供する第２の提供部を備え、前記第３の管理サーバは、前記機器履歴情報と前記サービス履歴情報に基づいて、提案情報を生成する提案情報生成部を備えるとしてもよい。

【０２７９】

また、本開示の一態様である情報管理システムは、前記第２の管理サーバは、さらに前記機器履歴情報と前記サービス履歴とに対する第２の署名を生成する第２の署名生成部と前記第２の提供部は機器履歴情報と前記サービス履歴と前記第２の署名とを含むサービス履歴情報を第３の管理サーバへ提供し、前記第３の管理サーバは、さらに前記サービス履歴情報の署名を検証する検証部を備えるとしてもよい。

【０２８０】

また、本開示の一態様である情報管理システムは、前記第３の管理サーバは、さらに、前記機器履歴情報と前記提案情報とに対する第３の署名を生成する第３の署名生成部と、前記機器履歴情報と前記提案情報と前記第２の署名とを含む第２の提案情報を第１の管理サーバへ提供する第３の提供部を備え、前記第１の管理サーバは、さらに前記第２の提案情報の署名を検証する検証部を備えるとしてもよい。

【０２８１】

また、本開示の一態様である情報管理システムは、前記第１の管理サーバは、さらに、前記機器への制御情報を生成する制御情報生成部を備え、前記検証部で署名検証が成功した場合にのみ、前記制御情報生成部で制御情報を生成するとしてもよい。

【０２８２】

また、本開示の一態様である情報管理システムは、前記機器履歴情報は、さらに前記機器履歴情報の有効期限を含み、前記第１の管理サーバの前記検証部は、さらに前記第２の提案情報に含まれる前記機器履歴情報の前記有効期限を検証するとしてもよい。

【０２８３】

また、本開示の一態様である情報管理システムは、前記第１の提供部は、さらに前記第１の履歴ＤＢに格納される前記機器履歴のうち、所定の期間内に格納された前記機器履歴のみを提供し、前記第１の提供部は、前記所定の期間と、提供する回数の所定の閾値を記録したリストを管理するとしてもよい。

【０２８４】

（２２）また、本開示の一態様である情報管理システムは、機器履歴を収集して管理する第１の管理サーバと、サービス履歴を収集して管理する第２の管理サーバと、前記機器履歴と前記サービス履歴を利用する第３の管理サーバと、前記機器履歴を前記第１の管理サーバへ送信する機器とからなる情報管理システムであって、前記第１の管理サーバは、前記機器履歴と前記機器履歴に関連するユーザ情報を格納する履歴ＤＢと、前記ユーザ情報から一時識別子を生成する一時識別子生成部と、前記一時識別子と前記機器履歴とに対する第１の署名を生成する署名生成部と前記一時識別子と前記機器履歴と前記第１の署名とを含む機器履歴情報を第３の管理サーバへ提供する第１の提供部とを備え、前記第２の管理サーバは、前記サービス履歴を前記第３のサーバへ提供する第２の提供部を備え、前記第３の管理サーバは、前記機器履歴と前記サービス履歴に基づいて、提案情報を生成する提案情報生成部を備えるとしてもよい。

【０２８５】

また、本開示の一態様である情報管理システムは、前記第３の管理サーバは、さらに前記機器履歴情報と前記提案情報とに対する第２の署名を生成する署名生成部と前記機器履歴情報と前記提案情報と前記第２の署名とを含む第２の提案情報を第１の管理サーバへ提供する第２の提供手段を備え、前記第１の管理サーバは、さらに前記第２の提案情報の署名を検証する検証部を備えるとしてもよい。

【０２８６】

また、本開示の一態様である情報管理システムは、前記第１の管理サーバは、さらに、

前記機器への制御情報を生成する制御情報生成部を備え、前記署名検証部で署名検証が成功した場合にのみ、前記制御情報生成部で制御情報を生成するとしてもよい。

【０２８７】

また、本開示の一態様である情報管理システムは、前記機器履歴情報は、さらに前記一時識別子と前記機器履歴の有効期限を含み、前記第１の管理サーバの前記検証部は、さらに前記第２の提案情報に含まれる前記機器履歴情報の前記有効期限を検証するとしてもよい。

【産業上の利用可能性】

【０２８８】

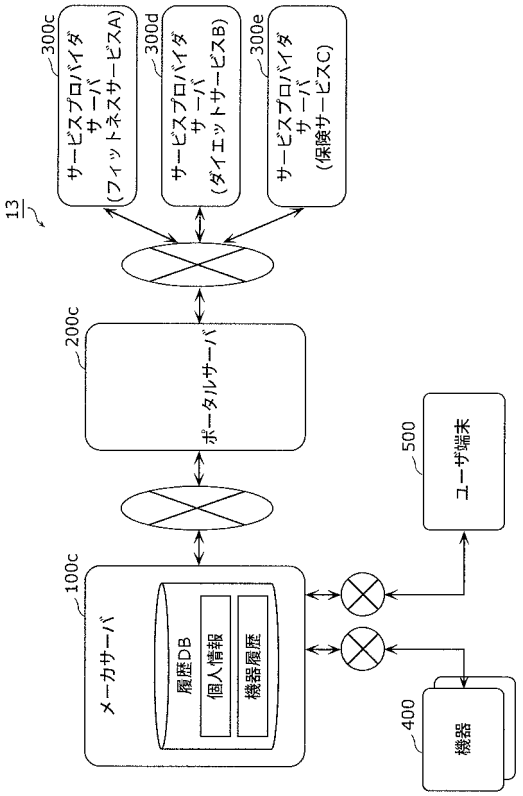
本発明は、情報管理方法および情報管理システムに利用でき、特に、互いに独立して稼動している複数のサーバと連携し、ユーザのプライバシに配慮して個人情報が提供されないポータルサーバ等の情報管理装置を備える情報管理方法および情報管理システムに利用することができる。

【符号の説明】

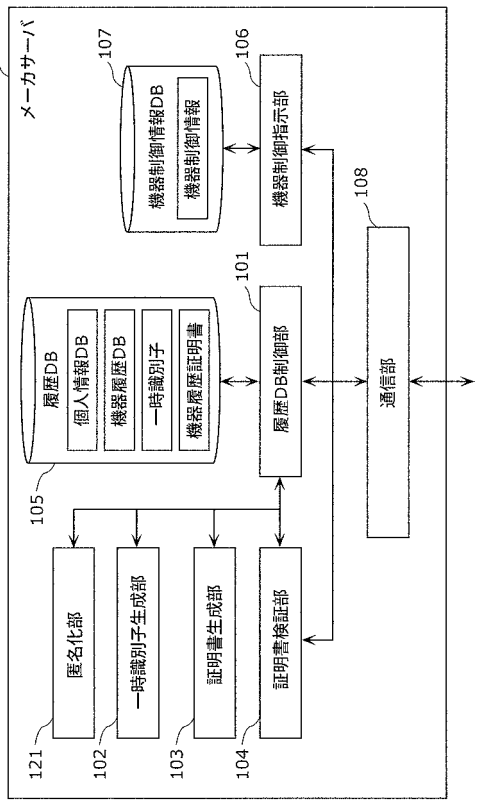
【０２８９】

１０、１１、１１Ａ、１２、１３　情報管理システム
１００、１００ａ、１００ｂ、１００ｃ　メーカサーバ
１０１、１０１Ａ、１０１Ｂ　履歴ＤＢ制御部
１０２　一時識別子生成部
１０３、１０３Ａ、１０３Ｂ、２０３、２０３Ａ、２０３Ｂ　証明書生成部
１０４、２０４、２０４Ａ　証明書検証部
１０５、３０３　履歴ＤＢ
１０６　機器制御指示部
１０７　機器制御情報ＤＢ
１０８、１０８Ａ、２０５、２０５Ａ、３０４、３０４Ａ　通信部
１１１　暗号処理部
１２１、３２１　匿名化部
２００、２００ｂ、２００ｃ　ポータルサーバ
２０１、２０１Ａ、２０１Ｂ　提案情報生成部
２０２　提案情報ＤＢ
２１１　匿名化ルール生成部
３００、３００ｂ、３００ｃ、３００ｄ、３００ｅ　サービスプロバイダサーバ
３０１、３０１Ａ、３０１Ｂ　履歴ＤＢ制御部
３０２　一時識別子生成部
３１１　暗号処理部
３１２　証明書検証部
３１３　証明書生成部
４００　機器
５００　ユーザ端末

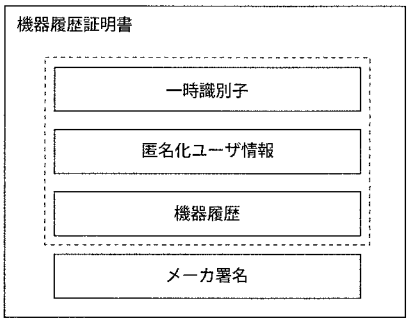
【図１】


13
300c
サービスプロバイダ
サーバ
(フィットネスサービスA)
300d
サービスプロバイダ
サーバ
(ダイエットサービスB)
300e
サービスプロバイダ
サーバ
(保険サービスC)
200c
ポータルサーバ
100c
メーカサーバ
履歴DB
個人情報
機器履歴
500
ユーザ端末
400
機器

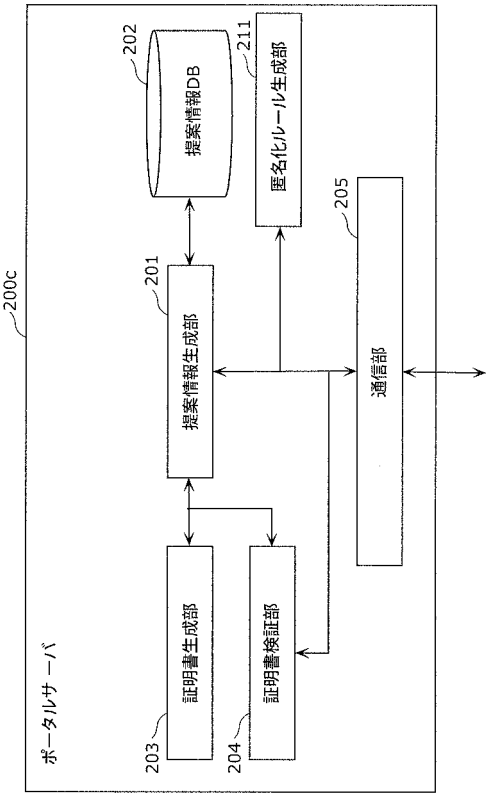
【図２】


100c
メーカサーバ
107
機器制御情報DB
機器制御情報
106
機器制御指示部
108
101
履歴DB制御部
通信部
履歴DB
個人情報DB
機器履歴DB
一時識別子
機器履歴証明書
105
匿名化部
一時識別子生成部
証明書生成部
証明書検証部
121
102
103
104

【図３】


機器履歴証明書
一時識別子
匿名化ユーザ情報
機器履歴
メーカ署名

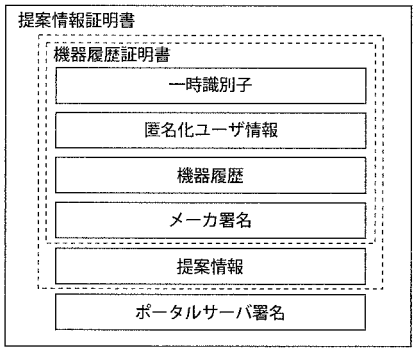
【図４】


200c
ポータルサーバ
202
提案情報DB
211
匿名化ルール生成部
205
201
提案情報生成部
通信部
証明書生成部
証明書検証部
203
204

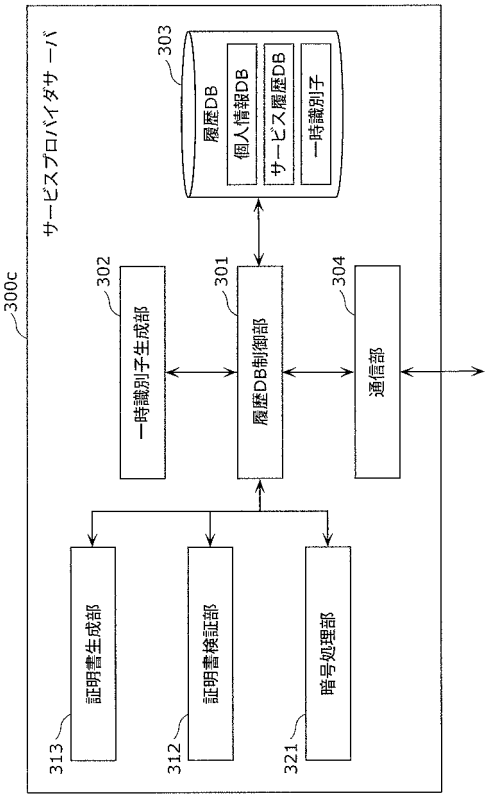
【図５】

項目	フィットネスサービス	ダイエットサービス	保険サービス
名前	削除	削除	削除
住所	市町村	都道府県	市町村
生年月日	年	年	年月日
性別	記載	記載	記載
メール	削除	削除	削除
趣味	削除	削除	記載

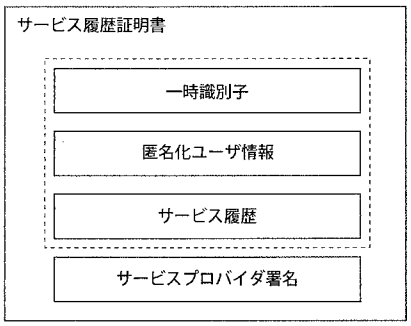
【図６】



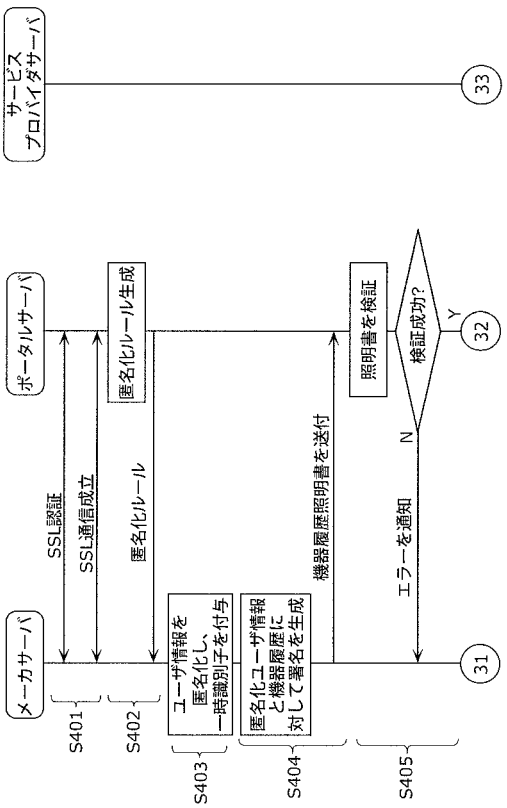
【図７】



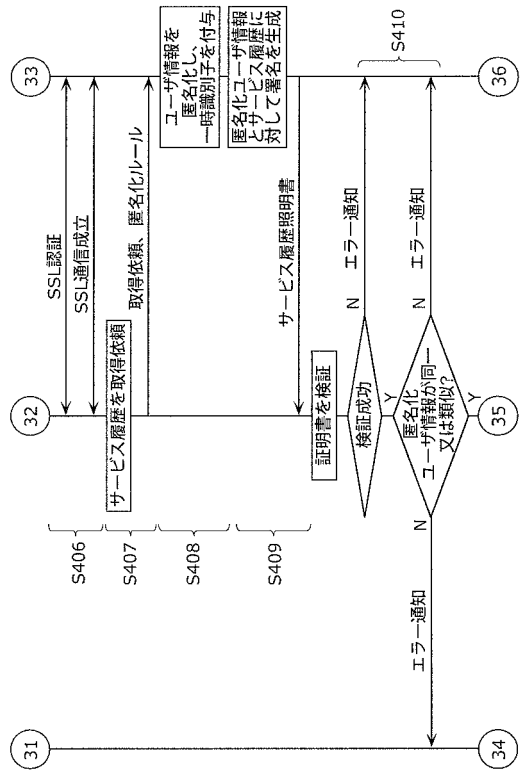
【図８】



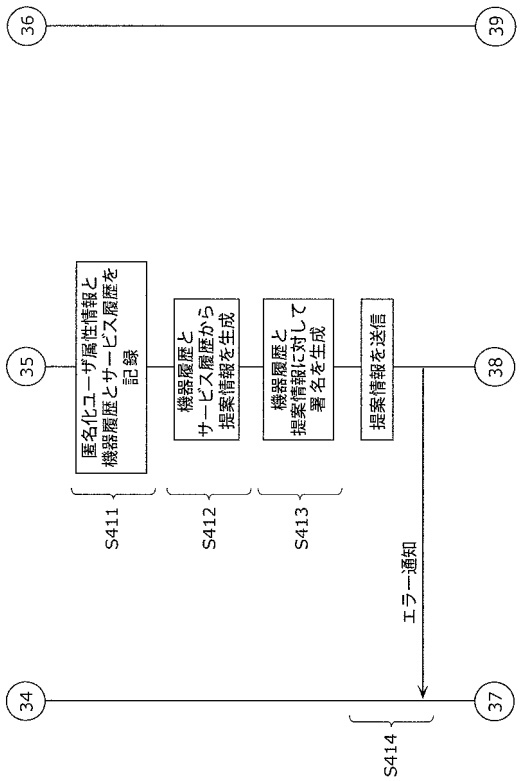
【図９】



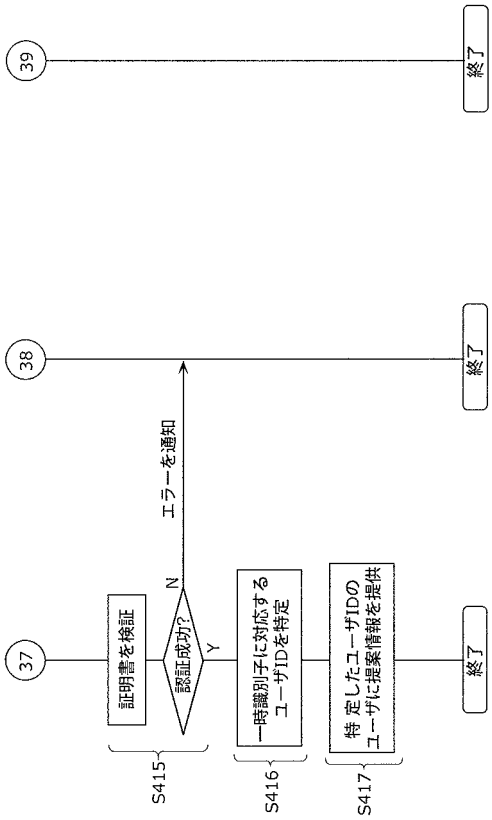
【図１０】



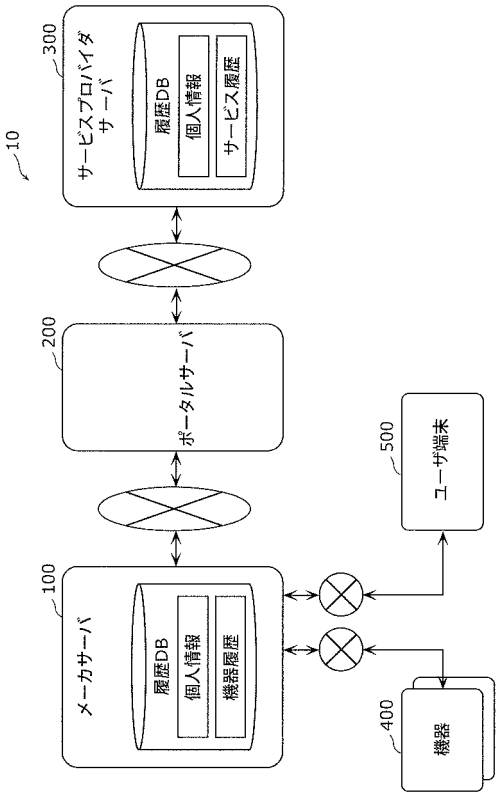
【図１１】



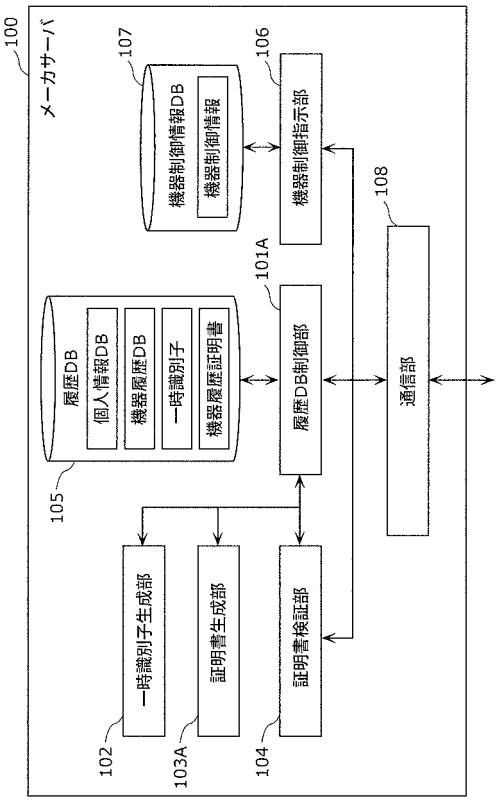
【図１２】



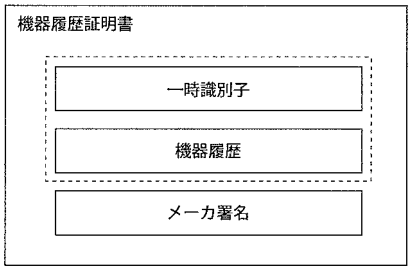
【図１３】



【図１４】



【図１５】



【図１６】

ユーザID	個人情報(ユーザ情報)
ID11	氏名:山田美紀 住所:大阪市福島区3丁目10 生年月日:1980年10月5日 性別:女 メールアドレス:yamada@aaa.com 趣味:エアロビクス
ID12	氏名:佐藤次郎 住所:東京都港区1丁目19 生年月日:1990年3月3日 性別:男 メールアドレス:sato@aaa.com 趣味:読書
…	..

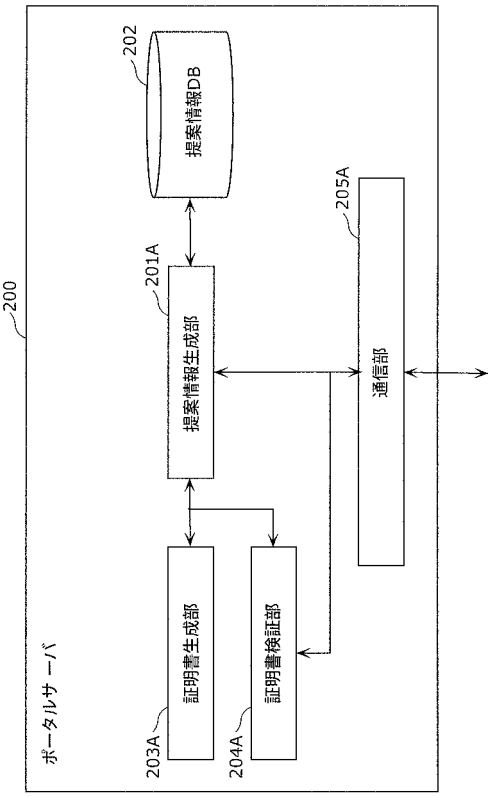
【図１７】

機器ID	機器履歴DB ID
体組成計	家電履歴DB IDA1
TV	家電履歴DB IDA2
活動量計	家電履歴DB IDA3

【図１８】

DBのID	ユーザID	ユーザIDに対応する家電履歴情報
IDA1	ID11	2012. 1. 1 体重55 キログラム、体脂肪率18% 2012. 1. 3 体重56 キログラム、体脂肪率19% ….
	ID12	2011. 12. 30 体重80 キログラム、体脂肪率22% 2012. 1. 3 体重82 キログラム、体脂肪率22% ….
IDA2	ID11	2012. 1. 1 18:00 ドラマ、20:00 ニュース 2012. 1. 3 10:00 アニメ、13:00 ドラマ ….
	ID12	
…	..	

【図１９】



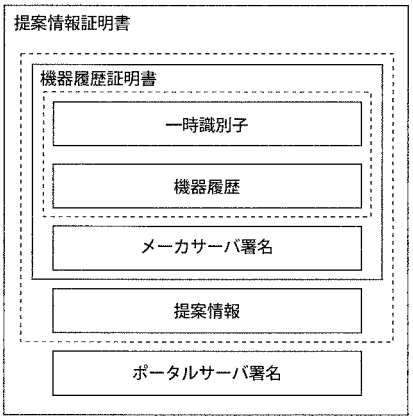
【図２０】

ジャンル	提案サービス情報DB
ダイエット	提案サービス情報DB IDS1
番組おすすめ	提案サービス情報DB IDS2

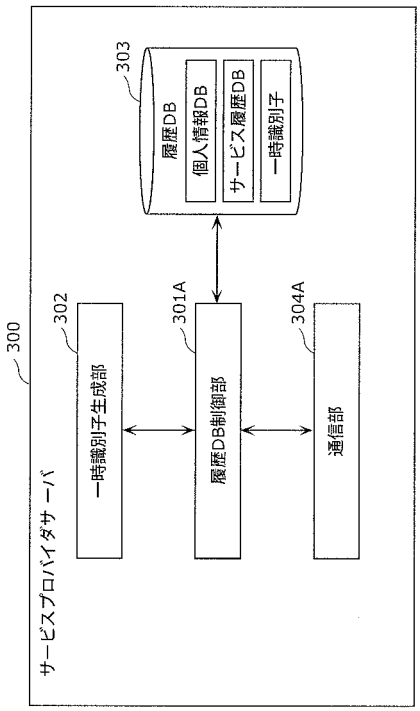
【図２１】

提案サービス情報DBのID	提案情報
IDS1	30代男性向けプログラム 30代女性向けプログラム ….
IDS2	アニメ好きおすすめ番組 スポーツ好きおすすめ番組 ….

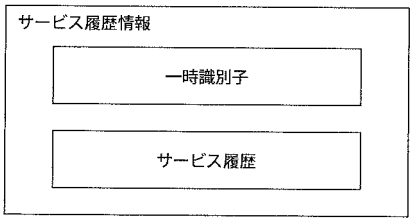
【図２２】



【図２３】



【図２４】



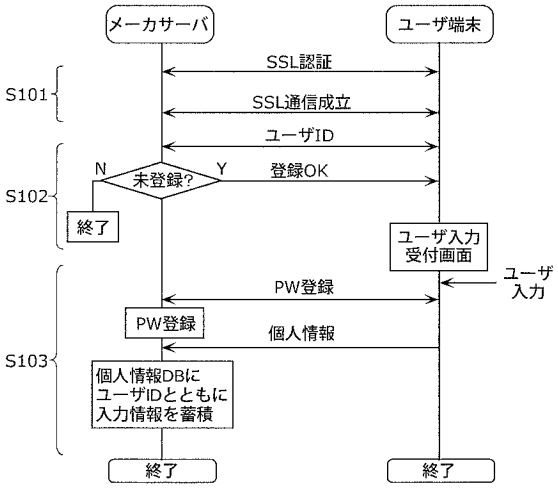
【図２５】

ユーザID	ユーザIDに個人情報
ID21	氏名:山田美紀 住所:大阪市福島区3丁目10 生年月日:1980年10月5日 性別:女 メールアドレス:yamada@aaa.com 趣味:エアロビクス
ID22	氏名:加藤五郎 住所:千葉市中央区1丁目19 生年月日:1975 年6月1日 性別:男 メールアドレス:kato@bbb.com 趣味:マラソン
…	..

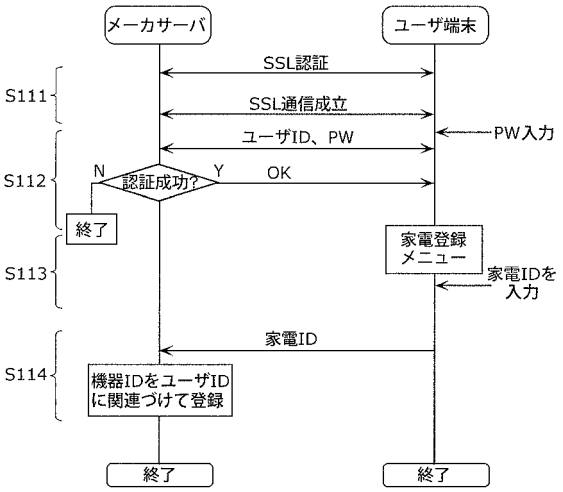
【図２６】

ユーザID	ユーザIDへの提供サービス
ID21	2011.12.28 走らないエアロ2セット、ラン30分、アドバイス 2012.1.3 上級エアロ1セット、バイク30分 …
ID22	2012.1.3 ラン60分、バイク60分 …
…	..

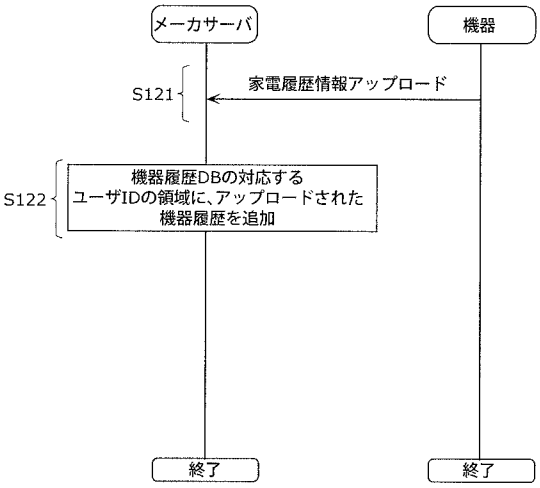
【図２７】



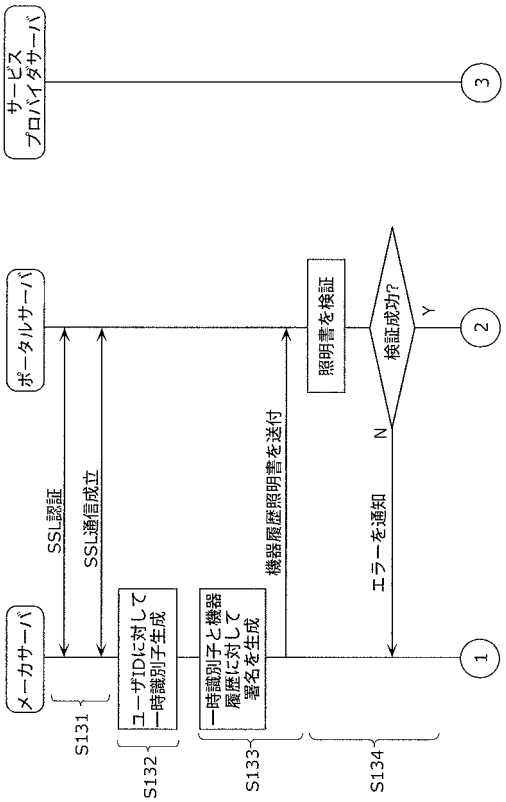
【図２８】



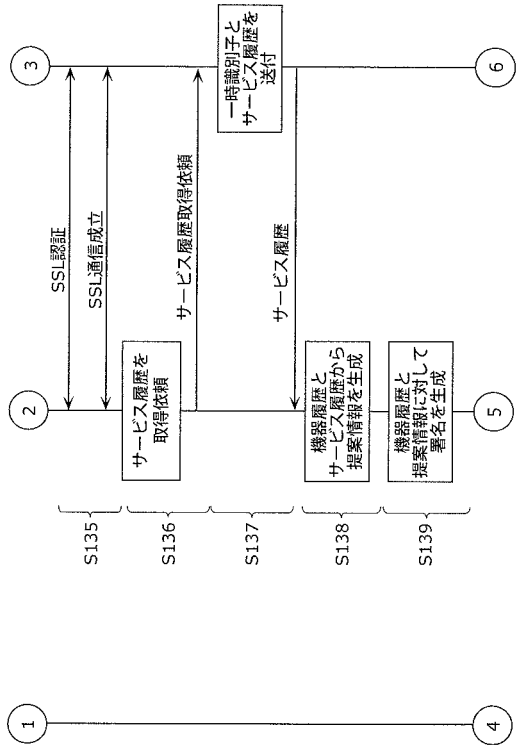
【図２９】



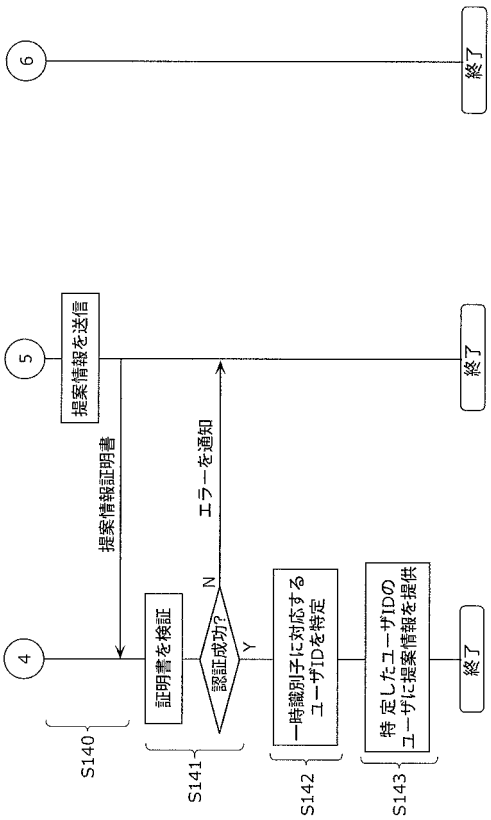
【図３０】



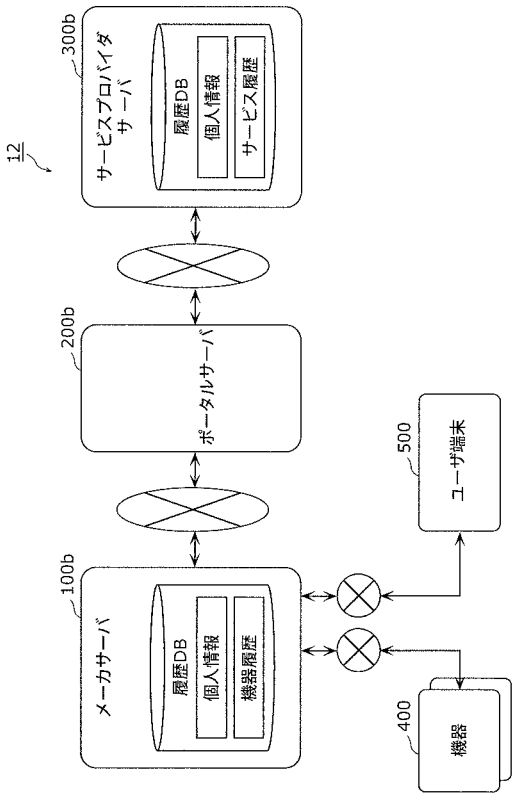
【図３１】



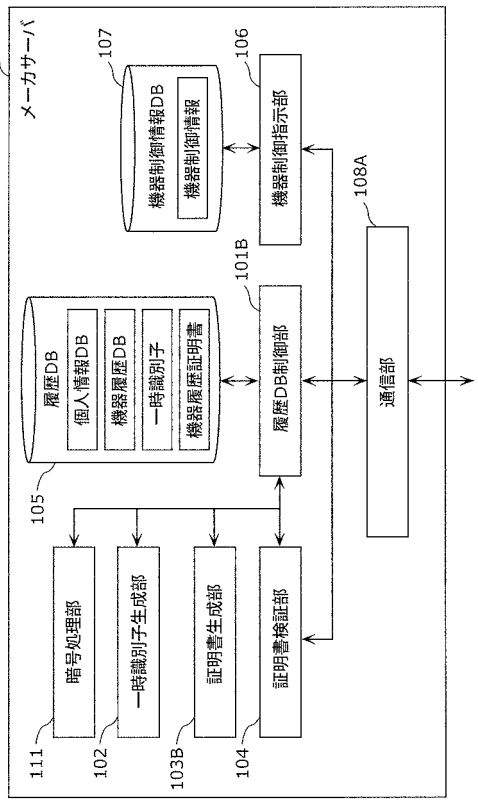
【図３２】



【図３３】



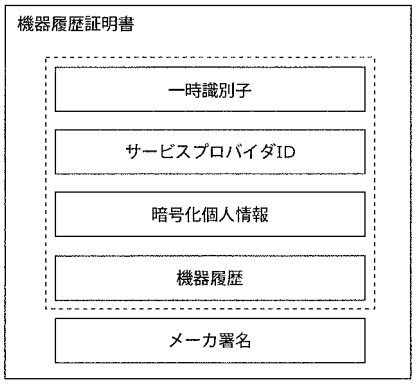
【図３４】



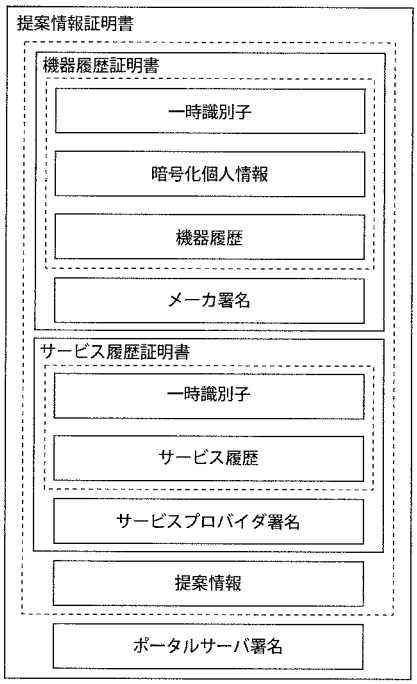
【図３５】

ユーザID	個人情報	提供可能サービスプロバイダID
ID11	氏名:山田美紀 住所:大阪市福島区3丁目10 生年月日:1980年10月5日 性別:女 メールアドレス:yamada@aaa.com 趣味:エアロビクス	SP1(フィットネスクラブA) SP2(クッキングスタジオB)
ID12	氏名:佐藤次郎 住所:東京都港区1丁目19 生年月日:1990年3月3日 性別:男 メールアドレス:sato@aaa.com 趣味:読書	SP3 SP4
…	…	

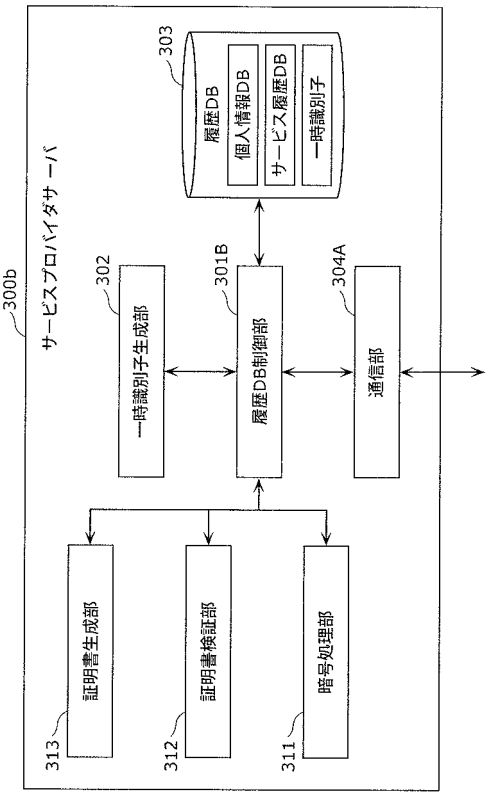
【図３６】



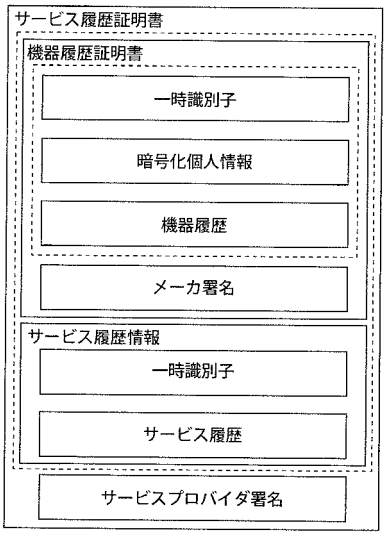
【図３７】



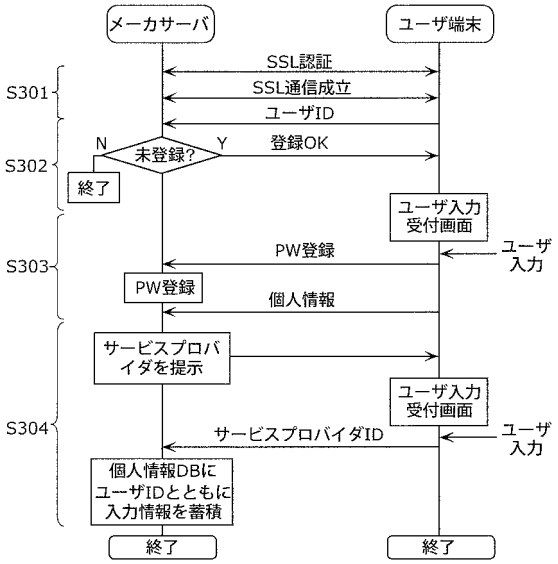
【図３８】



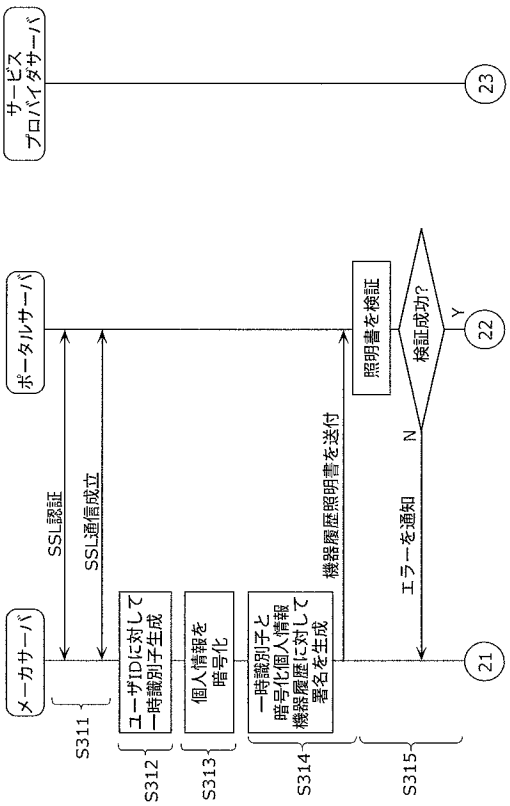
【図３９】



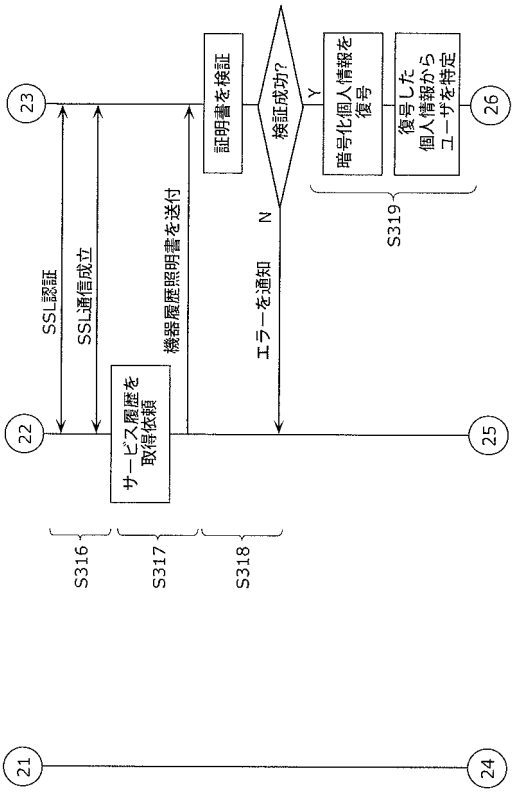
【図４０】



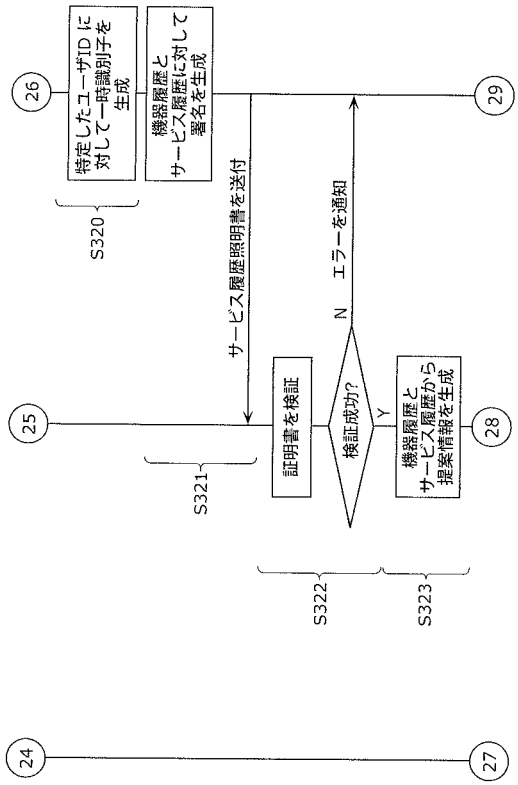
【図４１】



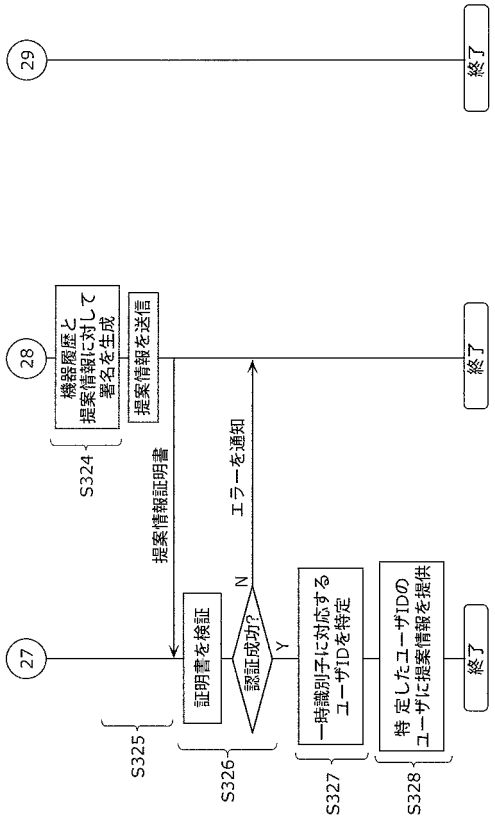
【図４２】



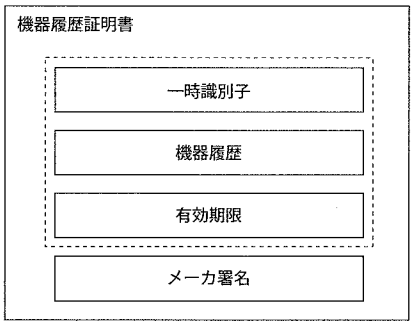
【図４３】



【図４４】



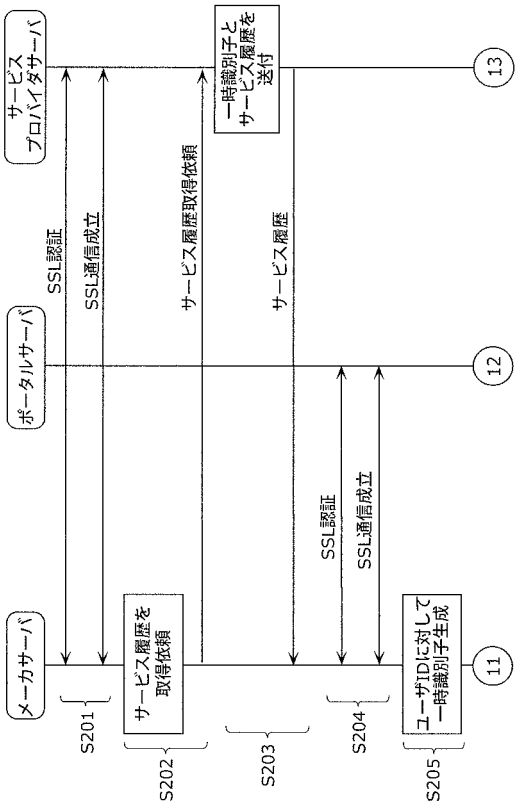
【図４５】



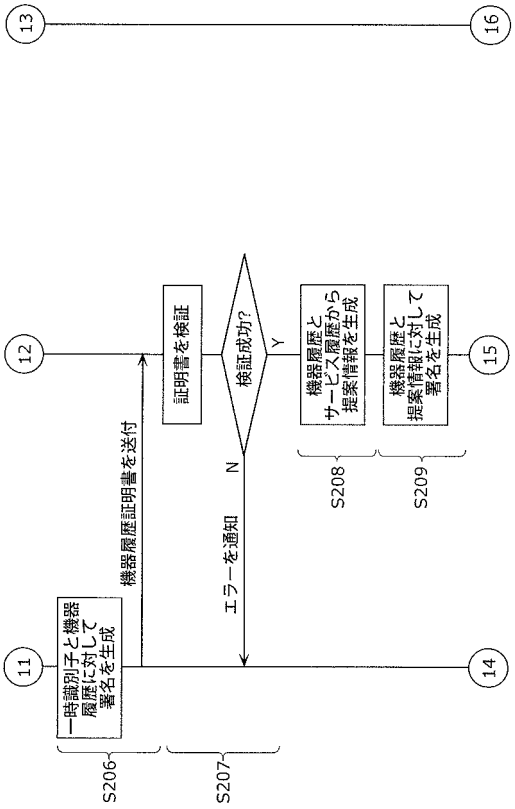
【図４６】

機器ID	機器履歴DB ID	一回に提供する履歴期間	送信許容回数
体組成計	家電履歴DB IDA1	1週間分	2回
TV	家電履歴DB IDA2	1ヶ月分	2回
活動量計	家電履歴DB IDA3	1週間分	4回

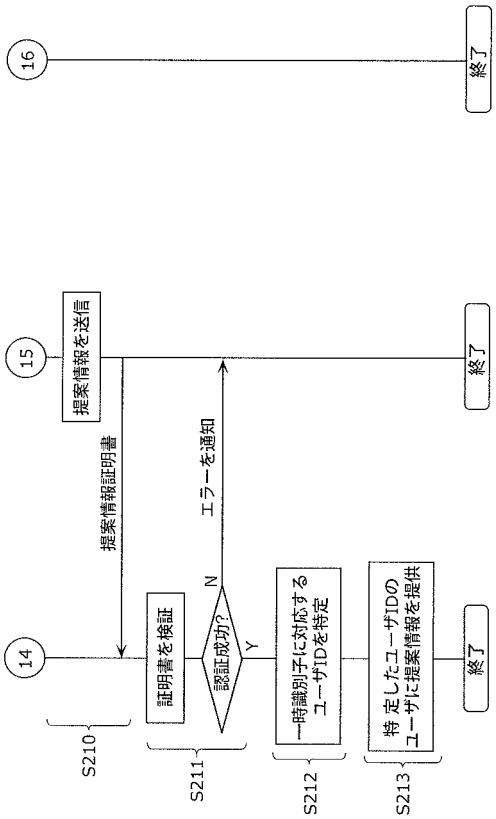
【図４７】



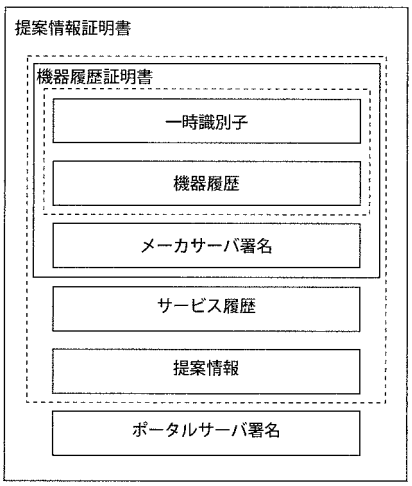
【図４８】



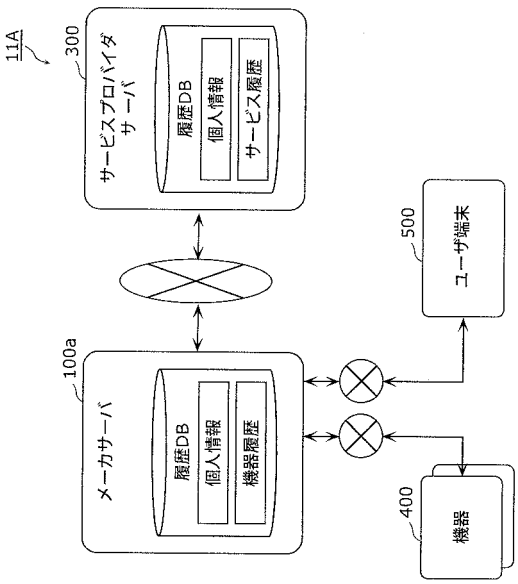
【図４９】



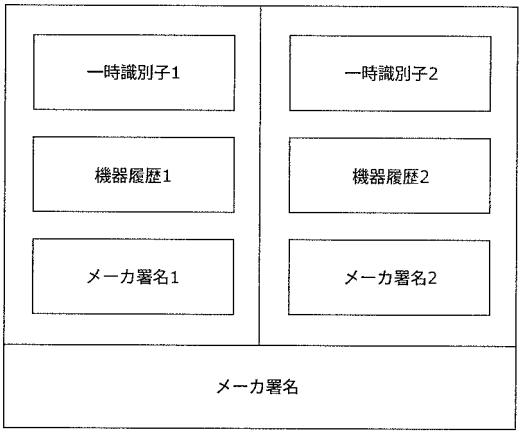
【図５０】



【図５１】


11A
300
サービスプロバイダ
サーバ
履歴DB
個人情報
サービス履歴
500
ユーザ端末
100a
メーカサーバ
履歴DB
個人情報
機器履歴
400
機器

【図５２】


一時識別子1
一時識別子2
機器履歴1
機器履歴2
メーカ署名1
メーカ署名2
メーカ署名

フロントページの続き

(72)発明者　梅谷　英生
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　笹川　路子
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　磯貝　和範
大阪府門真市大字門真１００６番地　パナソニック株式会社内