(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2007-272600
(P2007-272600A)
(43)公開日　平成19年10月18日(2007.10.18)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/20	(2006.01)	G06F 15/00	330F	5B285

審査請求 未請求　請求項の数 3　OL　（全 24 頁）

(21)出願番号　特願2006-97985(P2006-97985)
(22)出願日　平成18年3月31日(2006.3.31)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100097593
弁理士　田中　治幸
(74)代理人　100083297
弁理士　山谷　晧榮
(74)代理人　100087848
弁理士　小笠原　吉義
(72)発明者　田邊　浩靖
神奈川県横浜市神奈川区新子安一丁目２番４号　株式会社富士通アドバンストソリューションズ内

Fターム(参考)　5B285 AA06 BA02 CA31 CB02 CB12 CB32 CB72 CB83 DA05

(54)【発明の名称】環境認証と連携した本人認証方法、環境認証と連携した本人認証システムおよび環境認証と連携した本人認証用プログラム

(57)【要約】　（修正有）
【課題】本人認証に対するユーザ（クライアント）の操作負担の軽減を図りつつ、クライアントコンピュータの不正使用に対するセキュリティ強度を高めることを目的とする。
【解決手段】サーバが、サービスの提供に際してサービス依頼元のクライアントコンピュータにその環境認証（動作環境の認証）を依頼し、当該依頼に対する環境差異情報を受け取ってそれに基づく本人確認方法をクライアントコンピュータに新たに依頼する。環境差異情報として、クライアントコンピュータの現在の環境情報と、保持されている過去の環境情報と、の差異の程度を複数段階で示す差異レベルを用いる。また、過去の環境情報として、クライアントコンピュータの環境認証により得られた環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報を用いる。
【選択図】図５

環境差異レベル設定表

環境差異の内容	差異コード	差異レベル
機器が異なる(例：サーバ判定・共通認証の場合で別のマシンを操作した時)	1	3
ネットワーク接続環境が異なる(LAN接続、無線LAN接続、携帯電話接続など)	2	2
IPアドレスが異なるが、ネットワークアドレスが同一	3	1
周辺機器が追加されている	4	1
搭載ソフトが追加されている	5	1
電源がオンされてからはじめての取引	6	3
…	…	…

【特許請求の範囲】
【請求項１】
サービスを提供するコンピュータが、
サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブルを参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を実行することを特徴とする環境認証と連携した本人認証方法。
【請求項２】
サービスを提供するコンピュータが、サービスの提供に際してサービス利用の依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってそれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムにおいて、
クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報を保持した過去環境情報保持手段と、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、前記過去環境情報保持手段に保持された過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を作成する環境差異情報作成手段と、
前記環境差異情報を受け取って前記差異レベルを求める環境差異情報判断手段と、
差異レベルと本人認証方法とを対応付けて記憶したテーブルと、
前記環境差異情報判断手段で求めた差異レベルに対応する本人認証方法を前記テーブルから選択して、クライアントコンピュータに依頼する本人認証方法依頼手段と、
を備えていることを特徴とする環境認証と連携した本人認証システム。
【請求項３】
サービスを提供するコンピュータに実行させるプログラムであって、
サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブルを参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を備えていることを特徴とする環境認証と連携した本人認証用プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サービスを提供するコンピュータが、サービスの提供に際してサービス利用の依頼元であるクライアントコンピュータにその環境認証（動作環境の認証）を依頼し、当該依頼に対する環境差異情報を受け取ってそれに基づく本人確認方法をクライアントコンピュータに新たに依頼することに関する。
【０００２】
特に環境差異情報として、クライアントコンピュータの環境認証により得られた現在の環境情報と、クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる情報を用いたものである。さらには、有意な過去の環境情報として、クライアントコンピュータの環境認証によ

り得られた環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報を用いている。

【０００３】

今日ではコンピュータを利用した各種サービスを受ける機会、例えばネットワーク経由でコンピュータ（サーバ）にアクセスして各種サービスを受ける機会が増大している。

【０００４】

その場合の本人認証ツールである従来のユーザＩＤ，パスワードは他人に漏れることによる不正使用のリスクが高い。そこで、生体認証などのように不正使用に対する強度の高い認証手段が利用されている。

【０００５】

その一方で、例えばインターネット不正出金が社会問題化している中、利用者が、なるべく簡単な操作で複数銀行のサイトに繋げて自らの最新取引履歴や残高などのサービスデータを把握できる必要性もある。

【０００６】

すなわちサービスを受けるための本人認証のセキュリティ強度を上げつつ、サービスを真正に受ける側の利便性を維持することが必要であり、本発明はこのような要請に応えるものである。

【背景技術】

【０００７】

従来、より強固なセキュリティ対策として利用されている生体認証は、サービス提供者毎に操作が必要であると利便性に劣るため確認の頻度が減り、不正出金に気付くのが遅れる可能性がある。また、パソコン立上げ時に一回のみ生体認証による本人認証を行うという方法では、電源オフ前にそのパソコンを盗まれるなどした場合に不正使用されるリスクがある。

【０００８】

以上のようなユーザ側の利便性やことを配慮した本人認証手法を示すものとして例えば下記の特許文献１～３がある。

【０００９】

特許文献１では、ネットワーク上の複数のサービスのための認証処理においてユーザの負担を軽減するため、各サービス固有のユーザＩＤおよびパスワードの代わりに単一の共通証明書情報を用いて複数のサービスが受けられるようにすることが開示されている。

【００１０】

特許文献２では、複数の認証手段を備えた個人認証端末が、サーバからの認証要求を受信するたびに、その中で指定される認証手段・認証レベル指定情報にしたがって自ら使用する認証手段または認証レベルを設定し、また、この設定処理で用いた認証手段・認証レベル指定情報を実際の認証結果とともに改ざん検出可能な形式でサーバに返すことが開示されている。

【００１１】

特許文献３では、実装機器の監査機能とアカウント情報（ユーザＩＤ＋パスワード）の暗号化機能とを有するセキュリティチップが搭載された情報処理装置において、機器監査の結果が登録データと一致しない場合（ＯＳへのログオンが禁止されて真正なアカウント情報を入力しても無効となる場合）でも、記憶部に格納された使用許可用の暗証情報と入力された暗証情報との照合によりログオンを可能とすることが開示されている。

【００１２】

なお特許文献３の、機器監査の結果が登録データと一致しない場合は必ずしも不正使用とはいえず、例えばハードウェアトラブルによって真正ユーザが実装機器を交換したときもこの一致しない場合に該当する。上記暗証情報の照合はこのような場合のログオン処理を担保するためのものである。

【特許文献１】特開２００２－７３４４号公報

【特許文献２】特開２００４－１７８４０８号公報

【特許文献３】特開２００５－３０１５６４号公報
【発明の開示】
【発明が解決しようとする課題】
【００１３】
このような従来の本人認証手法は、
・特許文献１の場合、サービス提供者が、各サービス固有のユーザＩＤおよびパスワードの代わりに単一の共通証明書情報を用いるだけでは不十分と判断することも予想される、
・特許文献２の場合、例えば持ち運び可能な情報処理装置で既に認証が一度成功したような環境（実装機器環境，ネットワーク接続環境などの使用環境）についてその後の環境変化を検出することまでは想定されていない、
・特許文献３の場合、ユーザ側のコンピュータに現に実装されたハードウェア構成が登録済みの機器構成と一致しているかどうかの監査機能であって、「一致していない」ときにその差異レベルに応じた内容の再認証処理を実行することまでは想定されていない、
などの点で、それぞれ改善の余地を有している。
【００１４】
本発明では、例えばユーザがパーソナルコンピュータなどの情報処理装置（クライアントコンピュータ）を立ち上げる際、本人認証を行うとともにそのときのクライアントコンピュータの環境情報を保持しておき、これと、サービス開始時のクライアントコンピュータの使用環境とを比較・分析して本人以外の者が操作している可能性が高い、すなわち不正使用の可能性が高いと判断した場合、再度、この比較・分析に基づく環境情報の差異レベルや、サービス取引のセキュリティ要求レベルに応じた内容の本人認証を実行するようにして、本人認証に対するユーザ（クライアント）の操作負担の軽減を図りつつ、クライアントコンピュータの不正使用に対するセキュリティ強度を高めることを目的とする。
【００１５】
また、例えばクライアントコンピュータの立上時の環境情報からその後のサービス開始時ごとの環境情報を環境履歴の形で保持して次回以降の判断基準に利用する、例えば判断対象の環境情報が直前世代のものとは異なるものの認証済みの２世代前の環境情報と同じ場合は「差異なし」とみなして、クライアントコンピュータのいわば形式的な環境変化の場合には新たな本人認証を要求せずに、ユーザ側の一層の利便性確保を図ることを目的とする。
【００１６】
本発明は、このようにサービスのセキュリティレベルに応じ本人認証要求頻度を可能な限り低減して、クライアントパソコンの環境を含めた認証を要求するものである。
【課題を解決するための手段】
【００１７】
本発明は、以上の課題を次のようにして解決する。
（１）クライアントコンピュータ（例えば後述のクライアントパソコン１０，３０）の環境認証と連携した本人認証方法において、
サービスを提供するコンピュータ（例えば後述のサーバ２０，サービス提供サーバ５０）が、
サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブル（例えば図６の本人認証処理対応表）を参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を実行する。

（２）上記（１）において、
前記過去の環境情報として、クライアントコンピュータの環境認証により得られた前記環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報を用いる。
（３）上記（１）において、
前記テーブルとして、前記差異レベルに加えて、サービスの複数の提供内容に応じた個々のサービスレベルを前記本人認証方法と対応付けたものを用い、
前記本人認証方法として、前記差異レベルおよび前記サービスレベルに対応する本人認証方法を選択する。
（４）サービスを提供するコンピュータが、サービスの提供に際してサービス利用の依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってそれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムにおいて、
クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報を保持した過去環境情報保持手段（例えば後述の記憶手段１６，４２）と、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、前記過去環境情報保持手段に保持された過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を作成する環境差異情報作成手段（例えば後述の環境差異レポート作成部１１ｃ，４１ｂ）と、
前記環境差異情報を受け取って前記差異レベルを求める環境差異情報判断手段（例えば後述の環境差異レポート判断部２１ｃ，５１ｄ）と、
差異レベルと本人認証方法とを対応付けて記憶したテーブル（例えば図６の本人認証処理対応表）と、
前記環境差異情報判断手段で求めた差異レベルに対応する本人認証方法を前記テーブルから選択して、クライアントコンピュータに依頼する本人認証方法依頼手段（例えば後述の本人認証用情報・生体認証依頼部２１ｄ，５１ｅ）と、
を備える。
（５）上記（４）において、
前記過去環境情報保持手段は、クライアントコンピュータの環境認証により得られた前記環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報を、過去の環境情報として保持する。
（６）上記（４）において、
前記テーブルには、前記差異レベルに加えて、サービスの複数の提供内容に応じた個々のサービスレベルを前記本人認証方法と対応付け、
前記本人認証方法依頼手段は、前記差異レベルおよび前記サービスレベルに対応する本人認証方法を前記テーブルから選択する。
（７）サービス提供元が、サービスの提供に際してサービス利用依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってこれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムで用いられる、サービス提供元のコンピュータにおいて、
前記環境差異情報として、前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる情報を用い、
前記環境差異情報を受け取って前記差異レベルを求める環境差異情報判断手段（例えば後述の環境差異レポート判断部２１ｃ，５１ｄ）と、
差異レベルと本人認証方法とを対応付けて記憶したテーブル（例えば図６の本人認証処理対応表）と、
前記環境差異情報判断手段で求めた差異レベルに対応する本人認証方法を前記テーブルから選択して、クライアントコンピュータに依頼する本人認証方法依頼手段（例えば後述の

本人認証用情報・生体認証依頼部２１ｄ，５１ｅ）と、
を備える。
（８）サービスを提供するコンピュータに実行させるもので、クライアントコンピュータの環境認証と連携した本人認証用プログラムにおいて、
サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブルを参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を備える。
【００１８】
本発明は、後述の付記で示すような本人認証方法，本人認証システム，クライアントコンピュータや環境差異情報管理コンピュータ（図８の環境管理サーバ４０）などもその対象とする。
【００１９】
また、クライアントコンピュータ立上げ時に生体認証を行うが、この時のクライアントコンピュータ環境を保持しておき、サービス開始時のクライアント環境と比較し、差異を分析して、本人以外の者が操作している可能性が高いと判断した場合、再度本人認証を行う。なお、差異がある場合、次回の基準として環境情報を履歴として保存する（履歴は予め決められた世代数持つ）。
【００２０】
また、環境の差異のレベル、サービス取引のセキュリティ要求度、セキュリティポリシーによって、再度本人認証処理を行うか、先に進むかの判断を行う。そして、本人認証処理を実施する場合はどの認証方法を選択するかの判断を行う。本人認証方法としては、クライアントコンピュータ側の内部認証（生体認証など）とサービス提供コンピュータ側の認証（ログイン認証、第二パスワード認証など）の二つがある。
【００２１】
また、クライアントコンピュータの環境情報の履歴は、クライアントパソコン側で管理する方法と、環境管理サーバで管理する方法とがある。
【００２２】
クライアントコンピュータに生体認証装置が付いていない場合は、生体情報に代えて、当該コンピュータ内のセキュリティチップ内で管理するパスワードを用いる。
【発明の効果】
【００２３】
本発明は、ユーザのサービス利用に際して、クライアントコンピュータの環境情報と、それまでの有意な（本人認証で支持されている）過去の環境情報との、複数段階の差異レベルや、さらにはサービス取引のセキュリティ要求レベルに応じた内容の本人認証を実行するようにしているので、本人認証に対するユーザ（クライアント）の操作負担の軽減を図りつつ、クライアントコンピュータの不正使用に対するセキュリティ強度を高めることができる。
【００２４】
また、有意な過去の環境情報の履歴を世代環境情報として保持し、判断対象のクライアントコンピュータ環境情報が直前世代のものとは異なるものの認証済みの２世代前の環境情報と同じ場合は「差異なし」とみなすようにしているので、クライアントコンピュータのいわば形式的な環境変化の場合には新たな本人認証を要求せずに、ユーザ側の一層の利便性確保を図ることができる。
【発明を実施するための最良の形態】

【００２５】
図１乃至図１１を用いて本発明を実施するための最良の形態を説明する。
【００２６】
図１は、世代環境情報をクライアントパソコンで管理する場合の本人認証システム（サービス提供システム）を示している。
【００２７】
この本人認証システムにおいて、
１０は後述のサーバ２０からインターネットなどを介して例えば銀行や証券などの金融サービスを受ける（取引を実行する）クライアントパソコン，
１１は後述の本人認証，環境認証（環境情報認証）・保持，環境差異レポート作成などのための各種演算を実行して後述のメモリ１２や入出力接続部１３ａ～１６ａなどを制御するＣＰＵ，
１１ａは当該ＣＰＵのプログラム走行内容に対応し、後述の入力手段１４から得られる生体情報などに基づいて本人確認を実行する本人認証部，
１１ｂは当該ＣＰＵのプログラム走行内容に対応し、生体認証基準となる生体情報登録時や後述のサービス提供サーバ５０からの依頼時に、後述のセキュリティチップ１３の機器監査機能により得られる使用機器情報やその他の情報（例えばＯＳ，アプリケーションソフト，ＩＰアドレス，サブネットマスクなど）からなる環境情報（図４(a)参照）を求めて世代環境情報の形で後述の記憶手段１６に保持する環境認証・保持部，
１１ｃは当該ＣＰＵのプログラム走行内容に対応し、現在の環境情報とそれまでの世代の環境情報との違いに基づく報告書（図４(c)参照）を作成する環境差異レポート作成部，
１２はプログラム命令やデータを記憶するメモリ，
１３は実装機器（周辺機器）の監査機能やパスワード管理機能などを備えたセキュリティチップ，１３ａは当該セキュリティチップとＣＰＵ１１とを接続してデータの受け渡しをする入出力接続部，
１４は利用者がその生体情報，ユーザＩＤ，パスワードやサービス要求内容などを入力するための各種入力手段（静脈情報入力装置，指紋情報入力装置，声紋情報入力装置，画像情報入力装置，キーボード，マウスなど），１４ａは当該入力手段とＣＰＵ１１とを接続してデータの受け渡しをする入出力接続部，
１５は入力手段１４からの入力内容，後述のサーバ２０からの依頼内容，利用者への問い合わせや処理結果などを示すための表示手段，１５ａは当該表示手段とＣＰＵ１１とを接続してデータの受け渡しをする入出力接続部，
１６は認証済みの世代環境情報（図２参照），環境差異レポート作成のときに用いられる環境差異レベル設定表（図５参照），生体認証の基準情報となる生体登録情報や電源オン後の生体認証時刻などを保持する記憶手段，１６ａは当該記憶手段とＣＰＵ１１とを接続してデータの受け渡しをする入出力接続部，
１７はインターネット経由の通信処理を実行する通信インタフェース部，
２０はインターネットなどを介して例えば銀行や証券などの金融サービスを提供する（取引を実行する）サーバ，
２１は後述のサービス要求確認，環境認証依頼，環境差異レポート依頼，環境差異レポート分析，本人認証用情報依頼，生体認証依頼，本人認証，サービス提供などのための各種演算を実行してメモリ（図示省略）や入出力接続部（図示省略）などを制御するＣＰＵ，
２１ａは当該ＣＰＵにおけるプログラムの走行内容に対応し、クライアントパソコン１０から送信されるサービス要求を確認してそれに対する応答処理へと移行するサービス要求確認部，
２１ｂは当該ＣＰＵにおけるプログラムの走行内容に対応し、サービス要求元のクライアントパソコン１０での環境認証およびそれに基づく環境差異レポートの作成・送付を依頼する環境認証・環境差異レポート依頼部，
２１ｃは当該ＣＰＵにおけるプログラムの走行内容に対応し、クライアントパソコン１０から受け取った環境差異レポートを分析する環境差異レポート判断部，

２１ｄは当該ＣＰＵにおけるプログラムの走行内容に対応し、当該分析結果および図６の本人認証処理対応表に基づいて、サーバ側での本人認証に用いる情報（ログイン情報，第二パスワードなど）の送信や、クライアントパソコン１０での生体認証を依頼する本人認証用情報・生体認証依頼部，
２１ｅは当該ＣＰＵにおけるプログラムの走行内容に対応し、当該分析結果や、これで指示されるタイプの本人認証結果に基づいて「サービスの提供／サービスを提供できない旨の通知」を実行して、また、後述の環境情報Ｒｔの世代環境情報への追加を依頼するサービス提供部，
２１ｆは当該ＣＰＵにおけるプログラムの走行内容に対応し、クライアントパソコン１０から受け取った本人認証用情報と登録済みの基準情報とを比較してログイン情報や第二パスワード認証を実行する本人認証部，
２２は上記環境差異レポートの分析結果と上記本人認証処理との関係を規定した本人確認処理対応表（図６参照），サービス（取引）の種別を示す取引レベル設定表（図７参照）などを保持する記憶手段，
２３はインターネット経由の通信処理を実行する通信インタフェース部，
をそれぞれ示している。クライアントパソコン１０は周知の時計機能を備えている。

【００２８】

なお、記憶手段１６，２２に登録されている世代環境情報，環境差異レベル設定表，本人確認処理対応表および取引レベル設定表は例えばテーブル形式のデータである。

【００２９】

図１の本人認証システムの主たる特徴は、
(11)クライアントパソコン１０は生体認証機構を備え、本人の生体情報（＝生体認証用の基準情報）の登録時に自らの環境情報を初代環境情報として設定し、
(12)サーバ２０はクライアントパソコン１０へのサービス開始に先立って当該クライアントに環境認証（環境情報の取得）を依頼し、
(13)クライアントパソコン１０は今回取得した環境情報と登録済みの世代環境情報との違いの程度を示す例えば図４(c)の環境差異レポートを作成してサーバ２０に送り、
(14)サーバ２０はこの環境差異レポートおよび図６の本人認証処理対応表に基づいて、新たに実行する本人認証のタイプ、またはサービスの開始を決定する、
ことである。

【００３０】

ここで、サーバ２０から指示された本人認証に成功した場合には上記取得の環境情報が世代環境情報に追加される。なお、この世代環境情報として保持される世代数はあらかじめ設定されており、これを超えて旧世代のデータは世代環境情報から削除される。

【００３１】

図２は、クライアントパソコンの現在の環境情報および認証済みの世代環境情報から環境差異レポートの対象分を判定するときの考え方の概略を示す説明図であり、(a)は現在の環境情報，(b)は認証済みの世代環境情報，(c)は現在と前世代との環境差異テーブルをそれぞれ示している。

【００３２】

説明の便宜上、個々の環境要素の種別やその値などを抽象化しており、それぞれの具体例は図４のようになる。なお、世代環境情報(b)における「要素１」の３世代前の環境情報「なし」は、この要素１の例えばハードウェアが未実装であったことを示している。

【００３３】

現在の環境情報(a)と世代環境情報(b)とが同じであるかどうかを対応要素ごとに判断してまとめたものが、環境差異テーブル(c)である。

【００３４】

この環境差異テーブル(c)ですべての前世代と「差異あり」となる要素２が環境差異レポートに記載される。

【００３５】

なお、現在環境情報の要素３，４は直前世代のそれぞれと同一なので環境差異レポートへの記載対象にはならない。また、現在環境情報の要素１は直前世代のそれと異なっているものの、２世代前のそれと同一なので環境差異レポートへの記載対象にはならない。

【００３６】

図３は、図１の本人認証システムにおける処理手順でありその内容は次のようになっている。

(s11)環境認証・保持部１１ｂは、生体情報登録時の環境認証結果（環境情報）Ｒ１を初代環境情報として記憶手段１６に登録する。なお、その後のサーバ２０からの環境認証依頼に基づく所定の環境認証結果（サーバ２０から指示された本人認証に成功した場合の環境情報など）も世代環境情報として登録される。

(s12)クライアントパソコン１０は、入力手段１４の入力内容に基づいて例えば任意の金融サービスのｔ回目の提供（取引の実行）をサーバ２０に依頼する。

(s13)サービス要求確認部２１ａでこの提供依頼を確認した後、環境認証・環境差異レポート依頼部２１ｂは、クライアントパソコン１０に新たな環境認証とそれに基づく環境差異レポートの作成を依頼する。

(s14)環境認証・保持部１１ｂは、クライアントパソコン１０の環境認証を実行してそのときの環境情報Ｒｔをワーク領域（図示省略）に保持する。

(s15)環境差異レポート作成部１１ｃは、環境情報Ｒｔと認証済みの世代環境情報とに基づいて環境差異レポートを作成する。

(s16)クライアントパソコン１０は、この環境差異レポートおよび電源オン後に生体認証した時刻（記憶手段１６に保持された生体認証時刻データ）をサーバ２０に送信する。なお、送信された生体認証時刻データは記憶手段２２などに上書き保持される。

(s17)環境差異レポート判断部２１ｃは、受信した環境差異レポートと登録済みの本人認証処理対応表とに基づいて本人認証レベル（ログイン認証か生体認証かなど）またはサービス提供を決定する（図４，６参照）。

(s18)サーバ２０は、先の決定が「サービス提供」の場合、クライアントパソコン１０に所定のサービスを提供する（取引を実行する）。

(s19)サーバ２０は、先の決定が「本人認証」の場合、クライアントパソコン１０に認証タイプを指示する。

(s20)クライアントパソコン１０は、指示されたタイプの認証処理を実行する。すなわち、先ず表示手段１５に認証タイプを示し、生体認証（クライアント側認証）のときは利用者にその生体情報を入力させて本人認証部１１ａがそれと基準の生体登録情報との比較処理を実行することによりその認証結果を求め、また、サーバ側認証のときは利用者に本人認証用情報のログイン情報（ユーザＩＤ，パスワード）や第二パスワードを入力させる。

(s21)クライアントパソコン１０は、この本人認証結果や本人認証用情報をサーバ２０に送信する。

(s22)本人認証部２１ｆは、この本人認証結果や本人認証用情報に基づいてサービス利用依頼元が「本人」であるかどうかを判断する。

(s23)サーバ２０（サービス提供部２１ｅ）は、この判断結果が「本人」の場合、クライアントパソコン１０に対し、所定のサービスを提供するとともに先の環境情報Ｒｔを世代環境情報として追加することを依頼する。

(s24)環境認証・保持部１１ｂは、環境情報Ｒｔが直前世代の環境情報と異なっているときはこのＲｔを世代環境情報に追加する。

(s25)サーバ２０（サービス提供部２１ｅ）は、(s22)の判断結果が「本人ではない」の場合、クライアントパソコン１０に所定のサービスを提供できない旨を通知する。

【００３７】

図４は、クライアントパソコンの現在の環境情報などの概要を示す説明図であり、(a)は現在の環境情報ファイル，(b)はｎ世代前との環境差異ファイル，(c)は環境差異レポートをそれぞれ示している。これらの情報は必要に応じて記憶手段に保持される。

【００３８】

クライアントパソコンの環境情報はファイル(a)で示すように、
・ハードウェア（本体，ＬＡＮカード，ハードディスク）
・ＯＳ，ソフトウェア（アプリケーション）
・環境設定値（ＩＰアドレス，サブネットマスク，デフォルトゲートウェイアドレス）
などの各データからなり、例えば現在のＩＰアドレスは「10.123.234.5」である。

【００３９】

なお、図示していないが生体認証時刻も環境情報として取得される。この生体認証時刻はクライアントパソコンの電源オン時に「スペース」データとなる。

【００４０】

環境差異ファイル(b)によれば、現在のハードディスクおよびＩＰアドレスがｎ世代前のものと相違している。なお、当該ファイルの要素番号３（ハードディスク）の旧値欄は、ｎ世代前のクライアントパソコンがハードディスク未実装の環境であったことを示している。

【００４１】

また、当該ファイルの要素番号７（ＩＰアドレス）の現在値および旧値と、環境情報ファイル(a)の要素番号８（サブネットマスク）の値とから、現在およびｎ世代前それぞれのクライアントパソコンのＩＰアドレスは相違しているものの、両者のネットワークアドレスが一致していることを確認できる。

【００４２】

環境差異レポート(c)は、環境差異ファイル(b)の「相違あり」の要素であるハードディスクおよびＩＰアドレスについてのものである。なお、現在のハードディスクおよびＩＰアドレスは他の前世代それぞれの環境情報のものとも相違しているとする。このレポート作成に際しては図５の環境差異レベル設定表が参照される。

【００４３】

図５は、環境差異レポートの作成時に参照される環境差異レベル設定表を示している。
ここでは、
・使用機器が異なる（差異コード１）
・ネットワーク接続環境が異なる（差異コード２）
・ＩＰアドレスが異なるがネットワークアドレスは同一（差異コード３）
・周辺機器が追加されている（差異コード４）
・搭載ソフトが追加されている（差異コード５）
・電源がオンされてからはじめての取引（差異コード６）
のそれぞれに、差異レベル１（軽度差異），差異レベル２（中度差異）および差異レベル３（重度差異）の３段階の評価を設定している。

【００４４】

例えば差異コード２の「ネットワーク接続環境が異なる」ときは、クライアントパソコンの設置場所が例えば生体情報登録時と異なっているため不正使用の可能性ありということで、差異レベル２（中度差異）が設定されている。

【００４５】

一方、差異コード３の「ＩＰアドレスが異なるがネットワークアドレスは同一」のときは、ネットワークアドレスが同じであれば社内の別の場所で正当に利用していることが考えられるので、差異レベル１（軽度差異）が設定されている。

【００４６】

なお、差異コード６の「電源がオンされてからはじめての取引」であるかどうかの判断は、例えば生体認証時刻が有意の時刻データ（旧値）から「スペース」に変化しているかを調べることによる。この取引のときは、図１１のステップ(s81)の判断結果が「YES」となる。

【００４７】

図５の環境差異レベル設定表の差異コードはあらかじめ図４(b)の要素番号と対応付けられている。そして、この対応内容は記憶手段１６（図８の場合は記憶手段４２）に保持

される。
【００４８】
この対応内容は例えば、
・図４(b)の要素番号２－図５の差異コード４
・要素番号３－差異コード４
・要素番号５－差異コード５
・要素番号６－差異コード５
・要素番号７－差異コード３
などである。
【００４９】
したがって環境差異レポート作成部１１ｃ（図８の場合は４１ｂ）は、この対応内容に基づいて環境差異レポートへの記載対象（すべての前世代に対して「差異あり」の環境要素）である要素番号「３」，「７」の差異コードを求めた上で、図５の環境差異レベル設定表から当該記載対象それぞれの差異レベルを特定することができる。
【００５０】
なお、この記載対象に要素番号「７」の環境要素（ＩＰアドレス）が該当した場合、環境差異レポート作成部１１ｃは、環境情報ファイル(a)の要素番号「８」（サブネットマスク）の値を取り出してネットワークアドレスが一致しているかどうかを確認する。
【００５１】
そして、それが「一致している」の結果のときは図４(c)に示すように、要素番号「７」の環境要素に対する「差異コード３，差異レベル１」のデータを環境差異レポートに書き込む。
【００５２】
図６は、サービス提供サーバが環境差異レポートを分析して次の処理を決定するときに参照する本人認証処理対応表を示している。
【００５３】
ここでは、先の環境差異レベルと、図７の取引レベル（クライアントパソコンからのサービス利用依頼レベル）とに対応した認証処理などが規定されている。なお、図１１の決定フローはこの規定にしたがっている。
【００５４】
すなわち、環境差異レベル０（差異なし）の場合は、
・取引レベル０（ログイン）のとき、上述の共通認証を利用していないときはサービス提供側の新たなログイン認証に必要な情報の送付をクライアントパソコンへ依頼し、
・取引レベル１（照会）のとき、新たな認証処理をせずに、提供依頼されたサービス取引処理に進み、
・取引レベル２（資金移動）のとき、サービス提供側の新たな第二パスワード認証に必要な情報の送付をクライアントパソコンへ依頼する。
【００５５】
また、環境差異レベル１（軽度差異）の場合は、
・取引レベル０（ログイン）のとき、上述の共通認証を利用していないときはサービス提供側の新たなログイン認証に必要な情報の送付をクライアントパソコンへ依頼し、
・取引レベル１（照会）のとき、新たな認証処理をせずに、提供依頼されたサービス取引処理に進み、
・取引レベル２（資金移動）のとき、新たな生体認証結果および、サービス提供側の新たな第二パスワード認証に必要な情報の送付をクライアントパソコンへ依頼する。
【００５６】
また、環境差異レベル２（中度差異）の場合は、
・取引レベル０（ログイン）のとき、上述の共通認証を利用していないときはサービス提供側の新たなログイン認証に必要な情報の送付をクライアントパソコンへ依頼し、
・取引レベル１（照会）のとき、新たな生体認証結果の送付をクライアントパソコンへ依

頼し、
・取引レベル２（資金移動）のとき、新たな生体認証結果の送付および、サービス提供側の新たな第二パスワード認証に必要な情報の送付をクライアントパソコンへ依頼する。
【００５７】
また、環境差異レベル３（重度差異）の場合は、取引レベル０（ログイン），取引レベル１（照会）および取引レベル２（資金移動）のいずれのときも、新たな生体認証結果の送付および、サービス提供側の新たな第二パスワード認証に必要な情報の送付をクライアントパソコンへ依頼する。
【００５８】
図７は、サービス提供サーバが環境差異レポートを分析して本人認証処理対応表を用いる際に参照する取引レベル設定表を示している。
【００５９】
ここでは、サーバからクライアントパソコンへのサービス提供内容（取引種別）とその取引レベルが規定されている。
【００６０】
図８は、世代環境情報を環境管理サーバで管理する場合の本人認証システム（サービス提供システム）を示している。
【００６１】
この本人認証システムにおいて、
３０は後述のサービス提供サーバ５０からインターネットなどを介して例えば銀行や証券などの金融サービスを受けるクライアントパソコン，
３１は後述の本人認証，環境認証などのための各種演算を実行して後述のメモリ３２や入出力接続部３３ａ～３６ａなどを制御するＣＰＵ，
３１ａはクライアントパソコン１０と同様の本人認証部，
３１ｂは当該ＣＰＵのプログラム走行内容に対応し、生体情報（生体認証の基準情報）の登録時や後述のサービス提供サーバ５０からの依頼を受けた時に環境情報（図２，図４参照）を求める環境認証部，
３２はクライアントパソコン１０と同様のメモリ，
３３はクライアントパソコン１０と同様のセキュリティチップ，３３ａは当該セキュリティチップとＣＰＵ３１とを接続してデータの受け渡しをする入出力接続部，
３４はクライアントパソコン１０と同様の入力手段，３４ａは当該入力手段とＣＰＵ３１とを接続してデータの受け渡しをする入出力接続部，
３５はクライアントパソコン１０と同様の表示手段，３５ａは当該表示手段とＣＰＵ３１とを接続してデータの受け渡しをする入出力接続部，
３６は生体認証の基準情報となる生体登録情報や電源オン後の生体認証時刻などを保持する記憶手段，３６ａは当該記憶手段とＣＰＵ３１とを接続してデータの受け渡しをする入出力接続部，
３７はインターネット経由の通信処理を実行する通信インタフェース部，
４０はクライアントパソコン３０から受け取った環境情報を管理して上記環境差異レポートを作成する環境管理サーバ，
４１は後述の環境情報管理，環境差異レポート作成などのための各種演算を実行してメモリ（図示省略）や入出力接続部（図示省略）などを制御するＣＰＵ，
４１ａは当該ＣＰＵのプログラム走行内容に対応し、クライアントパソコン３０から送られる環境情報を（クライアントパソコン１０と同様の）世代環境情報の形で後述の記憶手段４２に保持する環境情報管理部，
４１ｂはクライアントパソコン１０と同様の環境差異レポート作成部，
４２は認証済みの世代環境情報（図２参照），環境差異レポート作成のときに用いられる環境差異レベル設定表（図５参照）などを保持する記憶手段，
４３はインターネット経由の通信処理を実行する通信インタフェース部，
５０は図１のサーバ２０と同様のサービスをクライアントパソコン３０に提供するサービ

ス提供サーバ，
５１は後述のサービス要求確認，クライアントパソコン３０への環境認証依頼，環境管理サーバ４０への環境認証結果（環境情報）の転送，環境管理サーバ４０への環境差異レポート作成の依頼，環境差異レポートの分析，クライアントパソコン３０への本人認証用情報依頼，クライアントパソコン３０への生体認証依頼，本人認証，サービス提供などのための各種演算を実行してメモリ（図示省略）や入出力接続部（図示省略）などを制御するＣＰＵ，
５１ａはサーバ２０と同様のサービス要求確認部，
５１ｂは当該ＣＰＵにおけるプログラムの走行内容に対応し、サービス要求元のクライアントパソコン３０に環境認証を依頼する環境認証依頼部，
５１ｃは当該ＣＰＵにおけるプログラムの走行内容に対応し、クライアントパソコン３０から受け取った環境認証結果（＝環境情報）を環境管理サーバ４０に送信し、また、環境差異レポートの作成を当該サーバに依頼する転送部（環境差異レポート依頼部），
５１ｄは当該ＣＰＵにおけるプログラムの走行内容に対応し、環境管理サーバ４０から送られる環境差異レポートを分析する環境差異レポート判断部，
５１ｅはサーバ２０と同様の本人認証用情報・生体認証依頼部，
５１ｆはサーバ２０と同様のサービス提供部，
５１ｇはサーバ２０と同様の本人認証部，
５２は上記環境差異レポートの分析結果と上記本人認証処理との関係を規定した本人確認処理対応表（図６参照），サービス（取引）の種別を示す取引レベル設定表（図７参照）などを保持する記憶手段，
５３はインターネット経由の通信処理を実行する通信インタフェース部，
をそれぞれ示している。クライアントパソコン３０は周知の時計機能を備えている。

【００６２】

なお、記憶手段４２，５２に登録されている世代環境情報，環境差異レベル設定表，本人確認処理対応表および取引レベル設定表は例えばテーブル形式のデータである。

【００６３】

図８の本人認証システムにおける図１との主たる相違点は、
(21)環境情報の管理（保持）および環境差異レポートの作成を実行するための環境管理サーバ４０を設け、
(22)サービス提供サーバ５０は、クライアントパソコン３０から受け取る環境情報（環境認証結果）を環境管理サーバ４０に転送し、また、環境差異レポートを環境管理サーバ４０から受け取る、
ことである。

【００６４】

すなわち、図１のクライアントパソコン１０の環境情報保持機能および、世代環境情報に基づく環境差異レポート作成機能を環境管理サーバ４０に移行させている。

【００６５】

図９は、図８の本人認証システムにおける処理手順でありその内容は次のようになっている。
(s31)環境認証部３１ｂは、生体情報登録時の環境認証結果（環境情報）Ｒ１を例えばＭＡＣアドレスとともに環境管理サーバ４０に送信する。
(s32)環境情報管理部４１ａは、クライアントパソコンごと（例えばＭＡＣアドレスごと）にこのＲ１を初代環境情報として記憶手段４２に登録する。なお、その後のサービス提供サーバ５０からの環境認証依頼に基づく所定の環境認証結果（サーバ５０から指示された本人認証に成功した場合の環境情報など）も世代環境情報として登録される。
(s33)クライアントパソコン３０は、入力手段３４の入力内容に基づいて例えば任意の金融サービスのｔ回目の提供をサービス提供サーバ５０に依頼する。
(s34)サービス要求確認部５１ａでこの提供依頼を確認した後、環境認証依頼部５１ｂは、クライアントパソコン３０に新たな環境認証を依頼する。

(s35)環境認証部３１ｂは、クライアントパソコン３０の環境認証を実行する。
(s36)クライアントパソコン３０は環境認証結果である環境情報Ｒｔおよび電源オン後に生体認証した時刻（記憶手段３６に保持された生体認証時刻データ）をサービス提供サーバ５０に送信する。
(s37)転送部５１ｃは、この環境情報Ｒｔを環境管理サーバ４０に送信して環境差異レポートの作成を依頼する。なお、クライアントパソコン３０から送信された生体認証時刻データは記憶手段５２などに上書き保持される。
(s38)環境差異レポート作成部４１ｂは、受信した環境情報Ｒｔと認証済みの世代環境情報とに基づいて環境差異レポートを作成する（図１０参照）。なお、環境情報Ｒｔは環境管理サーバ４０の例えばワーク領域（図示省略）に保持される。
(s39)環境管理サーバ４０は、作成された環境差異レポートをサービス提供サーバ５０に送信する。
(s40)環境差異レポート判断部５１ｄは、受信した環境差異レポートと登録済みの本人認証処理対応表とに基づいて本人認証レベル（ログイン認証か生体認証かなど）またはサービス提供を決定する（図１１参照）。
(s41)サービス提供サーバ５０は、先の決定が「サービス提供」の場合、クライアントパソコン３０に所定のサービスを提供する。
(s42)サービス提供サーバ５０は、先の決定が「本人認証レベル」の場合、クライアントパソコン３０に認証タイプを指示する。
(s43)クライアントパソコン３０は、指示されたタイプの認証処理を実行する。すなわち、先ず表示手段３５に認証タイプを示し、生体認証（クライアント側認証）のときは利用者にその生体情報を入力させて本人認証部３１ａがそれと基準の生体登録情報との比較処理を実行することによりその認証結果を求め、また、サービス提供者側認証のときは利用者に本人認証用情報のログイン情報（ユーザＩＤ，パスワード）や第二パスワードを入力させる。
(s44)クライアントパソコン３０は、この本人認証結果や本人認証用情報をサービス提供サーバ５０に送信する。
(s45)本人認証部５１ｇは、この本人認証結果や本人認証用情報に基づいてサービス利用依頼元が「本人」であるかどうかを判断する。
(s46)サービス提供サーバ５０（サービス提供部５１ｆ）は、この判断結果が「本人」の場合、クライアントパソコン３０に所定のサービスを提供する。
(s47)サービス提供サーバ５０（サービス提供部５１ｆ）は、また環境管理サーバ４０に対し先の環境情報Ｒｔを世代環境情報として追加することを依頼する。
(s48)環境情報管理部４１ａは、環境情報Ｒｔが直前世代の環境情報と異なっているときはこのＲｔを世代環境情報に追加する。
(s49)サービス提供サーバ５０（サービス提供部５１ｆ）は、(s45)の判断結果が「本人ではない」の場合、クライアントパソコン３０に所定のサービスを提供できない旨を通知する。

【００６６】

図１０は、図３の(s15)および図９の(s38)における環境差異レポートの作成フローを示している。

【００６７】

これは、現環境情報と世代環境情報とに基づいて環境差異レポートを作成するもので、クライアントパソコン１０および環境管理サーバ４０の環境差異レポート作成部１１ｃ，４１ｂによって実行される。

【００６８】

その内容は次のようになっている。
(s61)クライアントパソコン１０，３０の現在の環境情報Ｒｔを特定する。
(s62)世代変数「ｎ」を「０」に初期設定する。
(s63)「ｎ＝ｎ＋１」の演算を実行する。

(s64)「ｎ＞保有世代数」であるかどうかを判断して、「YES」の場合は(s75)に進み、「NO」の場合は次のステップに進む。「保有世代数」は認証済みの世代環境情報として保持する世代数であり、初期設定されている。当該世代環境情報の各世代データでこの保有世代数を越える旧世代分は除去される。
(s65)環境情報の要素変数「ｉ」を「０」に初期設定する。
(s66)「ｉ＝ｉ＋１」の演算を実行する。
(s67)「ｉ＞環境情報の要素数」であるかどうかを判断して、「YES」の場合は(s63)に戻り、「NO」の場合は次のステップに進む。「環境情報の要素数」は環境情報を構成する判定対象要素の総数であり、初期設定されている。例えば図４(a)の環境情報の要素数は「ハード本体」から「デフォルトゲートウェイアドレス」までの９個である。
(s68)要素「ｉ」がｎ世代前の環境情報と「差異なし」と判定済みのものであるかどうかを判断して、「YES」の場合は(s66)に戻り、「NO」の場合は次のステップに進む。なお、判定済みかどうかは、例えば図４(b)の環境差異ファイルにおける「差異有無」のフィールドデータが真正に設定されているかどうかに基づいて判断する。
(s69)要素「ｉ」とｎ世代前の環境情報の各要素を比較する。
(s70)要素「ｉ」がｎ世代前の環境情報に含まれているかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s73)に進む。
(s71)これら同じ要素の値が一致するかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s73)に進む。
(s72)図４(b)の環境差異ファイルにおける要素「ｉ」の該当欄（差異有無フィールド）に「無」を設定して、(s66)に戻る。
(s73)要素「ｉ」がｎ世代前の環境情報と「差異あり」と判定済みのものであるかどうかを判断して、「YES」の場合は(s66)に戻り、「NO」の場合は次のステップに進む。なお、判定済みかどうかは、例えば図４(b)の環境差異ファイルにおける「差異有無」の項目データが真正に設定されているかどうかに基づいて判断する。
(s74)図４(b)の環境差異ファイルの要素「ｉ」の該当欄（差異有無フィード）に「有」を設定し、また、ｎ世代前の環境情報との差異項目値および当該環境情報の旧値をそれぞれの該当欄に設定して、(s66)に戻る。
(s75)直前世代からｎ世代前までの各世代との環境差異ファイル（図４(b)参照）においてすべての世代で「差異あり」となる環境要素を特定して、次のステップに進む。図２の例では「環境要素２」のみが特定される。
(s76)この特定環境要素および図５の環境差異レベル設定表に基づいて図４(c)の環境差異レポートを作成する。

【００６９】

なお、(s76)の作成処理においては上述したように、図４(b)の要素番号と、図５の環境差異レベル設定表の差異コードとの対応表を用いる。

【００７０】

図１１は、図３の(s17)および図９の(s40)における決定フローを示している。

【００７１】

これは図４(c)の環境差異レポートと図６の本人認証処理対応表とに基づいて本人認証レベル（ログイン認証，第二パスワード認証か生体認証かなど）またはサービス提供を決定するもので、サーバ２０およびサービス提供サーバ５０の環境差異レポート判断部２１ｃ，５１ｄによって実行される。なお、環境差異レポートにおいて複数の差異コードが示される場合には、それぞれの差異レベルの中で最大レベルのもののみが図１１の決定処理で用いられる。

【００７２】

その内容は次のようになっている。
(s81)記憶手段２２，５２の生体認証時刻データが「スペース」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s83)に進む。ここで、「YES」となるのは、クライアントパソコン１０，３０が電源オンされてまだ生体認証が済んで

ない段階でのはじめての取引（サービス要求依頼）の場合である。このときの(s16), (s36)それぞれのいわば「空」の時刻データが「スペース」に相当する。
(s82)ログイン認証（ログイン入力用画面表示）および生体認証の依頼を決定する。
(s83)「環境差異レベル＝３」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s85)に進む。
(s84)ログイン認証（ログイン入力用画面表示）および生体認証の依頼を決定する。
(s85)「環境差異レベル＝２」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s91)に進む。
(s86)「取引レベル＝０」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s88)に進む。
(s87)上述の共通認証を利用していないときはログイン認証（ログイン画面表示）の依頼を決定する。共通認証を利用しているときはその処理へ移行する。
(s88)「取引レベル＝１」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s90)に進む。
(s89)生体認証の依頼を決定する。
(s90)第二パスワード認証（第二パスワード入力用画面表示）および生体認証の依頼を決定する。
(s91)「環境差異レベル＝１」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s96)に進む。
(s92)「取引レベル＝０」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s94)に進む。
(s93)上述の共通認証を利用していないときはログイン認証（ログイン画面表示）の依頼を決定する。共通認証を利用しているときはその処理へ移行する。
(s94)「取引レベル＝１」であるかどうかを判断して、「NO」の場合は次のステップに進み、「YES」の場合は(s99)に進む。
(s95)第二パスワード認証（第二パスワード入力用画面表示）および生体認証の依頼を決定する。
(s96)「取引レベル＝０」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s98)に進む。
(s97)上述の共通認証を利用していないときはログイン認証（ログイン画面表示）の依頼を決定する。共通認証を利用しているときはその処理へ移行する。
(s98)「取引レベル＝１」であるかどうかを判断して、「YES」の場合は次のステップに進み、「NO」の場合は(s100)に進む。
(s99)クライアントパソコン１０，３０から提供依頼されたサービス取引処理に進む。
(s100)第二パスワード認証（第二パスワード入力用画面表示）の依頼を決定する。

【００７３】

なお、クライアントパソコンが生体認証装置が付いていない場合は、生体情報の替わりに、パソコン内のセキュリティチップ内で管理するパスワードを用いればよい。

【００７４】

上述の環境認証と連携した本人認証用プログラムを格納する記録媒体としては、
・プログラム提供者側のデータベース（ＤＡＳＤなどの回線先メモリ）
・各種形式の可搬型記録媒体
・コンピュータ本体部側のＲＡＭやハードディスク
などのいずれでもよい。当該プログラムはコンピュータ本体部にローディングされてその主メモリ上で実行される。

【００７５】

本発明は、以上説明した実施形態に限定されないことは勿論であり他の種々の形態をとりえるものである。

【００７６】

（付記１）サービスを提供するコンピュータが、

サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブルを参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を実行することを特徴とする環境認証と連携した本人認証方法。

【００７７】

（付記２）前記過去の環境情報は、
クライアントコンピュータの環境認証により得られた前記環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報である、
ことを特徴とする付記１記載の環境認証と連携した本人認証方法。

【００７８】

（付記３）前記テーブルは、
前記差異レベルに加えて、サービスの複数の提供内容に応じた個々のサービスレベルを前記本人認証方法と対応付けたものであり、
前記本人認証方法の選択は、
前記差異レベルおよび前記サービスレベルに対応する本人認証方法の選択である、
ことを特徴とする付記１記載の環境認証と連携した本人認証方法。

【００７９】

（付記４）前記本人確認方法は、
クライアントコンピュータ側での本人認証とサービス提供コンピュータ側での本人認証を対象とするものである、
ことを特徴とする付記１～３のいずれかに記載の環境認証と連携した本人認証方法。

【００８０】

（付記５）サービスを提供するコンピュータが、サービスの提供に際してサービス利用の依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってそれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムにおいて、
クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報を保持した過去環境情報保持手段と、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、前記過去環境情報保持手段に保持された過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を作成する環境差異情報作成手段と、
前記環境差異情報を受け取って前記差異レベルを求める環境差異情報判断手段と、
差異レベルと本人認証方法とを対応付けて記憶したテーブルと、
前記環境差異情報判断手段で求めた差異レベルに対応する本人認証方法を前記テーブルから選択して、クライアントコンピュータに依頼する本人認証方法依頼手段と、
を備えていることを特徴とする環境認証と連携した本人認証システム。

【００８１】

（付記６）前記過去環境情報保持手段は、
クライアントコンピュータの環境認証により得られた前記環境情報の中で当該環境認証後の本人認証に成功した複数の履歴からなる世代環境情報を、過去の環境情報として保持している、
ことを特徴とする付記５記載の環境認証と連携した本人認証システム。

【００８２】

（付記７）前記テーブルは、
前記差異レベルに加えて、サービスの複数の提供内容に応じた個々のサービスレベルを前

記本人認証方法と対応付けたものであり、
前記本人認証方法依頼手段は、
前記差異レベルおよび前記サービスレベルに対応する本人認証方法を前記テーブルから選択する、
ことを特徴とする付記５記載の環境認証と連携した本人認証システム。
【００８３】
（付記８）前記本人確認方法は、
クライアントコンピュータ側での本人認証とサービス提供コンピュータ側での本人認証とを対象とするものである、
ことを特徴とする付記５～７のいずれかに記載の環境認証と連携した本人認証システム。
【００８４】
（付記９）サービスを提供するコンピュータが、サービスの提供に際してサービス利用の依頼元にその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってそれに基づく本人確認方法をサービス利用依頼元に新たに依頼する本人認証システムで用いられる、サービス利用依頼元のクライアントコンピュータにおいて、
それまでの環境認証により得られた有意な過去の環境情報を保持した過去環境情報保持手段と、
前記依頼に基づく環境認証により得られた現在の環境情報と、前記過去環境情報保持手段に保持された過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を作成する環境差異情報作成手段と、
前記環境差異情報作成手段が作成した前記環境差異情報を前記コンピュータに送信する環境差異情報通信手段と、
前記コンピュータから前記環境差異情報に基づいて依頼された本人認証方法を実行する本人認証方法実行手段と、
を備えていることを特徴とする環境認証と連携した本人認証用機能を有するクライアントコンピュータ。
【００８５】
（付記１０）サービス提供元が、サービスの提供に際してサービス利用依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってこれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムで用いられる、サービス提供元のコンピュータにおいて、
前記環境差異情報は、前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる情報であり、
前記環境差異情報を受け取って前記差異レベルを求める環境差異情報判断手段と、
差異レベルと本人認証方法とを対応付けて記憶したテーブルと、
前記環境差異情報判断手段で求めた差異レベルに対応する本人認証方法を前記テーブルから選択して、クライアントコンピュータに依頼する本人認証方法依頼手段と、
を備えていることを特徴とする環境認証と連携した本人認証用機能を有するサービス提供元のコンピュータ。
【００８６】
（付記１１）サービスを提供するコンピュータが、サービスの提供に際してサービス利用依頼元であるクライアントコンピュータにその環境認証を依頼し、当該依頼に対する後述の環境差異情報を受け取ってこれに基づく本人確認方法をクライアントコンピュータに新たに依頼する本人認証システムで用いられる、環境差異情報管理コンピュータにおいて、
クライアントコンピュータのそれまでの環境認証により得られた有意な過去の環境情報を受け取って管理する環境情報管理手段と、
前記依頼に基づく環境認証によりクライアントコンピュータから得られた現在の環境情報と、前記環境情報管理手段に保持された過去の環境情報と、の差異の程度を複数段階で示

す差異レベルからなる環境差異情報を作成する環境差異情報作成手段と、
前記環境差異情報作成手段が作成した前記環境差異情報をサービス提供元の前記コンピュータに送信する環境差異情報通信手段と、
を備えていることを特徴とする環境認証と連携した本人認証用機能を有する環境差異情報管理コンピュータ。
【００８７】
（付記１２）サービスを提供するコンピュータに実行させるプログラムであって、
サービスの提供に際し、サービス利用依頼元であるクライアントコンピュータにその環境認証を依頼する利用時環境認証依頼ステップと、
前記依頼に基づくクライアントコンピュータの環境認証により得られた現在の環境情報と、それまでの有意な過去の環境情報と、の差異の程度を複数段階で示す差異レベルからなる環境差異情報を受け取って当該差異レベルを求める環境差異情報判断ステップと、
差異レベルと本人認証方法とを対応付けて記憶したテーブルを参照して、前記環境差異情報判断ステップで求めた差異レベルに対応する本人認証方法を選択し、サービス利用依頼元のコンピュータに通知する本人認証方法通知ステップと、
を備えていることを特徴とする環境認証と連携した本人認証用プログラム。
【図面の簡単な説明】
【００８８】
【図１】世代環境情報をクライアントパソコンで管理する場合の本人認証システム（サービス提供システム）を示す説明図である。
【図２】クライアントパソコンの現在の環境情報および認証済みの世代環境情報から環境差異レポートの対象分を判定するときの考え方の概略を示す説明図であり、(a)は現在の環境情報，(b)は認証済みの世代環境情報，(c)は現在と前世代との環境差異テーブルをそれぞれ示している。
【図３】図１の本人認証システムにおける処理手順を示す説明図である。
【図４】クライアントパソコンの現在の環境情報などの概要を示す説明図であり、(a)は現在の環境情報ファイル，(b)はｎ世代前との環境差異ファイル，(c)は環境差異レポートをそれぞれ示している。
【図５】環境差異レポートの作成時に参照される環境差異レベル設定表を示す説明図である。
【図６】サービス提供サーバが環境差異レポートを分析して次の処理を決定するときに参照する本人認証処理対応表を示す説明図である。
【図７】サービス提供サーバが環境差異レポートを分析して本人認証処理対応表を用いる際に参照する取引レベル設定表を示す説明図である。
【図８】世代環境情報を環境管理サーバで管理する場合の本人認証システム（サービス提供システム）を示す説明図である。
【図９】図８の本人認証システムにおける処理手順を示す説明図である。
【図１０】図３の(s15)および図９の(s38)における環境差異レポートの作成フローを示す説明図である。
【図１１】図３の(s17)および図９の(s40)における決定フローを示す説明図である。
【符号の説明】
【００８９】
図１において、
１０：クライアントパソコン
１１：ＣＰＵ
１１ａ：本人認証部
１１ｂ：環境認証・保持部
１１ｃ：環境差異レポート作成部
１２：メモリ
１３：セキュリティチップ

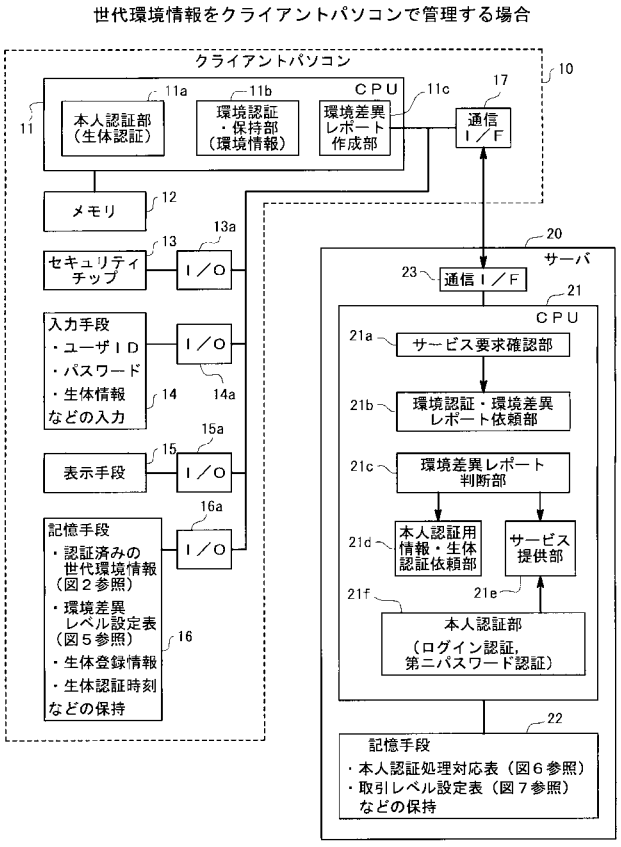
１３ａ：入出力接続部
１４：入力手段
１４ａ：入出力接続部
１５：表示手段
１５ａ：入出力接続部
１６：記憶手段
１６ａ：入出力接続部
１７：通信インタフェース部
２０：サーバ
２１：ＣＰＵ
２１ａ：サービス要求確認部
２１ｂ：環境認証・環境差異レポート依頼部
２１ｃ：環境差異レポート判断部
２１ｄ：本人認証用情報・生体認証依頼部
２１ｅ：サービス提供部
２１ｆ：本人認証部
２２：記憶手段
２３：通信インタフェース部

【００９０】

図８において、
３０：クライアントパソコン
３１：ＣＰＵ
３１ａ：本人認証部
３１ｂ：環境認証部
３２：メモリ
３３：セキュリティチップ
３３ａ：入出力接続部
３４：入力手段
３４ａ：入出力接続部
３５：表示手段
３５ａ：入出力接続部
３６：記憶手段
３６ａ：入出力接続部
３７：通信インタフェース部
４０：環境管理サーバ
４１：ＣＰＵ
４１ａ：環境情報管理部
４１ｂ：環境差異レポート作成部
４２：記憶手段
４３：通信インタフェース部
５０：サービス提供サーバ
５１：ＣＰＵ
５１ａ：サービス要求確認部
５１ｂ：環境認証依頼部
５１ｃ：転送部（環境差異レポート依頼部）
５１ｄ：環境差異レポート判断部
５１ｅ：本人認証用情報・生体認証依頼部
５１ｆ：サービス提供部
５１ｇ：本人認証部
５２：記憶手段

５３：通信インタフェース部

【図１】



【図２】

（ａ）現在の環境情報

要素1	A
要素2	B
要素3	C
要素4	E

（ｂ）認証済みの世代環境情報

クライアントパソコン環境要素＼世代	3世代前	2世代前	直前世代
要素1	なし	A	B
要素2	A	A	A
要素3	B	B	C
要素4	E	E	E

（ｃ）前世代との環境差異テーブル（ａとｂとの対比結果）

クライアントパソコン環境要素＼世代	3世代前	2世代前	直前世代
要素1	×	○	×
要素2	×	×	×
要素3	×	×	○
要素4	○	○	○

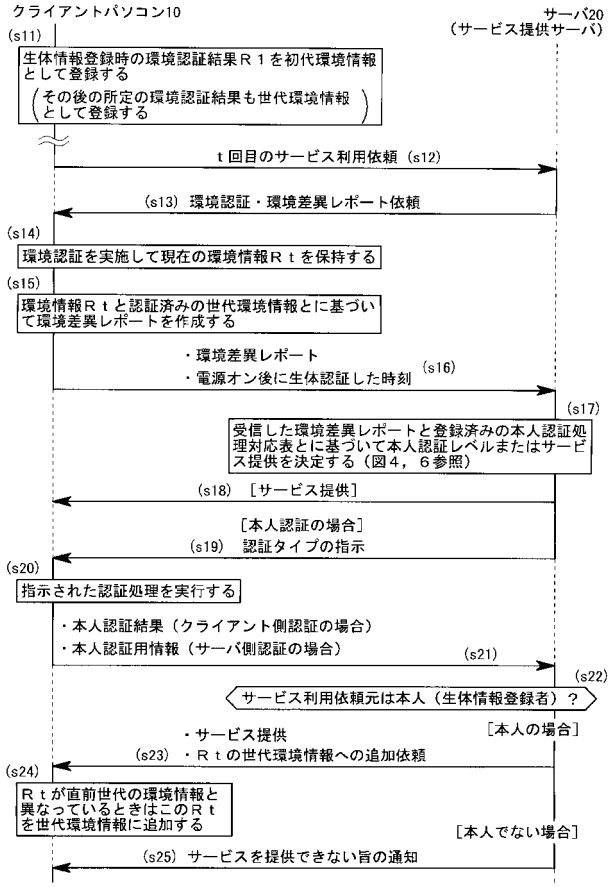
（○：差異なし
×：差異あり）

⇩

［現在の環境情報（ａ）の中で、全ての前世代と異なる環境要素２が環境差異レポートの対象となる］

【図３】

図１の本人認証システムにおける処理手順



【図４】

（ａ）現在の環境情報ファイル（クライアントパソコンでの環境認証結果）

要素番号	区分	要素名	値	備考（後の設定内容）
1	ハード／本体	本体	FMVNG2E3 CP123456	機器番号
2	ハード／周辺機器	LANカード	0A1B2CD3-99E9-4260-1234-4F1967G0H7I2	MACアドレス
3	ハード／周辺機器	ハードディスク	FJ HDD USB DEVICE	
4	OS	W－XP	2002 Service Pack2	バージョン・レベル
5	ソフト	IE	6.0 Service Pack2	バージョン・レベル
6	ソフト	OFFICE 2003	2003 Service Pack2	バージョン・レベル
7	環境設定値	IPアドレス	10.123.234.5	
8	環境設定値	サブネットマスク	255.255.255.0	
9	環境設定値	デフォルトゲートウェイアドレス	10.123.234.1	

（ｂ）ｎ世代前との環境差異ファイル（環境差異レポートの作成用データ）

要素番号	区分	要素名	差異有無	差異のある要素の項目	差異のある要素の旧値
1	ハード／本体	本体	無		
2	ハード／周辺機器	LANカード	無		
3	ハード／周辺機器	ハードディスク	有	FJ HDD USB DEVICE	
4	OS	W－XP	無		
5	ソフト	IE	無		
6	ソフト	OFFICE 2003	無		
7	環境設定値	IPアドレス	有	10.123.234.5	10.123.234.10
8	環境設定値	サブネットマスク	無		
9	環境設定値	デフォルトゲートウェイアドレス	無		

（ｃ）環境差異レポート

差異コード	差異レベル	
3	1	→ＩＰアドレスが異なるが、ネットワークアドレスが同一
4	1	→周辺機器（ハードディスク）が追加されている

【図５】

環境差異レベル設定表

環境差異の内容	差異コード	差異レベル
機器が異なる（例：サーバ判定・共通認証の場合で別のマシンを操作した時）	1	3
ネットワーク接続環境が異なる（LAN接続、無線LAN接続、携帯電話接続など）	2	2
IPアドレスが異なるが、ネットワークアドレスが同一	3	1
周辺機器が追加されている	4	1
搭載ソフトが追加されている	5	1
電源がオンされてからはじめての取引	6	3
：	：	：

【図６】

本人認証処理対応表

環境差異レベル	取引レベル	認証処理
0（差異なし）	0 ログイン	共通認証利用でない時、サービス提供側認証（ログイン認証）
	1（照会）	認証処理せず次に進む
	2（資金移動）	サービス提供側認証（第二パスワード）
1 軽度差異	0 ログイン	共通認証利用でない時、サービス提供側認証（ログイン認証）
	1（照会）	認証処理せず次に進む
	2（資金移動）	生体認証＋サービス提供側認証（第二パスワード認証）
2 中度差異	0 ログイン	共通認証利用でない時、サービス提供側認証（ログイン認証）
	1（照会）	生体認証
	2（資金移動）	生体認証＋サービス提供側認証（第二パスワード認証）
3 重度差異	すべてのレベル	生体認証＋サービス提供側認証（ログイン認証）

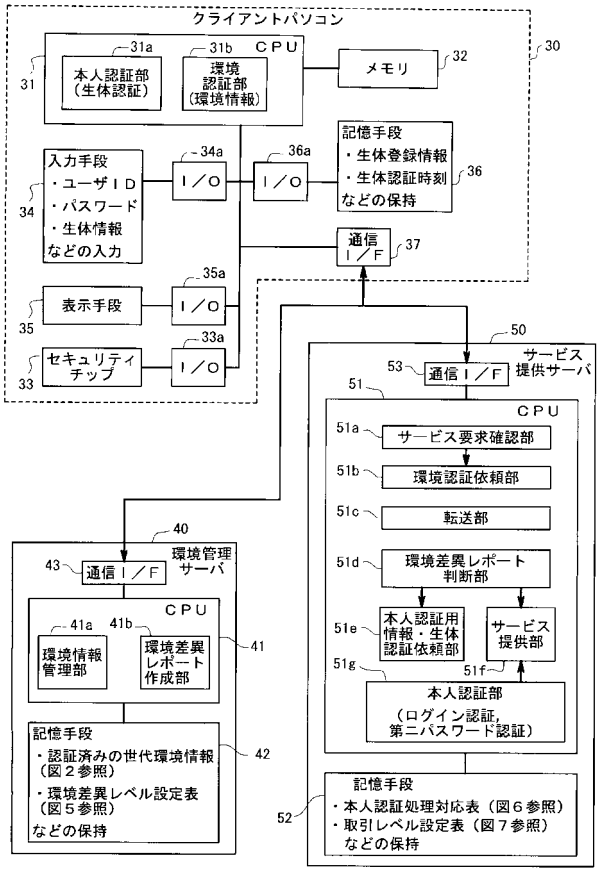
【図７】

取引レベル設定表

取引の種別（サービス提供内容）	取引レベル
ログイン	0
照会	1
資金移動	2
⋮	

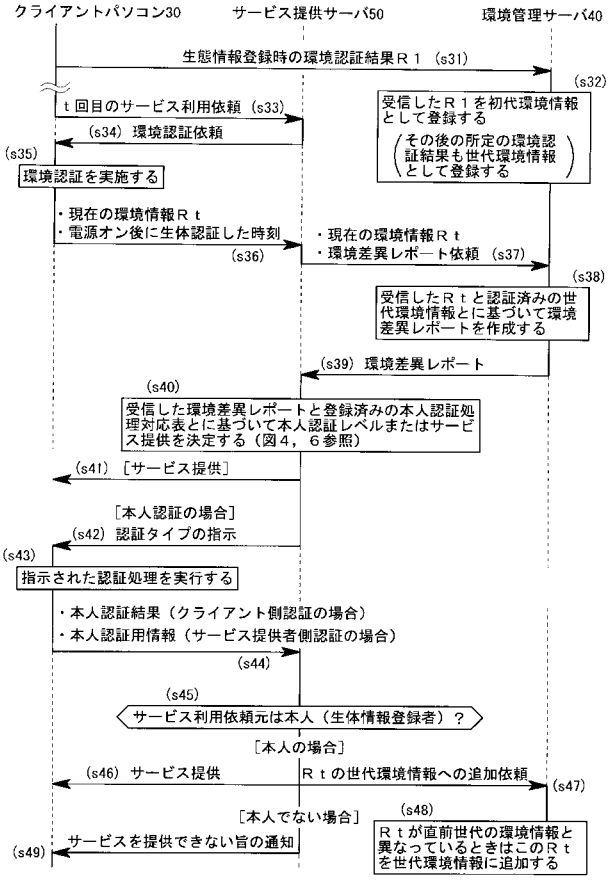
【図８】

世代環境情報を環境管理サーバで管理する場合



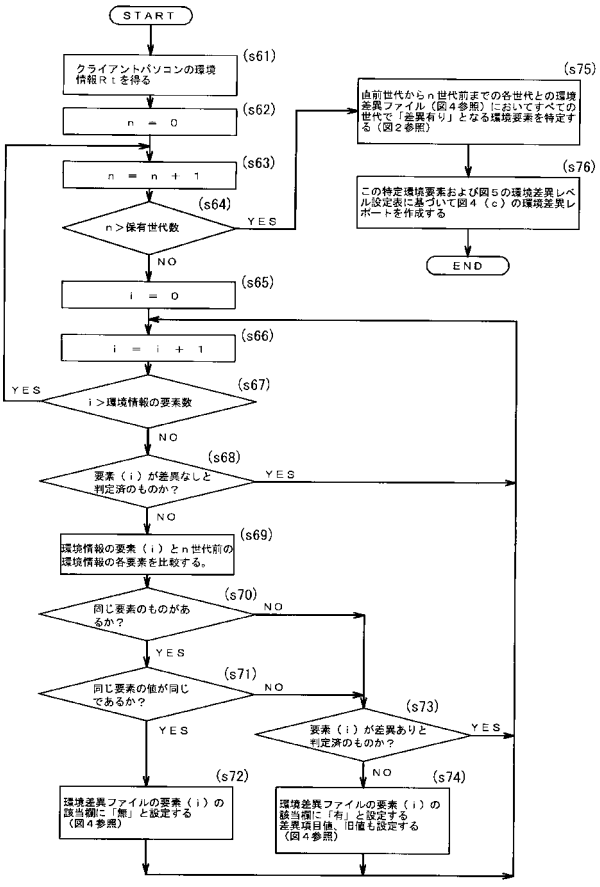
【図９】

図８の本人認証システムにおける処理手順



【図１０】

図３の(s15)および図９の(s38)における環境差異レポートの作成フロー



【図１１】

図３の(s17)および図９の(s40)における決定フロー