(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2007年1月18日 (18.01.2007)

PCT

(10) 国際公開番号
WO 2007/007690 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G09C 1/00* (2006.01)
G06F 21/20 (2006.01)

(21) 国際出願番号: PCT/JP2006/313615

(22) 国際出願日: 2006年7月7日 (07.07.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-199189 2005年7月7日 (07.07.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 森尻 智昭 (MORIJIRI, Tomoaki) [JP/JP]. 岡田 光司 (OKADA, Koji) [JP/JP]. 高見澤 秀久 (TAKAMIZAWA, Hidehisa) [JP/JP]. 山田 朝彦 (YAMADA, Asahiko) [JP/JP]. 池田 竜朗 (IKEDA, Tatsuro) [JP/JP].

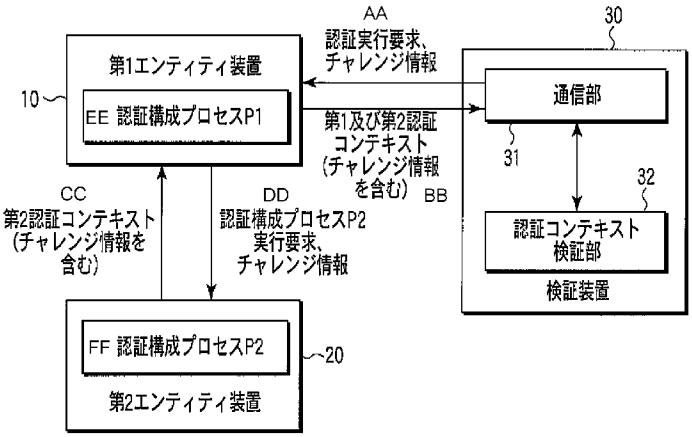
(74) 代理人: 鈴江 武彦, 外(SUZUYE, Takehiko et al.); 〒1050001 東京都港区虎ノ門１丁目１２番９号 鈴榮特許綜合事務所内 Tokyo (JP).

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

[続葉有]

(54) Title: AUTHENTICATION SYSTEM, DEVICE, AND PROGRAM

(54) 発明の名称: 認証システム、装置及びプログラム



10... FIRST ENTITY DEVICE
EE... AUTHENTICATION CONFIGURATION PROCESS P1
20... SECOND ENTITY DEVICE
FF... AUTHENTICATION CONFIGURATION PROCESS P2
30... VERIFICATION DEVICE
31... COMMUNICATION UNIT
32... AUTHENTICATION CONTEXT VERIFICATION UNIT
AA... AUTHENTICATION EXECUTION REQUEST, CHALLENGE INFORMATION
BB... FIRST AND SECOND AUTHENTICATION CONTEXT (INCLUDING CHALLENGE INFORMATION)
CC... SECOND AUTHENTICATION CONTEXT (INCLUDING CHALLENGE INFORMATION)
DD... AUTHENTICATION CONFIGURATION PROCESS P2 EXECUTION REQUEST, CHALLENGE INFORMATION

(57) Abstract: A verification device (30) transmits challenge information to a first entity device (10) and receives an authentication context in response. For each of the authentication contexts, the verification device (30) verifies that the same challenge information as the challenge information which has been sent in advance is described, thereby confirming that each authentication context is the current authentication context. Thus, it is possible to prevent repeated attack repeatedly using the past authentication context and improve the safety against the repeated attack.

(57) 要約: 検証装置３０は、第１エンティティ装置１０にチャレンジ情報を送信し、折り返し受信した各認証コンテキスト毎に、予め送信したチャレンジ情報と同一のチャレンジ情報が記述されていることを検証することにより、各認証コンテキストが現在の認証コンテキストであることを確認できるので、過去の認証コンテキストを繰り返し用いる繰り返し攻撃を防ぎ、繰り返し攻撃に対して安全性を向上できる。

WO 2007/007690 A1

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

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

添付公開書類:
— 国際調査報告書

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

明 細 書

認証システム、装置及びプログラム

技術分野

[0001] 本発明は、認証の実行結果を保証する認証コンテキストを検証者側に通知する認証システム、装置及びプログラムに係り、例えば、過去の認証コンテキストを繰り返し用いる繰り返し攻撃に対して安全性を向上し得る認証システム、装置及びプログラムに関する。

背景技術

[0002] ネットワークを介した通信やサービスにおいて、通信相手を認証することは必須な技術要素である。近年、特にオープンなネットワーク環境の普及や、分散されたサービス・リソースの連携技術の発達に伴い、認証対象がユーザから機器端末まで拡大している。

[0003] これに伴い、多様なレイヤでの認証手段が実現されている。例えば、OSI7層モデルのセッション層での、SSL(Secure Sockets Layer)／TLS(Transport Layer Security)が挙げられる。例えば、文献1([SSL3.0] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.)及び文献2([TLS1.0] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC2246, Jan 1999, <http://www.ietf.org/rfc/rfc2246.txt>)を参照。SSL／TLSは、上位層に対して透過的な秘匿通信を提供可能なため、標準的な秘匿通信プロトコルとして普及している。SSL／TLSでは、認証機構として、公開鍵証明書をベースとしたサーバ認証とクライアント認証をサポートしている。

[0004] また、OSI7層モデルのネットワーク層における通信プロトコルであるIP(Internet Protocol)を対象とした秘匿通信としてIPsecがある。例えば、文献3([IPsec] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", November 1998,<http://www.ietf.org/rfc/rfc2401.txt>)を参照。IPsecは、IPパケットレベルでの認証及び暗号化を図り、ホスト単位の秘匿通信を実現し、VPN(Virtual Private Network)等に利用される。IPsecは、既知共有鍵による通信相手の認証をサポートしており、動

的な認証には、上位のセキュリティ合意交渉機構であるIKEやIKEv2等の仕組みを利用可能としている。

[0005] 一方、ユーザ認証に関するセキュリティのステートメントを表明する産業標準仕様としては、SAML(Security Assertion Markup Language)が策定されている。例えば、文献4([SAML] OASIS Security Services TC, "Security Assertion Markup Language (SAML) v1.1", Sept 2003, <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security>)を参照。SAMLは、クライアントのセキュリティやポリシ決定に関わるステートメントをXML形式で表現し、電子的に保証するための枠組みである。

[0006] 以上のように、ネットワークを介した認証手段は、様々なレイヤでの適用が進んでおり、前述したように、通信やサービスに必須な技術要素となっている。

[0007] また、認証対象者が個人である場合に、個人が本人か否かを確認する技術も現在注目されている。通常、認証では、認証対象者を厳密に識別又は照合することが要件として挙げられる。このとき、認証対象者が個人である場合、個人が本人か否かを厳密に確認する本人確認技術が必要になる。

[0008] 現在、本人確認を実施する有望な技術として、バイオメトリクス(生体照合/認証技術)が挙げられる。バイオメトリクスは、個々人が有する固有の身体的特徴又は特性を事前に登録した生体情報(以下、参照生体情報)と照合し、本人か否かを確認する技術である。生体情報には、指紋や虹彩、網膜、顔、音声、キーストローク、サインなどが利用される。

[0009] バイオメトリクスでは、パスワードなどの既存の認証方法と異なり、紛失や忘失の心配が無い生体情報を利用するため、ユーザの負荷が軽減される。また、生体情報は複製が困難なものを前提としており、ユーザの成り済ましなどの防止策に有効である。

[0010] また、現在インターネットに代表されるオープンネットワークが普及し、電子商取引などにおいてネットワーク越しに通信相手を認証する方法としてバイオメトリクスを利用しようとする動きが高まってきている。また、身分証明などの分野でもバイオメトリクスを利用して、身分証明書の所有者の本人確認を行うことも検討されている。

[0011] ネットワーク経由を想定したバイオメトリクス利用には、照合結果や照合情報のネットワーク経路上での安全性が問題となるが、公開鍵認証基盤(Public Key Infrastructure)やICカードなどのセキュア媒体との組合せにより、通信経路上や機器等で、生体情報などの重要な情報の盗難や改竄の危険性が減少している。

[0012] さらに前述したような複数のバイオメトリック方式を組み合わせて総合的に本人確認をする複合型のバイオメトリック・システムにより、より精度の高い本人確認を実行可能になってきている。

[0013] しかしながら、現状の多くの認証技術は、認証を構成するプロセスを同一の管理ドメインが管理することを想定するため、各プロセス自体の保証を考慮していない問題がある。

[0014] 例えばバイオメトリクスの場合、生体情報の読取機能や照合機能といった認証構成プロセスが、実装されるデバイスや機器上でどのように配置されるかは、システム固有に決まる場合が多い。具体的には、バイオメトリック・モデルの一つであるマッチング・オン・カード(Matching on Card:MOC)モデルでは、生体情報の読取機能がスキャナ上に配置され、生体情報の照合機能と参照生体情報(テンプレート)の管理機能がカード(スマートカードなど)上に配置される。

[0015] このように認証構成プロセスは、プロセス毎に管理主体が異なる場合が多い。このため、各管理主体毎の認証構成プロセスが妥当か否かを、認証結果を検証する検証者側が明確に把握することが困難である。

[0016] よって、認証構成プロセスの妥当性を把握できないことから、認証構成プロセスを統合した認証プロセス全体としては、信頼性を低下させている心配がある。特に、オープンなネットワーク環境での認証処理では、同一管理ドメインで運用されるとは限らないため、この心配が顕著になると考えられる。

[0017] この問題を解決する技術として、バイオメトリクス認証コンテキスト(Biometric Authentication Context)に代表される認証コンテキストを用いた認証システムが知られている。例えば、文献5(Koji Okada, Tatsuro Ikeda, Hidehisa Takamizawa, Toshiaki Saisho, Extensible Personal Authentication Framework using Biometrics and PKI, Pre-Proceedings of The 3rd International Workshop for Applied PKI (IWAP2004), pp.96-10

7.)を参照。認証コンテキストとは、本人確認を構成する各構成プロセスを実行する管理主体(エンティティ装置)がその実行結果を保証することにより、検証者側で各構成プロセスの実行結果の正当性を検証可能とする技術である。

[0018] 具体的な実行手順は以下の通りである。

始めに、各構成プロセスを実行する管理主体は、予め秘密情報(例えば公開鍵暗号方式における秘密鍵)を保持する。本人確認を行う場合、各管理主体は、自身の実行した構成プロセスの実行結果に対して、保持している秘密情報を用いて認証子(例えばデジタル署名)を生成し、その実行結果と認証子を認証コンテキストと呼ばれる特定のフォーマットに従って整形して出力する。続いて、各管理主体は互いに、本人確認の実行順に認証コンテキストを受け渡す。最後の管理主体は、最終的に出力された認証コンテキストを検証者に送信する。

[0019] 検証者は、認証コンテキストに記述された認証子の正当性を(例えばデジタル署名に対応する公開鍵により)検証することによって、本人確認実行結果の正当性を検証することが可能となる。

発明の開示

[0020] 以上のような文献5に記載の認証システムは、通常は何の問題も無いが、本発明者の入念な検討によれば、以下の4通りの不都合(1)～(4)が生じる可能性があり、それぞれ別々に改良の余地があると考えられる。

[0021] (1)第1の不都合は、過去の認証コンテキストを繰り返し用いる「繰り返し攻撃」を受けた場合、過去の認証コンテキスト内の実行結果を現在の正しい実行結果と判断してしまうことである。

[0022] 補足すると、この場合の「繰り返し攻撃」とは、過去に行われた本人確認にて生成した認証コンテキストを現在の本人確認における認証コンテキストとして検証者へ送信する攻撃を意味する。検証者は、このような繰り返し攻撃に対し、本人確認の実行結果を正しいと判断してしまう。

[0023] 例えばMOCモデルにおいて過去にスキャナが出力した認証コンテキストにより、後段の本人確認(照合処理等)をした場合、検証者は、認証コンテキスト内の生体情報が過去にスキャンされた生体情報である旨を検出できず、正しい生体情報と判断して

しまう。

[0024] 従って、第1の不都合に関しては、過去の認証コンテキストを繰り返し用いる繰り返し攻撃に対し、安全性を向上させるように改良の余地があると考えられる。

[0025] (2)第2の不都合は、生体情報の「すり替え」を受けた場合、すり替え後の生体情報を照合処理に用いてしまうことである。

[0026] 補足すると、認証の際には、プライバシの観点から検証者へ送信したくない情報(秘匿情報)がある場合がある。秘匿情報は、例えば指紋等の生体情報である。一方、構成プロセスを実行する管理主体間では生体情報を受け渡さなければ本人確認を実行できない状況がある。

[0027] このため、文献5に記載の技術では、認証コンテキストに生体情報の関連情報(ハッシュ値など)を記述し、生体情報と認証コンテキストを別々に受け渡すことにより、検証者へ送信する認証コンテキスト内に生体情報を含めない方式を提案している。

[0028] 例えば、MOCモデルにおいて生体情報を検証者へ送信したくない場合、スキャナからカードへは、スキャンした生体情報と、その生体情報の関連情報(ハッシュ値など)を含む認証コンテキストとを別々に送信する。このとき、送信された生体情報のみをすり替えることにより、不正な本人確認が成功する可能性がある。これは、スキャンされた生体情報と、すり替え後の生体情報とが異なることを検証できず、すり替え後の不正な生体情報をカードが照合処理に用いてしまうことによる。

[0029] 文献5では、この不正を防ぐ方法として、入力された生体情報と認証コンテキスト内の関連情報(ハッシュ値など)とが対応することを各管理主体により検証する方式を提案している。しかしながら、各管理主体は、比較的計算能力が低いスキャナやスマートカードなどである。よって、このような各管理主体による検証は現実的でない。

[0030] 従って、第2の不都合に関しては、生体情報等の秘匿情報のすり替え攻撃に対し、安全性を向上させるように改良の余地があると考えられる。

[0031] (3)第3の不都合は、本人確認の実行主体(要求者)のセキュリティレベルが検証者のセキュリティポリシを満たす旨を保証するプロトコルにおいて、要求者の様々な実行環境が検証者に把握されてしまうことである。

[0032] 具体的には、文献5に記載の技術では、認証を実行する際、検証者は要求者に対

してプロファイルリスト要求情報を送信する。ここで、プロファイルとは、本人確認を実行する管理主体の組み合わせ、各管理主体が実行する構成プロセス、各管理主体間の情報交換規則、セキュリティ実施規則(セキュリティレベルを含む)などといった実行環境を規定した情報である。プロファイルリストとは、複数の上記プロファイルをリストとして記述した情報である。

[0033] 要求者はプロファイルリスト要求情報に対し、自身が保持する管理主体の組み合わせで実行可能な全てのプロファイルからなるプロファイルリストを生成し、検証者へ送信する。検証者は、受信したプロファイルリストの中から、自身の設定したセキュリティポリシに従い、実行するプロファイルを決定する。ここで、セキュリティポリシとは、検証者が受け入れ可能なセキュリティレベルを記述した情報である。このセキュリティポリシ内のセキュリティレベルとプロファイル内のセキュリティレベルとを比較することにより、プロファイルがセキュリティポリシを満たす旨を保証できる。

[0034] そして、検証者は、決定したプロファイルを要求者へ指定する。要求者は指定されたプロファイルに従って本人確認を実行する。

[0035] 以上の過程は、要求者が送信するプロファイルリストにより、要求者の様々な実行環境を検証者が把握してしまうので、要求者のプライバシ保護の観点から好ましくない。

[0036] 従って、第3の不都合に関しては、要求者の様々な実行環境を検証者から秘匿するように改良の余地があると考えられる。

[0037] (4)第4の不都合は、認証コンテキストの通信効率が低いことである。

例えば検証装置30が認証コンテキストを検証する際に、認証コンテキスト内の静的情報(各認証間で同一の情報)を参照する場合がある。ここで、静的情報には、エンティティ装置の作成メーカの情報や、バイオメトリクス認証におけるキャプチャ装置の精度情報、生体参照情報(テンプレート)の評価情報などがある。

[0038] いずれにしても静的情報を参照する場合、認証毎に、同一の静的情報を含む認証コンテキストを検証装置30に送信するので、通信量の観点から効率が低い。

[0039] 従って、第4の不都合に関しては、認証コンテキストの通信効率を向上させるように改良の余地があると考えられる。

[0040] 本発明の第1の目的は、過去の認証コンテキストを繰り返し用いる繰り返し攻撃に対して安全性を向上し得る認証システム、装置及びプログラムを提供することにある。

[0041] 本発明の第2の目的は、秘匿情報のすり替え攻撃に対して安全性を向上し得る認証システム、装置及びプログラムを提供することにある。

[0042] 本発明の第3の目的は、要求者の様々な実行環境を検証者から秘匿し得る認証システムを提供することにある。

[0043] 本発明の第4の目的は、認証コンテキストの通信効率を向上し得る認証システム、装置及びプログラムを提供することにある。

[0044] 本発明の第1の局面(aspect)は、認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置と、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置とを備えた認証システムであって、前記各認証エンティティ装置としては、前記検証装置により生成されたチャレンジ情報を受信するチャレンジ情報受信手段と、前記検証のための秘密情報が記憶された秘密情報記憶手段と、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子を生成する認証子生成手段と、前記認証子と前記実行内容及び前記チャレンジ情報とを特定のフォーマットに従って記述した認証コンテキストを生成する認証コンテキスト生成手段と、前記認証コンテキストを送信する認証コンテキスト送信手段とを備えており、前記検証装置としては、前記秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段と、前記チャレンジ情報を生成するチャレンジ生成手段と、このチャレンジ情報が記憶されるチャレンジ記憶手段と、前記チャレンジ情報を送信するチャレンジ情報送信手段と、前記各認証エンティティ装置により生成された各認証コンテキストを受信する認証コンテキスト受信手段と、前記受信した各認証コンテキスト毎に、前記チャレンジ記憶手段内のチャレンジ情報と同一のチャレンジ情報が記述されているか否かを検証するチャレンジ検証手段と、前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段と、前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段とを備えた認証システムである。

[0045] 第1の発明によれば、検証装置が、受信した各認証コンテキスト毎に、チャレンジ記憶手段内のチャレンジ情報と同一のチャレンジ情報が記述されていることを検証することにより、各認証コンテキストが現在の認証コンテキストであることを確認できるので、過去の認証コンテキストを繰り返し用いる繰り返し攻撃を防ぎ、繰り返し攻撃に対して安全性を向上できる。

[0046] 本発明の第2の局面は、認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置と、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置とを備えた認証システムであって、前記各認証エンティティ装置としては、少なくとも1台の前段側の認証エンティティ装置及び少なくとも1台の後段側の認証エンティティ装置を備えており、前記前段側の認証エンティティ装置としては、前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値を生成する前段側ハッシュ値生成手段と、前記検証のための秘密情報が記憶された前段側秘密情報記憶手段と、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子を生成する前段側認証子生成手段と、前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とを特定のフォーマットに従って記述した認証コンテキストを生成する前段側認証コンテキスト生成手段と、前記認証コンテキスト及び前記秘匿実行内容を送信する前段側送信手段とを備えており、前記後段側の認証エンティティ装置としては、前記送信された秘匿実行内容を受信する秘匿実行内容受信手段と、前記受信した秘匿実行内容を対象とした後段側ハッシュ値を生成する後段側ハッシュ値生成手段と、前記検証のための秘密情報が記憶された後段側秘密情報記憶手段と、この秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象とした認証子を生成する後段側認証子生成手段と、前記認証子、前記実行内容及び前記後段側ハッシュ値を特定のフォーマットに従って記述した認証コンテキストを生成する後段側認証コンテキスト生成手段と、この認証コンテキストを送信する後段側送信手段とを備えており、前記検証装置としては、前記各秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段と、前記各認証エン

ティティ装置により生成された各認証コンテキストを受信する認証コンテキスト受信手段と、前記受信した各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることを比較検証するハッシュ値比較検証手段と、前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段と、前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段とを備えた認証システムである。

[0047] 第2の局面によれば、検証装置が、各認証コンテキストに含まれるハッシュ値が互いに同一であることを検証することにより、前段の認証構成プロセスの秘匿実行内容と後段の認証構成プロセスの秘匿実行内容とが同一であることを確認できるので、秘匿情報のすり替え攻撃に対して安全性を向上できる。

[0048] 本発明の第3の局面は、第1又は第2の局面において、前記検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置を備え、前記検証装置としては、前記認証構成プロセスの実行に関し、受け入れ可能な実行環境を規定したプロファイルリストを生成するプロファイルリスト生成手段と、前記プロファイルリストを認証要求装置へ送信するリスト送信手段とを備えており、前記認証要求装置としては、前記プロファイルリストを受信するプロファイルリスト受信手段と、認証構成プロセスを実行する機能を規定した機能リストを前記各認証エンティティ装置毎に受信する機能リスト受信手段と、前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するプロファイル決定手段と、前記実行プロファイルを各認証エンティティ装置に送信する実行プロファイル送信手段とを備えており、前記各認証エンティティ装置としては、前記認証要求装置から前記実行プロファイルを受信する実行プロファイル受信手段と、この実行プロファイルに基づいて、前記認証構成プロセスを実行する認証構成プロセス実行手段とを備えた認証システムである。

[0049] 第3の局面によれば、第1又は第2の局面の作用に加え、検証装置の受け入れ可能な実行環境を示すプロファイルリストと、各認証エンティティ装置の機能リストとの両者を満たすように、各認証エンティティ装置の実行環境を示す実行プロファイルを認証要求装置が決定することにより、認証の実行に関係しない各エンティティ装置の様々な実行環境を検証装置から秘匿できるので、各認証エンティティ装置側の要求者

のプライバシを保つことができる。

[0050] 本発明の第4の局面は、第1乃至第3の局面のいずれかにおいて、前記各認証エンティティ装置としては、認証毎に同一内容を表す静的情報に関し、前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報が記憶されるリンク先情報記憶手段を備えており、前記認証コンテキスト生成手段としては、前記静的情報に代えて前記リンク先情報を含むように前記認証コンテキストを生成しており、前記検証装置としては、受信した認証コンテキスト内のリンク先情報に基づいて、静的情報を取得する手段と、この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理を検証する検証手段とを備えた認証システムである。

[0051] 第4の局面によれば、第1～第3の各局面の作用に加え、各エンティティ装置が、認証毎に同一内容を表す静的情報に関し、静的情報に代えて静的情報のデータ量よりも小さいデータ量からなり静的情報を取得するリンク先情報を含むように認証コンテキストを生成するので、認証コンテキストのサイズが小さくなることから、認証要求装置と検証装置間の通信量を低減でき、認証コンテキストの通信効率を向上できる。

[0052] なお、以上の各局面は、各装置からなる「システム」として表現したが、これに限らず、各装置からなる又は各装置毎の「装置」、「プログラム」、「コンピュータ読み取り可能な記憶媒体」又は「方法」として表現してもよい。

図面の簡単な説明

[0053] [図1]図1は、本発明の第1の実施形態に係る認証システムの構成を示す模式図である。

[図2]図2は、同実施形態における認証プロセスを説明するためのフローチャートである。

[図3]図3は、同実施形態における各エンティティ装置の構成を示す模式図である。

[図4A]図4Aは、同実施形態における認証コンテキストの構成を示す模式図である。

[図4B]図4Bは、同実施形態における認証コンテキストの構成を示す模式図である。

[図5]図5は、同実施形態における検証装置の構成を示す模式図である。

[図6]図6は、同実施形態における動作を説明するためのフローチャートである。

[図7]図7は、本発明の第2の実施形態に係る認証システムの構成を示す模式図である。

[図8]図8は、同実施形態における各エンティティ装置の構成を示す模式図である。

[図9]図9は、同実施形態における検証装置の構成を示す模式図である。

[図10]図10は、本発明の第3の実施形態に係る認証システムの構成を示す模式図である。

[図11]図11は、同実施形態における認証要求装置の構成を示す模式図である。

[図12]図12は、同実施形態におけるプロファイルリストを説明するための模式図である。

[図13]図13は、同実施形態における実行プロファイルを説明するための模式図である。

[図14]図14は、同実施形態における各エンティティ装置の構成を示す模式図である。

[図15]図15は、同実施形態における動作を説明するためのシーケンス図である。

[図16]図16は、同実施形態における変形例の構成を示す模式図である。

[図17]図17は、本発明の第4の実施形態に係る認証システムの構成を示す模式図である。

[図18]図18は、同実施形態におけるテンプレート証明書の例を示す模式図である。

[図19]図19は、同実施形態における各エンティティ装置の構成を示す模式図である。

[図20A]図20Aは、同実施形態における認証コンテキストの構成を示す模式図である。

[図20B]図20Bは、同実施形態における認証コンテキストの構成を示す模式図である。

[図21]図21は、同実施形態における変形例の構成を示す模式図である。

[図22]図22は、同実施形態における変形例の構成を示す模式図である。

発明を実施するための最良の形態

[0054] 以下、本発明の各実施形態について図面を参照して詳細に説明する。

[0055] （第1の実施形態）

図1は本発明の第1の実施形態に係る認証システムの構成を示す模式図である。この認証システムにおいては、図2に示すように、認証プロセスが認証構成プロセスP1及び認証構成プロセスP2という2つのプロセスから構成され、それぞれの構成プロセスP1，P2の実行結果を基に認証結果が得られ、それぞれの構成プロセスP1，P2が異なるエンティティ装置10，20で実行される、すなわち認証構成プロセスP1が第1エンティティ装置10で実行され、認証構成プロセスP2が第2エンティティ装置20で実行される場合の一例である。

[0056] ここで、認証構成プロセスP1，P2とは、認証プロセスの構成要素である各プロセスであり、具体的には、認証プロセス全体を各プロセスに分離したときの当該各プロセスである。言い換えると、認証プロセスを全体プロセスとした場合、認証構成プロセスP1，P2は、全体プロセスの中の各部分プロセスを意味している。

[0057] 認証プロセスは、2つの認証構成プロセスに限らず、3つ以上の認証構成プロセスに分離されていてもよく、それらがそれぞれ異なるエンティティ装置で実行されてもよい。また、後段の認証構成プロセスは、前段の認証構成プロセスの結果を参照して実行されてもよく、また参照しなくてもよい。

[0058] 図1に示す認証システムは、検証装置30、第1エンティティ装置10及び第2エンティティ装置20からなる。検証装置30は、第1エンティティ装置10と通信可能な通信部31と、第1及び第2エンティティ装置10，20が生成した認証コンテキストを検証する認証コンテキスト検証部32とを備えている。

[0059] 各エンティティ装置10，20は、図3に示すように、通信部11，21、認証構成プロセスP1実行部12，認証構成プロセスP2実行部22，秘密情報管理部13，23、認証子生成部14，24及び認証コンテキスト生成部15，25を備えている。なお、符号が10番台の要素は、第1エンティティ装置10に属しており、符号が20番台の要素は、第2エンティティ装置に属している。

[0060] 各通信部11，21は、検証装置30及び他エンティティ装置20，10等の外部装置と、自装置10，20内との間の通信を実行するものである。

[0061] 例えば通信部11は、検証装置30から認証実行要求及びチャレンジ情報を受信す

る機能と、受信した認証実行要求から認証構成プロセスP2実行要求を生成する機能と、この認証構成プロセスP2実行要求及びチャレンジ情報を第2エンティティ装置20に送信する機能と、第2エンティティ装置から第2認証コンテキストを受信する機能と、前述した認証実行要求を認証構成プロセスP1実行部12に送出する機能と、前述したチャレンジ情報を認証コンテキスト生成部15に送出する機能と、認証コンテキスト生成部15から得られた第1認証コンテキストを前述した第2認証コンテキストと共に検証装置30に送信する機能とをもっている。

[0062] 一方、通信部21は、第1認証エンティティ装置10から認証構成プロセスP2実行要求及びチャレンジ情報を受信する機能と、受信した認証構成プロセスP2実行要求を認証構成プロセスP2実行部22に送出する機能と、受信したチャレンジ情報を認証コンテキスト生成部25に送出する機能と、認証コンテキスト生成部25から得られた第2認証コンテキストを第1認証エンティティ装置10に送信する機能とをもっている。

[0063] 認証構成プロセスP1実行部12は、通信部11から受けた認証実行要求に基づいて、前述の認証構成プロセスP1を実行し、その実行結果を認証コンテキスト生成部15に出力するものである。

[0064] 認証構成プロセスP2実行部22は、通信部21から受けた認証実行要求に基づいて、前述の認証構成プロセスP2を実行し、その実行結果を認証コンテキスト生成部25に出力するものである。

[0065] 秘密情報管理部13は、予め認証子を生成するための秘密情報1が格納された記憶装置であり、認証子生成部14から読出可能となっている。

[0066] 秘密情報管理部23は、予め認証子を生成するための秘密情報2が格納された記憶装置であり、認証子生成部24から読出可能となっている。

[0067] 認証子生成部14，24は、認証コンテキスト生成部15，25から入力されたデータ(実行結果、チャレンジ情報等)を対象として、秘密情報管理部13，23から読み出した秘密情報1，2を用いて認証子を生成し、得られた認証子を認証コンテキスト生成部15，25に送出するものである。

[0068] 認証子とは、例えばデジタル署名、メッセージ認証符号(Message Authentication Code:MAC)である。秘密情報1，2とは、(認証コンテキストを検証するための)認証子

を生成するための鍵情報であり、例えば認証子がデジタル署名の場合は公開鍵暗号方式における秘密鍵であり、認証子がメッセージ認証符号の場合は予め検証装置30と共有された共通鍵である。

[0069] 認証コンテキスト生成部15，25は、認証構成プロセスP1，P2実行部12，22の実行結果、認証子生成部14，24から送出された認証子、通信部11，21から送出されるチャレンジ情報を、特定のフォーマットに従って記述及び整形し、得られた認証コンテキストを通信部11，21に送出するものである。

[0070] ここで、図4Aに示すように、第1認証コンテキストAc1のフォーマットは、ヘッダブロックh1、データブロックd1、認証子ブロックa1から構成される。なお、第1認証コンテキストAc1は、ヘッダブロックh1、データブロックd1及び認証子ブロックa1からなる情報である。詳しくは、第1認証コンテキストAc1は、ヘッダブロックh1及びデータブロックd1からなるコンテキスト情報と、このコンテキスト情報を対象に生成された認証子ブロックa1とからなる情報である。

[0071] ヘッダブロックh1は、例えばリクエスタのように、この認証コンテキストAc1を特定する情報や、チャレンジ情報のように認証コンテキストの正当性を示す情報などが記述される。チャレンジ情報は、「繰り返し攻撃」を防ぐ観点から、認証実行要求毎に発行される変数情報であり、例えば乱数、また予め検証装置と各エンティティ装置間で取り決められたシリアル番号や時間情報などの一時的な変数が使用可能となっている。

[0072] データブロックd1には、エンティティ情報が記述される。エンティティ情報は、認証構成プロセスP1の実行結果などの動的な情報（認証毎に生成される情報）を含み、これに限らず、例えば実行環境などの静的情報（各認証を通じて同じ情報）が使用可能となっている。静的情報は、例えばエンティティ装置の作成メーカの情報、バイオメトリクス認証におけるキャプチャ装置の精度情報、生体参照情報（テンプレート）の評価情報などが使用可能となっている。

[0073] 認証子ブロックa1には、ヘッダブロックh1及びデータブロックd1を対象に秘密情報1に基づいて生成された認証子が記述される。

[0074] 第2認証コンテキストAc2のフォーマットは、図4Bに示すように、第1認証コンテキストAc1のフォーマットと同様である。このため、第2認証コンテキストAc2は、同様に、

ヘッダブロックh2、データブロックd2及び認証子ブロックa2からなる情報である。詳しくは、第2認証コンテキストAc2は、ヘッダブロックh2及びデータブロックd2からなるコンテキスト情報と、このコンテキスト情報を対象に生成された認証子ブロックa2とからなる情報である。認証子の生成について補足すると、認証子ブロックa2には、ヘッダブロックh2及びデータブロックd2を対象に秘密情報2に基づいて生成された認証子が記述される。

[0075] 一方、検証装置30は、図5に示すように、通信部31及び認証コンテキスト検証部32を備えている。

[0076] ここで、通信部31は、認証実行要求と、チャレンジ保存部34内のチャレンジ情報とを第1エンティティ装置10に送信する機能と、第1エンティティ装置10から第1及び第2認証コンテキストを受信する機能と、受信した第1及び第2認証コンテキストを認証コンテキスト検証部32に送出する機能とをもっている。

[0077] 認証コンテキスト検証部32は、チャレンジ生成部33、チャレンジ保存部34、チャレンジ検証部35、コンテキスト検証部36、秘密情報管理部37及び認証子検証部38を備えている。

[0078] チャレンジ生成部33は、例えば乱数などの変数情報からなるチャレンジ情報を生成し、得られたチャレンジ情報をチャレンジ保存部34に保存する機能をもっている。

[0079] チャレンジ保存部34は、チャレンジ情報が記憶されるメモリであり、例えばチャレンジ生成部33から書込可能で且つ通信部31及びチャレンジ検証部35から読出可能なメモリである。

[0080] チャレンジ検証部35は、コンテキスト検証部36から受けた各認証コンテキスト毎に、チャレンジ保存部34内のチャレンジ情報と同一のチャレンジ情報が記述されているか否かを検証する機能と、得られたチャレンジ情報検証結果をコンテキスト検証部36に返す機能とをもっている。

[0081] コンテキスト検証部36は、通信部31から各認証コンテキストを受けると、各認証コンテキストを認証子検証部38に送出する機能と、認証子検証部38から認証子検証結果を受ける機能と、各認証コンテキストをチャレンジ検証部35に送出する機能と、チャレンジ検証部35からチャレンジ検証結果を受ける機能と、認証子検証結果及びチ

ャレンジ検証結果に基づいて、各認証コンテキストの正当性を検証する機能と、各認証コンテキスト内のデータブロックの情報に基づいて、各認証構成プロセスP1，P2の内容（実行環境、実行結果など）を確認する機能とをもっている。

[0082] 秘密情報管理部37は、秘密情報1，2に対応する認証子検証情報が記憶されたメモリであり、認証子検証部38から読出可能となっている。ここで、認証子検証情報とは、（秘密情報1，2により生成された）認証子を検証するための鍵情報であり、例えば認証子がデジタル署名の場合は公開鍵暗号方式における公開鍵であり、認証子がメッセージ認証符号の場合は予めエンティティ装置10，20と共有された共通鍵である。なお、認証子検証情報は、秘密情報1，2により生成された認証子を検証することから、秘密情報1，2に対応した鍵情報となっている。ここでいう対応とは、例えば秘密情報1，2が暗号化鍵の場合、認証子検証情報が復号鍵であるといった対応関係を意味している。このため、秘密情報1，2と認証子検証情報とは、対応関係にあれば、互いに異なる内容（一方が秘密鍵で他方が公開鍵）でもよく、同一の内容（両者とも共通鍵）でもよい。

[0083] 認証子検証部38は、秘密情報管理部37内の認証子検証情報に基づいて、コンテキスト検証部36から受けた各認証コンテキスト毎に認証子を検証し、認証子検証結果をコンテキスト検証部36に送出する機能をもっている。

[0084] 次に、以上のように構成された認証システムの動作を図6のフローチャートを用いて説明する。

[0085] 認証プロセスの実行を開始するとき、検証装置30においては、チャレンジ生成部33によりチャレンジ情報を生成し、このチャレンジ情報をチャレンジ保存部34に一時的に保存する。なお、このチャレンジ情報は、後に認証実行要求と認証コンテキストとの対応付けを検証するために用いられる。

[0086] しかる後、検証装置30においては、通信部31により、認証実行要求及びチャレンジ情報を第1エンティティ装置10に送信する（ST1）。認証実行要求は、実行する認証プロセスの指定などを含む。

[0087] 第1エンティティ装置10は、認証実行要求及びチャレンジ情報を受けると（ST2）、予め決められた又は認証実行要求で指定された認証プロセスに従う。すなわち、第1

エンティティ装置10は、認証構成プロセスP2実行要求及びチャレンジ情報を第2エンティティ装置20に送信する(ST3)。この実行要求には、例えば、検証装置30からの認証実行要求に含まれる認証プロセスの指定、図示しない認証構成プロセスP2の実行に必要で且つ第1エンティティ装置10のみが保持している情報が含まれてもよい。

[0088] 第2エンティティ装置20は、第1エンティティ装置10から認証構成プロセスP2実行要求及びチャレンジ情報を受信すると(ST4)、予め決められた又は検証装置30からの認証実行要求で指定された認証プロセスに従う。すなわち、第2エンティティ装置20は、認証構成プロセスP2実行部12にて認証構成プロセスP2を実行し(ST5)、実行結果を得る。

[0089] 次に、認証コンテキスト生成部25において、チャレンジ情報と、認証構成プロセスP2の実行結果とを入力として、図4Bに示したフォーマットの第2認証コンテキストAc2を生成する(ST6～ST9)。

[0090] 具体的には、認証コンテキスト生成部25は、リクエスタ及びチャレンジ情報を含むヘッダブロックh2と、実行結果などエンティティ情報を含むデータブロックd2とを記述し、各ブロックh2, d2からなるコンテキスト情報を生成する(ST6)。なお、チャレンジ情報は、ステップST4で受信したものである。

[0091] 次に、認証子生成部24は、秘密情報管理部23から認証子生成のための秘密情報2を読み出す(ST7)。そして、前述のヘッダブロックh2及びデータブロックd2を対象に秘密情報2を用いて認証子を生成する(ST8)。最後に、生成された認証子を認証子ブロックa2へ記述し、各ブロックh2, d2, a2からなる第2認証コンテキストAc2を生成する(ST9)。

[0092] 第2エンティティ装置20は、この第2認証コンテキストAc2を通信部21を介して第1エンティティ装置10へ送信する(ST10)。

[0093] 第1エンティティ装置10は、第2認証コンテキストAc2を受信すると(ST11)、認証構成プロセスP1実行部12により認証構成プロセスP1を実行し(ST12)、実行結果を得る。

[0094] 次に、認証コンテキスト生成部15において、認証構成プロセスP1の実行結果とチ

ャレンジ情報を入力とし、図4Aに示したフォーマットの第1認証コンテキストAc1を生成する(ST13～ST16)。

[0095] 具体的には、認証コンテキスト生成部15は、リクエスタ及びチャレンジ情報を含むヘッダブロックh1と、実行結果などエンティティ情報を含むデータブロックd1とを記述し、各ブロックh1, d1からなるコンテキスト情報を生成する(ST13)。なお、チャレンジ情報は、ステップST2で受信したものである。

[0096] 次に、認証子生成部14は、秘密情報管理部13から認証子生成のための秘密情報1を読み出す(ST14)。そして、前述のヘッダブロックh1及びデータブロックd1を対象に秘密情報1を用いて認証子を生成する(ST15)。最後に、生成された認証子を認証子ブロックa1へ記述し、各ブロックh1, d1, a1からなる第1認証コンテキストAc1を生成する(ST16)。

[0097] 第2エンティティ装置20は、これら第1認証コンテキストAc1及び第2認証コンテキストAc2を通信部11を介して検証装置30へ送信する(ST17)。

[0098] 検証装置30は、第1及び第2認証コンテキストAc1, Ac2を受信する(ST18)。認証コンテキスト検証部32においては、コンテキスト検証部36が、第1及び第2認証コンテキストを認証子検証部38に送出する。認証子検証部38では、第1及び第2認証コンテキストAc1, Ac2の完全性を確認するため、秘密情報管理部37内の認証子検証情報に基づいて、各認証コンテキストAc1, Ac2内の認証子をそれぞれ検証し(ST19)、各認証子検証結果をコンテキスト検証部36に送出する。

[0099] また、コンテキスト検証部36では、第1及び第2認証コンテキストAc1, Ac2が認証要求に対応していることを確認するため、各認証コンテキストAc1, Ac2をチャレンジ情報検証部35に送出する。なお、チャレンジ情報検証部35への送出は、チャレンジ情報を含む各ヘッダブロックh1, h2のみとしてもよい。

[0100] チャレンジ情報検証部35は、チャレンジ保存部34内のチャレンジ情報に基づいて、各認証コンテキストAc1, Ac2のチャレンジ情報をそれぞれ検証し(ST20)、各チャレンジ情報検証結果をコンテキスト検証部36に返す。

[0101] さらに、コンテキスト検証部36は、各認証コンテキストAc1, Ac2のコンテキスト情報を検証する(ST21)。具体的には、コンテキスト検証部36は、コンテキスト情報内の

データブロックd1，d2に含まれる各認証構成プロセスP1，P2の実行結果を検証する。

[0102] ここで、コンテキスト検証部36は、ステップST19～ST21の各検証結果（認証子検証結果、チャレンジ情報検証結果、コンテキスト情報検証結果）に一つでも異常があるとき、各認証コンテキストAc1，Ac2に正当性が無いと判断し、処理を終了する（ST22）。

[0103] また、コンテキスト検証部36は、ステップST19～ST21の各検証結果の全てが正当のとき、各認証コンテキストAc1，Ac2に正当性があると判断し、処理を終了する（ST23）。なお、ステップST19～ST21の各検証処理は、互いに他の検証処理の結果を利用しないため、前述した順序に限らず、任意の順序で実行可能である。

[0104] 上述したように本実施形態によれば、検証装置30は、第1エンティティ装置10にチャレンジ情報を送信すると共に、このチャレンジ情報をチャレンジ保存部34に記憶し、折り返し受信した各認証コンテキストAc1，Ac2毎に、チャレンジ保存部34内のチャレンジ情報と同一のチャレンジ情報が記述されていることを検証することにより、各認証コンテキストAc1，Ac2が現在の認証コンテキストであることを確認できるので、過去の認証コンテキストを繰り返し用いる繰り返し攻撃を防ぎ、繰り返し攻撃に対して安全性を向上できる。

[0105] （第2の実施形態）

図7は本発明の第2の実施形態に係る認証システムの構成を示す模式図であり、図8は同システムの各エンティティ装置の構成を示す模式図であり、図9は同システムの検証装置の構成を示す模式図である。図7～図9については、各装置本体以外で前述した図面と同一部分には同一符号を付してその詳しい説明を省略し、前述した図面と異なる部分には異なる符号又はダッシュ符号（アポストロフィ符号）を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

[0106] すなわち、第2の実施形態は、第1の実施形態の変形例であり、検証装置30には通知せずに秘匿したい情報である秘匿実行内容を取り扱う認証システムを示している。

[0107] 秘匿実行内容としては、例えばバイオメトリクス認証における参照生体情報（テンプレート）や、実行時にセンサにより取得した生体情報などがある。参照生体情報は、生体認証に必須の情報であり、各エンティティ装置10，20間では共有する必要があるが、プライバシ保護の観点から検証装置30には通知されない方が望ましい情報である。

[0108] 第2エンティティ装置20は、図8の左側に示すように、前述した構成に加え、秘匿実行内容管理部26及びハッシュ値生成部27が付加されている。これに伴い、通信部21'、認証構成プロセスP2実行部22'及び認証コンテキスト生成部25'の処理内容が若干異なるものとなっている。

[0109] 通信部21'は、検証装置30から認証実行要求を受けると、認証構成プロセスP2実行部22'を起動する機能と、秘匿内容管理部26から受けた秘匿実行内容を第1エンティティ装置10に送信する機能と、認証コンテキスト生成部25'から受けた第2認証コンテキストを検証装置30に送信する機能とをもっている。なお、第2及び第1エンティティ装置20，10間の秘匿実行内容の通信は、図示しない別手段により確立された秘密通信路などを用いて外部から秘匿することが望ましい。

[0110] 認証構成プロセスP2実行部22'は、通信部21'に起動され、通信部21'から受ける認証実行要求及び秘匿内容管理部26から受ける秘匿実行内容に基づいて認証構成プロセスP2を実行し、実行結果を認証コンテキスト生成部25'に送出する機能をもっている。

[0111] 認証コンテキスト生成部25'は、認証子生成部24により生成された認証子と、認証構成プロセスP2実行部22'における第2ハッシュ値の対象（秘匿実行内容）以外の実行内容と、ハッシュ値生成部27から受ける第2ハッシュ値とを特定のフォーマットに従って記述して第2認証コンテキストを生成する機能と、この第2認証コンテキストを通信部21'に送出する機能とをもっている。ここで、認証子生成部24により生成された認証子は、秘密情報管理部23内の秘密情報2に基づいて、認証構成プロセスP2の実行内容及び第2ハッシュ値を対象として生成されたものである。

[0112] 秘匿内容管理部26は、秘匿実行内容を保持する機能と、認証構成プロセスP2実行部22'が起動されると、秘匿実行内容を通信部21'、認証構成プロセスP2実行部

22’及びハッシュ値生成部27に送出する機能をもっている。

[0113] ハッシュ値生成部27は、秘匿内容管理部26から秘匿実行内容（後段の認証構成プロセスP1にも入力され且つ検証装置30に対して秘匿する秘匿実行内容）を受けると、この秘匿実行内容を対象としたハッシュ値である第2ハッシュ値（前段側ハッシュ値）を生成する機能と、この第2ハッシュ値を認証コンテキスト生成部25’に送出する機能とをもっている。

[0114] 第1エンティティ装置10は、図8の右側に示すように、前述した構成に加え、ハッシュ値生成部17が付加されている。これに伴い、通信部11’、認証構成プロセスP1実行部12’及び認証コンテキスト生成部15’の処理内容が若干異なるものとなっている。

[0115] 通信部11’は、検証装置30からの認証実行要求と第2エンティティ装置20からの秘匿実行内容とを受けると、認証構成プロセスP1実行部12’を起動する機能と、起動した認証構成プロセスP1実行部12’に認証実行要求及び秘匿実行内容を送出すると共に、秘匿実行内容をハッシュ値生成部17に送出する機能と、認証コンテキスト生成部15’から受けた第1認証コンテキストを検証装置30に送信する機能とをもっている。

[0116] 認証構成プロセスP1実行部12’は、通信部11’に起動され、通信部11’から受ける認証実行要求及び秘匿実行内容に基づいて認証構成プロセスP1を実行し、実行結果を認証コンテキスト生成部15’に送出する機能をもっている。

[0117] 認証コンテキスト生成部15’は、認証子生成部14により生成された認証子と、認証構成プロセスP1実行部12’の実行内容と、ハッシュ値生成部17から受ける第1ハッシュ値とを特定のフォーマットに従って記述して第1認証コンテキストを生成する機能と、この第1認証コンテキストを通信部11’に送出する機能とをもっている。ここで、認証子生成部14により生成された認証子は、秘密情報管理部13内の秘密情報1に基づいて、認証構成プロセスP1の実行内容及び第1ハッシュ値を対象として生成されたものである。

[0118] ハッシュ値生成部17は、通信部11’から秘匿実行内容を受けると、この秘匿実行内容を対象としたハッシュ値である第1ハッシュ値（後段側ハッシュ値）を生成する機

能と、この第1ハッシュ値を認証コンテキスト生成部15'に送出する機能とをもっている。

[0119] 検証装置30は、図9に示すように、前述したチャレンジ情報に関する各部33～35を省略し、ハッシュ値比較部39を備えている。これに伴い、コンテキスト検証部36'の処理内容が若干異なるものとなっている。但し、チャレンジ情報に関する各部33～35は、省略せずに備えていてもよい。すなわち、前述したチャレンジ情報の検証と、本実施形態のハッシュ値の検証とは、別々に備える構成に限らず、同時に備える構成としてもよい。

[0120] 通信部31は、認証実行要求を第1及び第2エンティティ装置10，20に送信する機能と、第1及び第2エンティティ装置10，20から第1及び第2認証コンテキストを個別に受信する機能と、受信した各認証コンテキストをコンテキスト検証部36'に送出する機能とをもっている。

[0121] コンテキスト検証部36'は、認証子検出部38に各認証コンテキストを送出する機能と、認証子検証部38から認証子検証結果を受ける機能と、各認証コンテキストに個別に含まれる第1ハッシュ値及び第2ハッシュ値をハッシュ値比較部39に送出する機能と、ハッシュ値比較部39からハッシュ値比較検証結果を受ける機能と、認証子検証結果及びハッシュ値比較検証結果に基づいて、各認証コンテキストの正当性を検証する機能と、各認証コンテキスト内のデータブロックの情報に基づいて、各認証構成プロセスP1，P2の内容（実行環境、実行結果など）を確認する機能とをもっている。

[0122] ハッシュ値比較部39は、コンテキスト検証部36'から受けた第2ハッシュ値と第1ハッシュ値とが互いに同一であることを比較検証する機能と、得られたハッシュ値比較検証結果をコンテキスト検証部36'に返す機能とをもっている。

[0123] 次に、以上のように構成された認証システムの動作を説明する。

[0124] 始めに、検証装置30においては、通信部31が認証実行要求を第1及び第2エンティティ装置10，20に送信する。

[0125] 第2エンティティ装置20においては、通信部21'が認証実行要求を受けると、認証構成プロセスP2実行部22'を起動する。また、秘匿内容管理部26は、認証構成プロ

セスP2実行部22'が起動されると、秘匿実行内容を通信部21'、認証構成プロセスP2実行部22'及びハッシュ値生成部27に送出する。通信部21'は、受けた秘匿実行内容を第1エンティティ装置10に送信する。

[0126] 一方、認証構成プロセスP2実行部22'は、起動されると、通信部21'から受ける認証実行要求及び秘匿内容管理部26から受ける秘匿実行内容に基づいて認証構成プロセスP2を実行し、実行結果を認証コンテキスト生成部25'に送出する。

[0127] ここで、認証構成プロセスP2実行部22'の実行結果を秘匿実行内容としても良い。例えば、外部のセンサにより取得された生体情報などを秘匿実行内容とするような場合である。

[0128] この場合、通信部21'から受ける認証実行要求に応じて、認証構成プロセスP2実行部22'の実行結果を秘匿内容管理部22に送出する。秘匿内容管理部22は、認証構成プロセスP22実行部22'より受け取った実行結果を秘匿実行内容として保持し、通信部21'及びハッシュ値生成部27に対して当該秘匿実行内容を送信する。

[0129] この場合、秘匿内容管理部26に秘匿実行内容が予め保持されている場合には、秘匿内容管理部26は、この予め保持している秘匿実行内容と、認証構成プロセスP22実行部22'より受け取った実行内容をあわせた秘匿実行内容を通信部21'及びハッシュ値生成部27に送出することが望ましい。または、それぞれ別に送信して、ハッシュ値生成部27の側で合わせてもよい。

[0130] また、ハッシュ値生成部27は、秘匿内容管理部26から秘匿実行内容を受けると、この秘匿実行内容を対象としたハッシュ値である第2ハッシュ値を生成し、この第2ハッシュ値を認証コンテキスト生成部25'に送出する。

[0131] 認証コンテキスト生成部25'は、認証子生成部24により生成された認証子と、認証構成プロセスP2実行部22'における秘匿実行内容以外の実行内容と、ハッシュ値生成部27から受けた第2ハッシュ値とを特定のフォーマットに従って記述して第2認証コンテキストを生成し、この第2認証コンテキストを通信部21'に送出する。

[0132] 通信部21'は、この第2認証コンテキストを検証装置30に送信する。

[0133] 一方、第1エンティティ装置10においては、通信部11'が、検証装置30からの認証実行要求と第2エンティティ装置20からの秘匿実行内容とを受けると、認証構成プロ

セスP1実行部12'を起動し、この認証構成プロセスP1実行部12'に認証実行要求及び秘匿実行内容を送出すると共に、秘匿実行内容をハッシュ値生成部17に送出する。

[0134] ここで、検証装置30は第1エンティティ装置10と第2エンティティ装置の各々に認証実行要求を送信せずに、図示しない認証実行制御装置に認証実行要求を送信し、この認証実行制御装置が第1エンティティ装置10と第2エンティティ装置の各々に認証実行要求を送信しても良い。

[0135] この場合、認証実行制御装置において予めいずれのエンティティ装置に認証実行要求を送信するかが決まっていれば、検証装置30はエンティティ装置を指定することなく認証実行要求を認証実行制御装置に送っても良い。

[0136] また、第1エンティティ装置10及び第2エンティティ装置20の各々が生成した第1認証コンテキスト及び第2認証コンテキストは、直接検証装置30へ送信せずに、認証実行制御装置へ送信し、認証実行制御装置がそれらをまとめて検証装置30へ送信してもよい。

[0137] 認証構成プロセスP1実行部12'は、通信部11'から受ける認証実行要求及び秘匿実行内容に基づいて認証構成プロセスP1を実行し、実行結果を認証コンテキスト生成部15'に送出する。

[0138] ハッシュ値生成部17は、通信部11'から秘匿実行内容を受けると、この秘匿実行内容を対象としたハッシュ値である第1ハッシュ値を生成し、この第1ハッシュ値を認証コンテキスト生成部15'に送出する。

[0139] 認証コンテキスト生成部15'は、認証子生成部14により生成された認証子と、認証構成プロセスP1実行部12'の実行内容と、ハッシュ値生成部17から受ける第1ハッシュ値とを特定のフォーマットに従って記述して第1認証コンテキストを生成し、この第1認証コンテキストを通信部11'に送出する。

[0140] 通信部11'は、この第1認証コンテキストを検証装置30に送信する。

[0141] 検証装置30においては、通信部31が第1及び第2認証コンテキストを個別に受信し、各認証コンテキストをコンテキスト検証部36'に送出する。

[0142] コンテキスト検証部36'は、認証子検出部38に各認証コンテキストを送出し、認証

子検証部38から認証子検証結果を受ける。

[0143] また、コンテキスト検証部36'は、各認証コンテキストに個別に含まれる第1ハッシュ値及び第2ハッシュ値をハッシュ値比較部39に送出する。ハッシュ値比較部39は、第1及び第2ハッシュ値とが互いに同一であることを比較検証し、得られたハッシュ値比較検証結果をコンテキスト検証部36'に返す。

[0144] これにより、コンテキスト検証部36'は、認証子検証結果及びハッシュ値比較検証結果に基づいて、各認証コンテキストの正当性を検証する。また、コンテキスト検証部36'は、各認証コンテキスト内のデータブロックの情報に基づいて、各認証構成プロセスP1，P2の内容（実行環境、実行結果など）を確認する。

[0145] 上述したように本実施形態によれば、検証装置30が、各認証コンテキストAc1，Ac2に含まれるハッシュ値が互いに同一であることを検証することにより、前段の認証構成プロセスP1の秘匿実行内容と後段の認証構成プロセスP2の秘匿実行内容とが同一であることを確認できるので、秘匿情報のすり替え攻撃に対して安全性を向上できる。これにより、例えばバイオメトリクス本人確認における生体情報の「すり替え」を防ぎ、安全性を向上できる。

[0146] また、本実施形態は第1エンティティ装置10および第2エンティティ装置20の2つのエンティティ装置によって構成されているが、さらに多くのエンティティ装置により構成されていても良い。この場合、各々のエンティティ装置は第1エンティティ装置10または第2エンティティ装置20と同じ構成か、第1エンティティ装置10と第2エンティティ装置20両方の機能をあわせ持った構成でも良い。この場合、同じ機能を実行する機能部は1つの機能部で実行しても良い。

[0147] （第3の実施形態）

図10は本発明の第3の実施形態に係る認証システムの構成を示す模式図である。ここでは、特に、バイオメトリクス認証を用いた認証システムの一例を示す。

[0148] 本実施形態は、認証構成プロセスP2の実行結果に基づいて、認証構成プロセスP1の実行結果が得られる場合の認証システムの一例である。

[0149] この認証システムは、第1エンティティ装置10、第2エンティティ装置20及び検証装置30の三者の間に、認証要求装置40を備えている。詳しくは、認証を開始する際に

、検証装置30が認証要求装置40に対し、チャレンジ情報と、検証装置30が受入可能な実行環境を規定したプロファイルを纏めたプロファイルリストを送信する。認証要求装置40は、このプロファイルリストと各装置10，20の機能リストとの両者を満たすように実行プロファイルを決定し、この実行プロファイルに沿って各装置10，20に認証を実行させる。認証要求装置40は、得られた第1及び第2認証コンテキストと当該実行プロファイルとを検証装置40に返信する。すなわち、この認証システムは、認証要求装置40を備えた構成により、検証装置30に対し、各装置10，20の機能リストを秘匿できるものである。

[0150] ここで、認証要求装置40は、図11に示すように、通信部41及び制御部42を備えている。制御部42は、通信制御部43及びプロファイル決定部44を備えている。

[0151] 通信部41は、各装置10，20，30と、通信制御部43との間の通信インターフェイスである。以下の説明中では、記載の簡略化のため、各装置10，20，30と、通信制御部43との間の通信に通信部41を介在させる旨の記載を省略する。

[0152] 通信制御部43は、認証要求を検証装置30に送信する機能と、検証装置30からチャレンジ情報及びプロファイルリストを受信する機能と、このプロファイルリストをプロファイル決定部44に送出する機能と、第1及び第2エンティティ装置10，20に個別に機能リスト要求を送信する機能と、各エンティティ装置10，20から個別に機能リストを受信する機能と、この機能リストをプロファイル決定部44に送出する機能と、プロファイル決定部44から受けた実行プロファイルと共に、認証実行要求及び前述した検証装置30からのチャレンジ情報を第2エンティティ装置20に送信する機能と、第2エンティティ装置20から第2認証コンテキストを受信する機能と、この第2認証コンテキストと共に、認証実行要求及び前述したチャレンジ情報及び実行プロファイルを第1エンティティ装置10に送信する機能と、第1エンティティ装置10から第1認証コンテキストを受信する機能と、第1及び第2認証コンテキスト並びに実行プロファイルを検証装置30に送信する機能とをもっている。

[0153] なお、機能リスト要求は、認証処理を行う毎に送信してもよいし、認証要求装置40の初期化の際に送信してもよい。初期化の際に送信した場合、得られた機能リストは認証要求装置40内に保存される。

[0154] プロファイル決定部44は、通信制御部43から受けたプロファイルリスト及び機能リストの両者を満たすように、認証に使用する実行プロファイルを決定する機能と、この実行プロファイルを通信制御部43に送出する機能とをもっている。

[0155] ここで、プロファイルリストは、検証装置30が受け入れ可能なエンティティ装置10，20のプロファイル（実行環境）の情報が記載されたもの（情報）であり、例えば図12に示すように、リスト形式でハッシュ値計算アルゴリズムの候補や、認証子計算アルゴリズムの候補等が列挙されている。なお、プロファイルリストは、必ずしもリスト形式である必要はない。例えば、プロファイルリストは、受け入れ可能なプロファイルの情報が（改行無しに）羅列される形式（文章形式）で記載された情報でもよく、表形式（広義のリスト形式）にて記載された情報でもよい。すなわち、プロファイルリストとは、検証装置30の受け入れ可能なプロファイルの情報が記載された情報を意味しており、記載形式には限定されない。

[0156] 機能リストは、各エンティティ装置10，20において、認証構成プロセスを実行する機能（実行環境）を規定したものである。

[0157] 実行プロファイルは、プロファイルリスト及び各機能リストを満たすように決定（又は選択）され且つ認証時に実行されるプロファイルであり、例えば図13に示すように、ハッシュ値計算アルゴリズムや認証子計算アルゴリズムが記載されている。

[0158] 第1及び第2エンティティ装置10，20は、図14に示すように、前述した構成において、認証コンテキスト検証部16が付加され、機能リスト格納部18，28が明記されている。これに伴い、各通信部11”，21”は、認証要求装置40から受けた機能リスト要求に対して機能リスト格納部18，28内の機能リストを返信し、認証実行要求、チャレンジ情報及び実行プロファイルに対しては認証コンテキストを返信する機能を有する。なお、チャレンジ情報は、機能リストを秘匿する観点からは省略可能であるが、ここでは用いる例を述べる。

[0159] また、認証構成プロセスP2実行部22”は、生体情報入力処理機能22－1及び信号処理機能22－2を備えている。認証構成プロセスP1実行部12”は、参照生体情報格納部12－1及び照合処理機能12－2を備えている。

[0160] ここで、認証構成プロセスP2実行部22”は、通信部21”から認証実行要求及び実

行プロファイルを受けると、実行プロファイルに基づいて、生体情報入力処理機能22－1及び信号処理機能22－2を実行し、実行結果を認証コンテキスト生成部25に送出するものである。

[0161] 生体情報入力処理機能22－1は、入力される生体情報に基づいて入力生体情報を生成し、この入力生体情報を信号処理機能22－2に送出する機能である。信号処理機能22－2は、生体情報入力処理機能22－1から受けた入力生体情報に基づいてサンプル生体情報を生成し、このサンプル生体情報からなる実行結果を認証コンテキスト生成部25に送出する機能である。

[0162] 認証構成プロセスP1実行部12”は、通信部11”から認証実行要求、実行プロファイルを受け、且つ認証コンテキスト検証部16から第2認証コンテキストを受けると、実行プロファイル及び第2認証コンテキストに基づいて、参照生体情報格納部12－1を参照しながら照合処理機能12－2を実行し、実行結果を認証コンテキスト生成部15に送出するものである。

[0163] 参照生体情報格納部12－1は、予め参照生体情報が格納されるメモリであり、照合処理機能12－2から参照可能となっている。

[0164] 照合処理機能12－2は、参照生体情報格納部12－1内の参照生体情報と、第2認証コンテキスト内のサンプル生体情報とを照合する照合処理を実行し、照合結果を示す実行結果を認証コンテキスト生成部15に送出する機能である。

[0165] 認証コンテキスト検証部16は、通信部11”から受けた第2認証コンテキストを秘密情報管理部10内の秘密情報1に基づいて検証し、検証結果が正当のとき、この第2認証コンテキストを認証構成プロセスP1実行部12”に送出するものである。

[0166] 次に、以上のように構成された認証システムの動作を図15のシーケンス図を用いて説明する。ここでは、第2エンティティ装置20の認証構成プロセスP2実行部22が、生体データ収集及び信号処理を行い、第1エンティティ装置10の認証構成プロセスP1実行部12が参照生体情報（テンプレート）保持と照合処理を行う場合について述べる。

[0167] 検証装置30は、第1及び第2認証コンテキストの構成データについて、受け入れるプロファイルを予めまとめたプロファイルリストを保存している（ST30）。

[0168] 認証要求装置は、検証装置30に生体認証の認証要求を送信する(ST31)。

[0169] 検証装置30は、認証要求を受けると、チャレンジ情報とプロファイルリストを認証要求装置40に送信する(ST32)。

[0170] 認証要求装置40は、チャレンジ情報及びプロファイルリストを受信し、第1及び第2エンティティ装置10, 20に個別に機能リストを要求する(ST33)。

[0171] 第1及び第2エンティティ装置10, 20は、それぞれ機能リスト格納部18, 28から読み出した機能リストを認証要求装置40に送信する(ST34)。

[0172] 認証要求装置40においては、通信制御部43が、各エンティティ装置10, 20から受信した各機能リストと、検証装置30から受信したプロファイルリストとをプロファイル決定部44に送出する。

[0173] プロファイル決定部44は、各機能リストとプロファイルリストとを比較し、3つのリストを満たすように実行プロファイルを決定し(ST35)、実行プロファイルを通信制御部43に送出する。

[0174] 認証要求装置40は、通信制御部43により、認証実行要求、チャレンジ情報及び実行プロファイルを第2エンティティ装置20に送信する(ST36)。なお、実行プロファイルが決定できなかった場合には、認証要求装置40は、認証不可のメッセージを検証装置に返す(ST36')。

[0175] 第2エンティティ装置20は、認証実行要求、チャレンジ情報、実行プロファイルを受けると、認証構成プロセスP2(生体情報入力処理と信号処理)を実行する。このとき、認証構成プロセスP2実行部12"は、実行プロファイルに従ってサンプル生体情報を生成し、このサンプル生体情報からなる実行結果を認証コンテキスト生成部15に送出する。

[0176] 認証コンテキスト生成部15は、実行プロファイルに従って認証子生成部14により認証子を生成し、この認証子、チャレンジ情報及び実行結果を含む第2認証コンテキストを生成する(ST37)。

[0177] 第2エンティティ装置20は、得られた第2認証コンテキストを認証要求装置40に送信する(ST38)。

[0178] 認証要求装置40は、第2認証コンテキスト、認証実行要求、チャレンジ情報及び実

行プロファイルを第1エンティティ装置10に送信する(ST39)。

[0179] 第1エンティティ装置10においては、認証コンテキスト検証部16により、第2認証コンテキストの完全性を検証する。しかる後、認証構成プロセスP1実行部12”は、実行プロファイルに従って、第2認証コンテキスト内のサンプル生体情報と、参照情報格納部12－1内の参照生体情報とを照合する照合処理を実行し、その実行結果を認証コンテキスト生成部15に送出する。認証コンテキスト生成部15は、実行プロファイルに従って認証子生成部14により認証子を生成し、この認証子、チャレンジ情報及び実行結果を含む第1認証コンテキストを生成する(ST40)。

[0180] 第1エンティティ装置10は、この第1認証コンテキストを認証要求装置40に送信する(ST41)。

[0181] 認証要求装置40は、第1及び第2認証コンテキスト並びに実行プロファイルを検証装置30に送信する(ST42)。

[0182] 検証装置30は、受信した各認証コンテキストを検証する(ST43)。

[0183] 具体的には例えば、検証装置30は、各認証コンテキスト内の認証子に基づいて、各認証コンテキストの完全性を検証する。これに加え、検証装置30は、サンプル生体情報の認証子、参照生体情報の認証子を確認することにより、それぞれの生体情報が改竄されずに認証処理が行われたことを確認する構成にしてもよい。この場合、各生体情報及びその認証子は、それぞれのエンティティ装置10，20が各認証コンテキストに含めるようにすればよい。

[0184] また、検証装置30は、各認証コンテキスト内のチャレンジ情報がステップST32で送信した値と一致することを確認し、繰り返し攻撃がされていないことを確認する。

[0185] 最後に、検証装置30は、認証コンテキストに含まれている情報、実行プロファイル、プロファイルリストを比較し、最終的な認証の可否を判断する。これにより、検証装置30は、ステップST43の検証処理を終了する。

[0186] このとき、実行プロファイルの内容を比較の対象から外してもよい。なぜなら、実行プロファイルの内容は認証コンテキストにも含まれているので、これを外したとしても、発明の効果を損なわないからである。

[0187] 上述したように本実施形態によれば、検証装置30の受け入れ可能な実行環境を示

すプロファイルリストと、各認証エンティティ装置10，20の機能リストとの両者を満たすように、各認証エンティティ装置10，20の実行環境を示す実行プロファイルを認証要求装置40が決定することにより、認証の実行に関係しない各エンティティ装置10，20の様々な実行環境を検証装置30から秘匿できるので、各認証エンティティ装置10，20側の要求者のプライバシを保つことができる。

[0188] なお、本実施形態は、チャレンジ情報を用いる第1の実施形態に限らず、図10及び図16に示すように、ハッシュ値を用いる第2の実施形態に適用しても同様の作用効果を得ることができる。なお、図16に示す変形例の場合、秘匿実行内容は、第2エンティティ装置20から認証要求装置40を介して第1エンティティ装置10に送信されている。

[0189] （第4の実施形態）

図17は本発明の第4の実施形態に係る認証システムの構成を示す模式図である。

[0190] 第1～第3の実施形態においては、検証装置30が認証コンテキストを検証する際、例えばデータブロックd1，d2内の静的情報（認証を行う都度、変化しない情報）を参照する必要がある場合がある。しかし、静的情報を、認証を行う都度、認証コンテキストに記述して送信するのは通信量の観点から効率が低い。

[0191] 本実施形態では、第3の実施形態に適用した例を代表例とし、認証コンテキストに静的情報を記述する代わりに、静的情報のリンク先を表すリンク先情報（例、URL(Uniform Resource Locator)、URN(Uniform Resource Name)又はURI(Uniform Resource Identifier)等の識別情報）を認証コンテキストに記述することにより、通信量の低減を図っている。なお、言うまでもないが、リンク先情報は、静的情報のデータ量よりも小さいデータ量からなるリンク先が記述されている。

[0192] リンク先としては、例えば静的情報が各エンティティ装置10，20に関する情報の場合、各エンティティ装置10，20の作成メーカや公正な第三者機関が管理する静的情報管理サーバ50などを備えている。

[0193] この静的情報管理サーバ50は、外部から受信した静的情報の要求に応じて静的情報記憶部52内の静的情報を要求元に返信する通信部51と、この通信部51から読出可能に静的情報が記憶された静的情報記憶部52とを備えている。

[0194] なお、静的情報が参照生体情報(テンプレート)に関する情報の場合、図示しないが、生体情報の登録機関のサーバや公的な評価機関のサーバなどをリンク先としてもよい。

[0195] また、リンク先としてはサーバに限らない。例えば、静的情報を対象に信頼できる機関により発行された証明書を特定可能な情報をリンク先情報としてもよい。例えばテンプレートに関する評価情報の場合、テンプレートのハッシュ値と評価情報を対象に登録機関などにより発行されたテンプレート証明書を特定可能な情報、例えば発行者名とシリアル番号などをリンク先情報としてもよい。この場合のテンプレート証明書Ctの例を図18に示す。

[0196] このテンプレート証明書Ctは、基本領域及び署名領域から構成されている。

基本領域は、各項目(及びその内容)として、バージョン(証明書形式のバージョン)、シリアル番号(証明書のシリアル番号)、署名アルゴリズム(発行者署名の署名アルゴリズム)、有効期限(テンプレートの有効期限)、発行者名(証明書の発行者名情報)、ハッシュアルゴリズム(テンプレートダイジェストのハッシュアルゴリズム)、テンプレートダイジェスト(テンプレートのハッシュ値)、テンプレート評価結果(テンプレートの評価結果)、テンプレート評価基準(テンプレートの評価基準)、などを備えている。

[0197] 署名領域は、各項目(及びその内容)として、発行者署名(基本領域を対象とした、発行者のデジタル署名)を備えている。

[0198] 次に、第1及び第2エンティティ装置10, 20は、図19に示すように、前述した構成に加え、静的情報へのリンク先情報を格納した静的情報リンク先管理部19, 29を備えている。これに伴い、認証コンテキスト生成部15"', 25"'は、認証構成プロセスP1, P2実行部12", 22"の実行結果の他に、静的情報に代えてリンク先情報を含む第1又は第2認証コンテキストを生成する。

[0199] この第1及び第2認証コンテキストAc1, Ac2の例を図20A及び図20Bに示す。この例では、データブロックd1"', d2"'内に、静的情報へのリンク先情報dLiと、エンティティ情報dEnとが格納されている。リンク先情報dLiには、例えばエンティティの評価レポートや、エンティティの精度情報、照合処理に用いたテンプレートの証明書などの静的情報へのリンク先が示されている。なお、認証毎に異なる情報は、エンティティ

情報（実行結果等）に格納されている。エンティティ情報dEnとしては、例えばサンプル生体情報の品質、照合の一致度などである。

[0200] 次に、以上のように構成された認証システムの動作を説明する。

[0201] 検証装置30は、第3の実施形態と同様にして、認証要求装置40から第1及び第2認証コンテキスト並びに実行プロファイルを受信したとする。

[0202] 検証装置30は、前述同様に、各認証コンテキストを検証し、必要に応じて各認証コンテキスト内の静的情報リンク先情報に基づき、例えば静的情報管理サーバ50に静的情報の要求を送信する。

[0203] 静的情報管理サーバ50は、静的情報の要求を通信部51が受信すると、この静的情報の要求に基づいて、静的情報記憶部52内の該当する静的情報を通信部51から検証装置30に返信する。

[0204] 検証装置30は、受信した静的情報に基づいて各認証コンテキストの検証を継続し、最終的に認証の可否を判断する。なお、検証装置30は、リンク先へのアクセス速度を向上させるために、過去に受信した静的情報をキャッシュメモリ（図示せず）に保存してもよい。

[0205] 上述したように本実施形態によれば、各エンティティ装置10，20が、認証毎に同一内容を表す静的情報に関し、静的情報に代えて静的情報のデータ量よりも小さいデータ量からなり静的情報を取得するリンク先情報を含むように認証コンテキストAc1，Ac2を生成するので、認証コンテキストのサイズが小さくなることから、認証要求装置40と検証装置30間の通信量を低減でき、認証コンテキストの通信効率を向上できる。

[0206] なお、本実施形態は、認証要求装置40を用いる第3の実施形態に限らず、図21及び図22に示すように、認証要求装置40の無い第1又は第2の実施形態に適用しても同様の作用効果を得ることができる。なお、この変形例の場合も同様に、各エンティティ装置10，20は、それぞれ静的情報リンク先管理部19，29を有し、認証コンテキスト生成部15，25が、静的情報に代えてリンク先情報を含めるように各認証コンテキストを生成することは言うまでもない。

[0207] なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプロ

グラムとして、磁気ディスク(フロッピー(登録商標)ディスク、ハードディスクなど)、光ディスク(CD−ROM、DVDなど)、光磁気ディスク(MO)、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0208] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0209] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW(ミドルウェア)等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0210] さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0211] また、記憶媒体は1つに限らず、複数の媒体から上記実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0212] 尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0213] また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0214] なお、本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

産業上の利用可能性

[0215] 以上説明したように本発明の認証システム、装置及びプログラムによれば、過去の

認証コンテキストを繰り返し用いる繰り返し攻撃に対して安全性を向上できる。また、秘匿情報のすり替え攻撃に対して安全性を向上できる。さらに、要求者の様々な実行環境を検証者から秘匿できる。また、認証コンテキストの通信効率を向上できる。

請求の範囲

[1] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置(10, 20)と、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)とを備えた認証システムであって、

前記各認証エンティティ装置は、

前記検証装置により生成されたチャレンジ情報を受信するチャレンジ情報受信手段(11, 21)と、

前記検証のための秘密情報が記憶された秘密情報記憶手段(13, 23)と、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子を生成する認証子生成手段(14, 24)と、

前記認証子と前記実行内容及び前記チャレンジ情報とを特定のフォーマットに従って記述した認証コンテキストを生成する認証コンテキスト生成手段(15, 25)と、

前記認証コンテキストを送信する認証コンテキスト送信手段(11, 21)とを備えており、

前記検証装置は、

前記秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段(37)と、

前記チャレンジ情報を生成するチャレンジ生成手段(33)と、

このチャレンジ情報が記憶されるチャレンジ記憶手段(34)と、

前記チャレンジ情報を送信するチャレンジ情報送信手段(31)と、

前記各認証エンティティ装置により生成された各認証コンテキストを受信する認証コンテキスト受信手段(31)と、

前記受信した各認証コンテキスト毎に、前記チャレンジ記憶手段内のチャレンジ情報と同一のチャレンジ情報が記述されているか否かを検証するチャレンジ検証手段(35)と、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)と、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を

検証する認証コンテキスト検証手段(36)と

を備えたことを特徴とする認証システム。

[2] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置と、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)とを備えた認証システムであって、

前記各認証エンティティ装置は、少なくとも1台の前段側の認証エンティティ装置(20)及び少なくとも1台の後段側の認証エンティティ装置(10)を備えており、

前記前段側の認証エンティティ装置は、

前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値を生成する前段側ハッシュ値生成手段(27)と、

前記検証のための秘密情報が記憶された前段側秘密情報記憶手段(23)と、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子を生成する前段側認証子生成手段(24)と、

前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とを特定のフォーマットに従って記述した認証コンテキストを生成する前段側認証コンテキスト生成手段(25')と、

前記認証コンテキスト及び前記秘匿実行内容を送信する前段側送信手段(21')とを備えており、

前記後段側の認証エンティティ装置は、

前記送信された秘匿実行内容を受信する秘匿実行内容受信手段(11')と、

前記受信した秘匿実行内容を対象とした後段側ハッシュ値を生成する後段側ハッシュ値生成手段(17)と、

前記検証のための秘密情報が記憶された後段側秘密情報記憶手段(13)と、

この秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象とした認証子を生成する後段側認証子生成手段(14)と、

前記認証子、前記実行内容及び前記後段側ハッシュ値を特定のフォーマットに従って記述した認証コンテキストを生成する後段側認証コンテキスト生成手段(15')と、

この認証コンテキストを送信する後段側送信手段(11')とを備えており、

前記検証装置は、

前記各秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段(37)と、

前記各認証エンティティ装置により生成された各認証コンテキストを受信する認証コンテキスト受信手段(31)と、

前記受信した各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることを比較検証するハッシュ値比較検証手段(39)と、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)と、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段(36')と

を備えたことを特徴とする認証システム。

[3] 請求項1又は請求項2に記載の認証システムにおいて、

前記検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置(40)を備え、

前記検証装置は、

前記認証構成プロセスの実行に関し、受け入れ可能な実行環境を規定したプロファイルリストを生成するプロファイルリスト生成手段と、

前記プロファイルリストを認証要求装置へ送信するリスト送信手段(31)とを備えており、

前記認証要求装置は、

前記プロファイルリストを受信するプロファイルリスト受信手段(41)と、

認証構成プロセスを実行する機能を規定した機能リストを前記各認証エンティティ装置毎に受信する機能リスト受信手段(41)と、

前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するプロファイル決定手段(44)と、

前記実行プロファイルを各認証エンティティ装置に送信する実行プロファイル送信

手段(41)とを備えており、

前記各認証エンティティ装置は、

前記認証要求装置から前記実行プロファイルを受信する実行プロファイル受信手段(11", 21")と、

この実行プロファイルに基づいて、前記認証構成プロセスを実行する認証構成プロセス実行手段(12", 22")と

を備えたことを特徴とする認証システム。

[4] 請求項1乃至請求項3のいずれか1項に記載の認証システムにおいて、

前記各認証エンティティ装置(10, 20)は、

認証毎に同一内容を表す静的情報に関し、前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報が記憶されるリンク先情報記憶手段(19, 29)を備えており、

前記認証コンテキスト生成手段は、前記静的情報に代えて前記リンク先情報を含むように前記認証コンテキストを生成しており、

前記検証装置(30)は、

受信した認証コンテキスト内のリンク先情報に基づいて、静的情報を取得する手段と、

この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理を検証する検証手段と

を備えたことを特徴とする認証システム。

[5] 認証処理を検証するための検証装置(30)に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する各認証エンティティ装置(10, 20)であって、

前記検証装置により生成されたチャレンジ情報を受信する受信手段(11, 21)と、

前記検証のための秘密情報が記憶された秘密情報記憶手段(13, 23)と、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子を生成する認証子生成手段(14, 24)と、

前記認証子と前記実行内容及び前記チャレンジ情報とを特定のフォーマットに従っ

て記述した認証コンテキストを生成する認証コンテキスト生成手段(15, 25)と、

前記認証コンテキストを前記検証装置に送信する認証コンテキスト送信手段(11, 21)とを備えており、

前記認証コンテキストは、

前記検証装置により、当該検証装置が生成したチャレンジ情報と同一のチャレンジ情報が記述されているか否かが検証され、前記検証装置により、前記秘密情報に対応する認証子検証情報に基づいて、認証子が検証され、当該各検証結果に基づいて正当性が検証されるものであることを特徴とする認証エンティティ装置。

[6] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置(10, 20)に通信可能であり、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)であって、

前記各認証エンティティ装置に記憶された秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段(37)と、

前記チャレンジ情報を生成するチャレンジ生成手段(33)と、

このチャレンジ情報が記憶されるチャレンジ記憶手段(34)と、

前記チャレンジ情報を送信するチャレンジ情報送信手段(31)と、

前記各認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子が生成され、この認証子と前記実行内容及び前記チャレンジ情報とが特定のフォーマットに従って記述されて各認証コンテキストが生成された後、前記各認証エンティティ装置から送信された各認証コンテキストを受信する認証コンテキスト受信手段(31)と、

前記受信した各認証コンテキスト毎に、前記チャレンジ記憶手段内のチャレンジ情報と同一のチャレンジ情報が記述されているか否かを検証するチャレンジ検証手段(35)と、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)と、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段(36)と

を備えたことを特徴とする検証装置。

[7] 認証処理を検証するための検証装置に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置のうち、少なくとも1台の後段側の認証エンティティ装置(10)にも通信可能な少なくとも1台の前段側の認証エンティティ装置(20)であって、

前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値を生成する前段側ハッシュ値生成手段(27)と、

前記検証のための秘密情報が記憶された前段側秘密情報記憶手段(23)と、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子を生成する前段側認証子生成手段(24)と、

前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とを特定のフォーマットに従って記述した前段側の認証コンテキストを生成する前段側認証コンテキスト生成手段(25')と、

前記認証コンテキスト及び前記秘匿実行内容を送信する前段側送信手段(21')とを備えており、

前記秘匿実行内容は、前記後段側の認証エンティティ装置により受信されて当該秘匿実行内容を対象とした後段側ハッシュ値に変換されるものであり、

前記後段側ハッシュ値は、前記後段側の認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容と共に当該後段側ハッシュ値を対象とした認証子に変換される一方、この認証子及び当該実行内容と共に特定のフォーマットに従って後段側の認証コンテキストに記述され、この後段側の認証コンテキストと共に送信されるものであり、

前記各認証コンテキストは、

前記検証装置により、それぞれ受信されて当該各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることが比較検証され、前記秘密情報に対応する認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子が検証され、当該各検証結果に基づいて、正当性が検証されるものであることを特

徴とする前段側の認証エンティティ装置。

[8] 認証処理を検証するための検証装置に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置のうち、少なくとも1台の前段側の認証エンティティ装置(20)にも通信可能な少なくとも1台の後段側の認証エンティティ装置(10)であって、

前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を前記前段側の認証エンティティ装置から受信する秘匿実行内容受信手段(11')と、

前記受信した秘匿実行内容を対象とした後段側ハッシュ値を生成する後段側ハッシュ値生成手段(17)と、

前記検証のための秘密情報が記憶された後段側秘密情報記憶手段(13)と、

この秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象とした認証子を生成する後段側認証子生成手段(14)と、

前記認証子、前記実行内容及び前記後段側ハッシュ値を特定のフォーマットに従って記述した認証コンテキストを生成する後段側認証コンテキスト生成手段(15')と、

この認証コンテキストを送信する後段側送信手段(11')とを備えており、

前記秘匿実行内容は、前記前段側の認証エンティティ装置から送信される前に、当該前段側の認証エンティティ装置により当該秘匿実行内容を対象とした前段側ハッシュ値に変換されるものでもあり、

前記前段側ハッシュ値は、前記前段側の認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容と共に当該前段側ハッシュ値を対象とした認証子に変換される一方、この認証子及び当該実行内容と共に特定のフォーマットに従って前段側の認証コンテキストに記述され、この前段側の認証コンテキストと共に送信されるものであり、

前記各認証コンテキストは、

前記検証装置により、それぞれ受信されて当該各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることが比較検証され、前記秘密情報に対応する認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証

子が検証され、当該各検証結果に基づいて、正当性が検証されるものであることを特徴とする後段側の認証エンティティ装置。

[9] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置に通信可能であり、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)であって、

前記各認証エンティティ装置に記憶された秘密情報に対応する認証子検証情報が記憶された検証情報記憶手段(37)と、

前記各認証エンティティ装置のうち、少なくとも1台の前段側の認証エンティティ装置により、前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値が生成され、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子が生成され、前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とが特定のフォーマットに従って記述されて前段側の認証コンテキストが生成された後、前記前段側の認証エンティティ装置から送信された前段側の認証コンテキストを受信する第1の認証コンテキスト受信手段(31)と、

前記各認証エンティティ装置のうち、少なくとも1台の後段側の認証エンティティ装置により、前記前段側の認証エンティティ装置から送信された秘匿実行内容が受信され、この秘匿実行内容を対象とした後段側ハッシュ値が生成され、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象とした認証子が生成され、この認証子、当該実行内容及び前記後段側ハッシュ値が特定のフォーマットに従って記述されて後段側の認証コンテキストが生成された後、前記後段側の認証エンティティ装置から送信された後段側の認証コンテキストを受信する第2の認証コンテキスト受信手段(31)と、

前記受信した各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることを比較検証するハッシュ値比較検証手段(39)と、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)と、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段（36’）と

を備えたことを特徴とする検証装置。

[10] 請求項6又は請求項9に記載の検証装置において、

前記認証構成プロセスの実行に関し、受け入れ可能な実行環境を規定したプロファイルリストを生成するプロファイルリスト生成手段と、

前記プロファイルリストを送信するリスト送信手段（31）とを備えており、

前記プロファイルリストは、

前記検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置に受信され、当該認証要求装置により、前記各認証エンティティ装置毎に取得された、認証構成プロセスを実行する機能を規定した機能リストと比較されるものであり、

この比較は、

前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するための処理であり、

前記実行プロファイルは、

前記各認証エンティティ装置に送信され、前記認証構成プロセスを実行する実行環境を規定したものであることを特徴とする検証装置。

[11] 請求項10に記載の検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置（40）において、

前記検証装置からプロファイルリストを受信するプロファイルリスト受信手段（41）と、

認証構成プロセスを実行する機能を規定した機能リストを前記各認証エンティティ装置毎に受信する機能リスト受信手段（41）と、

前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するプロファイル決定手段（44）と、

前記実行プロファイルを各認証エンティティ装置に送信する実行プロファイル送信手段（41）と

を備えたことを特徴とする認証要求装置。

[12] 請求項5、請求項7又は請求項8に記載の認証エンティティ装置において、

認証毎に同一内容を表す静的情報に関し、前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報が記憶されるリンク先情報記憶手段(19, 29)を備えており、

前記認証コンテキスト生成手段は、前記静的情報に代えて前記リンク先情報を含むように前記認証コンテキストを生成しており、

この認証コンテキストは、

前記検証装置により受信され、当該認証コンテキスト内のリンク先情報に基づいて、静的情報が取得され、この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理が検証されるものであることを特徴とする認証エンティティ装置。

[13] 請求項6、請求項9又は請求項10に記載の検証装置において、

前記各認証コンテキストが、認証毎に同一内容を表す静的情報に関し、前記静的情報に代えて前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報を含むとき、前記認証コンテキスト受信手段により受信した認証コンテキスト内のリンク先情報に基づいて、静的情報を取得する手段と、

この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理を検証する検証手段と

を備えたことを特徴とする検証装置。

[14] 認証処理を検証するための検証装置(30)に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する各認証エンティティ装置(10, 20)に関し、当該各認証エンティティ装置のコンピュータに用いられるプログラムであって、

前記コンピュータを、

前記検証装置により生成されたチャレンジ情報を受信する受信手段(11, 21)、

前記検証のための秘密情報が記憶された秘密情報記憶装置(13, 23)、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子を生成する認証子生成手段(14, 24)、

前記認証子と前記実行内容及び前記チャレンジ情報とを特定のフォーマットに従って記述した認証コンテキストを生成する認証コンテキスト生成手段(15, 25)、

前記認証コンテキストを前記検証装置に送信する認証コンテキスト送信手段(11, 21)、として機能させるためのプログラムであり、

前記認証コンテキストは、

前記検証装置により、当該検証装置が生成したチャレンジ情報と同一のチャレンジ情報が記述されているか否かが検証され、前記検証装置により、前記秘密情報に対応する認証子検証情報に基づいて、認証子が検証され、当該各検証結果に基づいて正当性が検証されるものであることを特徴とするプログラム。

[15] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置(10, 20)に通信可能であり、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)に関し、当該検証装置のコンピュータに用いられるプログラムであって、

前記コンピュータを、

前記各認証エンティティ装置に記憶された秘密情報に対応する認証子検証情報が記憶された検証情報記憶装置(37)、

前記チャレンジ情報を生成するチャレンジ生成手段(33)、

このチャレンジ情報が記憶されるチャレンジ記憶装置(34)、

前記チャレンジ情報を送信するチャレンジ情報送信手段(31)、

前記各認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記チャレンジ情報を対象とした認証子が生成され、この認証子と前記実行内容及び前記チャレンジ情報とが特定のフォーマットに従って記述されて各認証コンテキストが生成された後、前記各認証エンティティ装置から送信された各認証コンテキストを受信する認証コンテキスト受信手段(31)、

前記受信した各認証コンテキスト毎に、前記チャレンジ記憶装置内のチャレンジ情報と同一のチャレンジ情報が記述されているか否かを検証するチャレンジ検証手段(35)、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を

検証する認証コンテキスト検証手段(36)、

として機能させるためのプログラム。

[16] 認証処理を検証するための検証装置に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置のうち、少なくとも1台の後段側の認証エンティティ装置(10)にも通信可能な少なくとも1台の前段側の認証エンティティ装置(20)に関し、当該前段側の認証エンティティ装置のコンピュータに用いられるプログラムであって、

前記コンピュータを、

前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値を生成する前段側ハッシュ値生成手段(27)、

前記検証のための秘密情報が記憶された前段側秘密情報記憶装置(23)、

前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子を生成する前段側認証子生成手段(24)、

前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とを特定のフォーマットに従って記述した前段側の認証コンテキストを生成する前段側認証コンテキスト生成手段(25')、

前記認証コンテキスト及び前記秘匿実行内容を送信する前段側送信手段、として機能させるためのプログラムであり、

前記秘匿実行内容は、前記後段側の認証エンティティ装置により受信されて当該秘匿実行内容を対象とした後段側ハッシュ値に変換されるものであり、

前記後段側ハッシュ値は、前記後段側の認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容と共に当該後段側ハッシュ値を対象とした認証子に変換される一方、この認証子及び当該実行内容と共に特定のフォーマットに従って後段側の認証コンテキストに記述され、この後段側の認証コンテキストと共に送信されるものであり、

前記各認証コンテキストは、

前記検証装置により、それぞれ受信されて当該各認証コンテキストに含まれる前段

側ハッシュ値と後段側ハッシュ値とが互いに同一であることが比較検証され、前記秘密情報に対応する認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子が検証され、当該各検証結果に基づいて、正当性が検証されるものであることを特徴とするプログラム。

[17] 認証処理を検証するための検証装置に通信可能であり、前記認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置のうち、少なくとも1台の前段側の認証エンティティ装置(20)にも通信可能な少なくとも1台の後段側の認証エンティティ装置(10)に関し、当該後段側の認証エンティティ装置のコンピュータに用いられるプログラムであって、

前記コンピュータを、

前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を前記前段側の認証エンティティ装置から受信する秘匿実行内容受信手段(11')、

前記受信した秘匿実行内容を対象とした後段側ハッシュ値を生成する後段側ハッシュ値生成手段(17)、

前記検証のための秘密情報が記憶された後段側秘密情報記憶装置(13)、

この秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象とした認証子を生成する後段側認証子生成手段(14)、

前記認証子、前記実行内容及び前記後段側ハッシュ値を特定のフォーマットに従って記述した認証コンテキストを生成する後段側認証コンテキスト生成手段(15')、

この認証コンテキストを送信する後段側送信手段(11')、として機能させるためのプログラムであり、

前記秘匿実行内容は、前記前段側の認証エンティティ装置から送信される前に、当該前段側の認証エンティティ装置により当該秘匿実行内容を対象とした前段側ハッシュ値に変換されるものでもあり、

前記前段側ハッシュ値は、前記前段側の認証エンティティ装置により、前記秘密情報に基づいて、前記認証構成プロセスの実行内容と共に当該前段側ハッシュ値を対象とした認証子に変換される一方、この認証子及び当該実行内容と共に特定のフォ

ーマットに従って前段側の認証コンテキストに記述され、この前段側の認証コンテキストと共に送信されるものであり、

前記各認証コンテキストは、

前記検証装置により、それぞれ受信されて当該各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることが比較検証され、前記秘密情報に対応する認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子が検証され、当該各検証結果に基づいて、正当性が検証されるものであることを特徴とするプログラム。

[18] 認証処理を構成する認証構成プロセスを個別に実行する複数の認証エンティティ装置に通信可能であり、前記各認証エンティティ装置で実行された前記認証処理を検証するための検証装置(30)に関し、当該検証装置のコンピュータに用いられるプログラムであって、

前記コンピュータを、

前記各認証エンティティ装置に記憶された秘密情報に対応する認証子検証情報が記憶された検証情報記憶装置(37)、

前記各認証エンティティ装置のうち、少なくとも1台の前段側の認証エンティティ装置により、前記認証構成プロセスの実行内容のうち、後段の認証構成プロセスに入力され且つ前記検証装置に対して秘匿する秘匿実行内容を対象とした前段側ハッシュ値が生成され、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記前段側ハッシュ値を対象とした認証子が生成され、前記認証子と前記前段側ハッシュ値の対象以外の実行内容及び前記前段側ハッシュ値とが特定のフォーマットに従って記述されて前段側の認証コンテキストが生成された後、前記前段側の認証エンティティ装置から送信された前段側の認証コンテキストを受信する第1の認証コンテキスト受信手段(31)、

前記各認証エンティティ装置のうち、少なくとも1台の後段側の認証エンティティ装置により、前記前段側の認証エンティティ装置から送信された秘匿実行内容が受信され、この秘匿実行内容を対象とした後段側ハッシュ値が生成され、前記秘密情報に基づいて、前記認証構成プロセスの実行内容及び前記後段側ハッシュ値を対象と

した認証子が生成され、この認証子、当該実行内容及び前記後段側ハッシュ値が特定のフォーマットに従って記述されて後段側の認証コンテキストが生成された後、前記後段側の認証エンティティ装置から送信された後段側の認証コンテキストを受信する第2の認証コンテキスト受信手段(31)、

前記受信した各認証コンテキストに含まれる前段側ハッシュ値と後段側ハッシュ値とが互いに同一であることを比較検証するハッシュ値比較検証手段(39)、

前記認証子検証情報に基づいて、前記各認証コンテキスト毎に、認証子を検証する認証子検証手段(38)、

前記各検証手段による検証結果に基づいて、前記各認証コンテキストの正当性を検証する認証コンテキスト検証手段(36')、

として機能させるためのプログラム。

[19] 請求項15又は請求項18に記載のプログラムにおいて、

前記コンピュータを、

前記認証構成プロセスの実行に関し、受け入れ可能な実行環境を規定したプロファイルリストを生成するプロファイルリスト生成手段、

前記プロファイルリストを送信するリスト送信手段(31)、として機能させるためのプログラムであり、

前記プロファイルリストは、

前記検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置に受信され、当該認証要求装置により、前記各認証エンティティ装置毎に取得された、認証構成プロセスを実行する機能を規定した機能リストと比較されるものであり、

この比較は、

前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するための処理であり、

前記実行プロファイルは、

前記各認証エンティティ装置に送信され、前記認証構成プロセスを実行する実行環境を規定したものであることを特徴とするプログラム。

[20] 請求項19に記載の検証装置と前記各認証エンティティ装置との間で通信を中継する認証要求装置(40)のコンピュータに用いられるプログラムにおいて、

前記認証要求装置のコンピュータを、

前記検証装置からプロファイルリストを受信するプロファイルリスト受信手段(41)、

認証構成プロセスを実行する機能を規定した機能リストを前記各認証エンティティ装置毎に受信する機能リスト受信手段(41)、

前記プロファイルリスト及び前記機能リストの両者を満たすように、実行プロファイルを決定するプロファイル決定手段(44)、

前記実行プロファイルを各認証エンティティ装置に送信する実行プロファイル送信手段(41)、として機能させるためのプログラム。

[21] 請求項14、請求項16又は請求項17に記載のプログラムにおいて、

前記コンピュータを、

認証毎に同一内容を表す静的情報に関し、前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報が記憶されるリンク先情報記憶装置(19, 29)、として機能させ、

前記認証コンテキスト生成手段は、前記静的情報に代えて前記リンク先情報を含むように前記認証コンテキストを生成するように前記コンピュータを機能させ、

この認証コンテキストは、

前記検証装置により受信され、当該認証コンテキスト内のリンク先情報に基づいて、静的情報が取得され、この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理が検証されるものであることを特徴とするプログラム。

[22] 請求項15、請求項18又は請求項19に記載のプログラムにおいて、

前記コンピュータを、

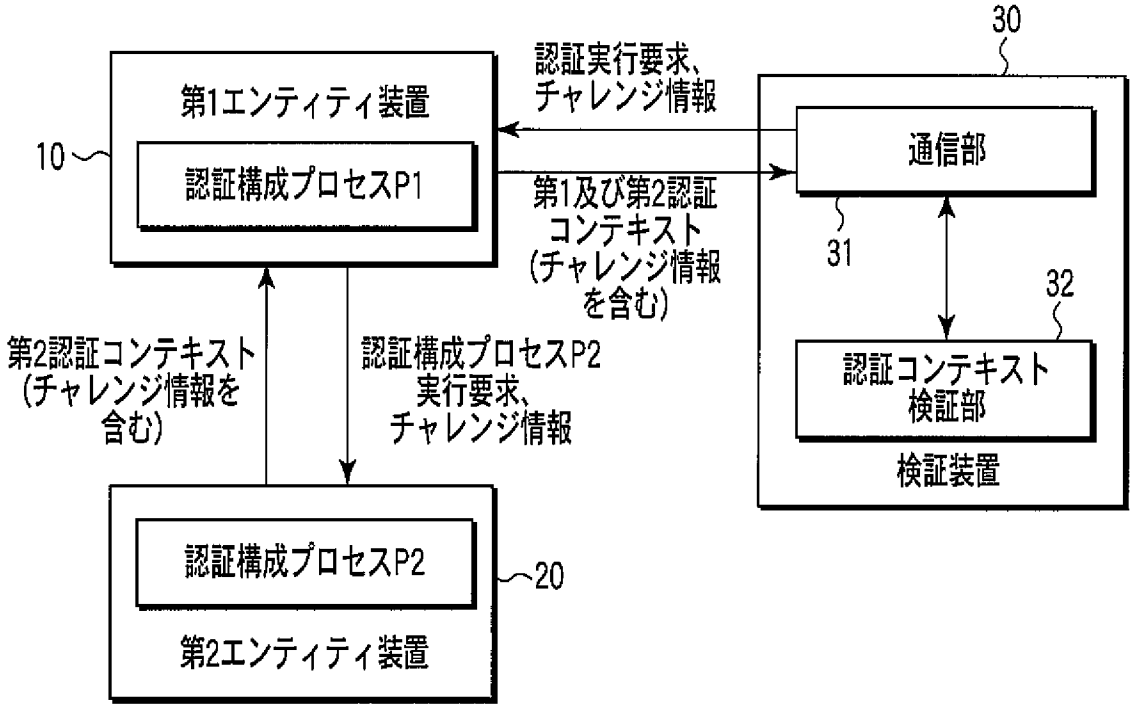
前記各認証コンテキストが、認証毎に同一内容を表す静的情報に関し、前記静的情報に代えて前記静的情報のデータ量よりも小さいデータ量からなり前記静的情報を取得するためのリンク先情報を含むとき、前記認証コンテキスト受信手段により受信した認証コンテキスト内のリンク先情報に基づいて、静的情報を取得する手段、

この静的情報と当該認証コンテキスト内の実行内容とに基づいて、前記認証処理を

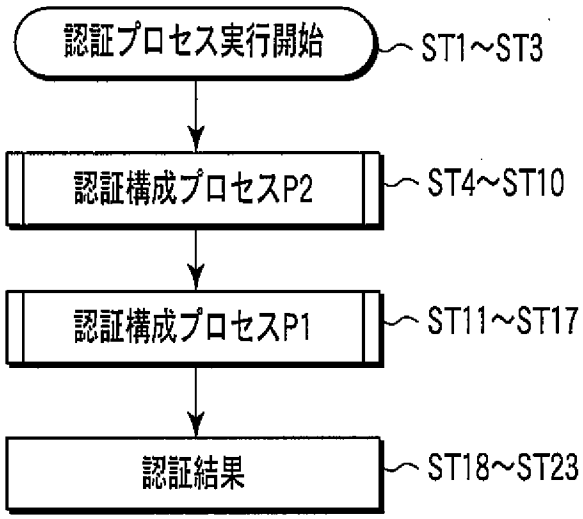
検証する検証手段、

として機能させるためのプログラム。

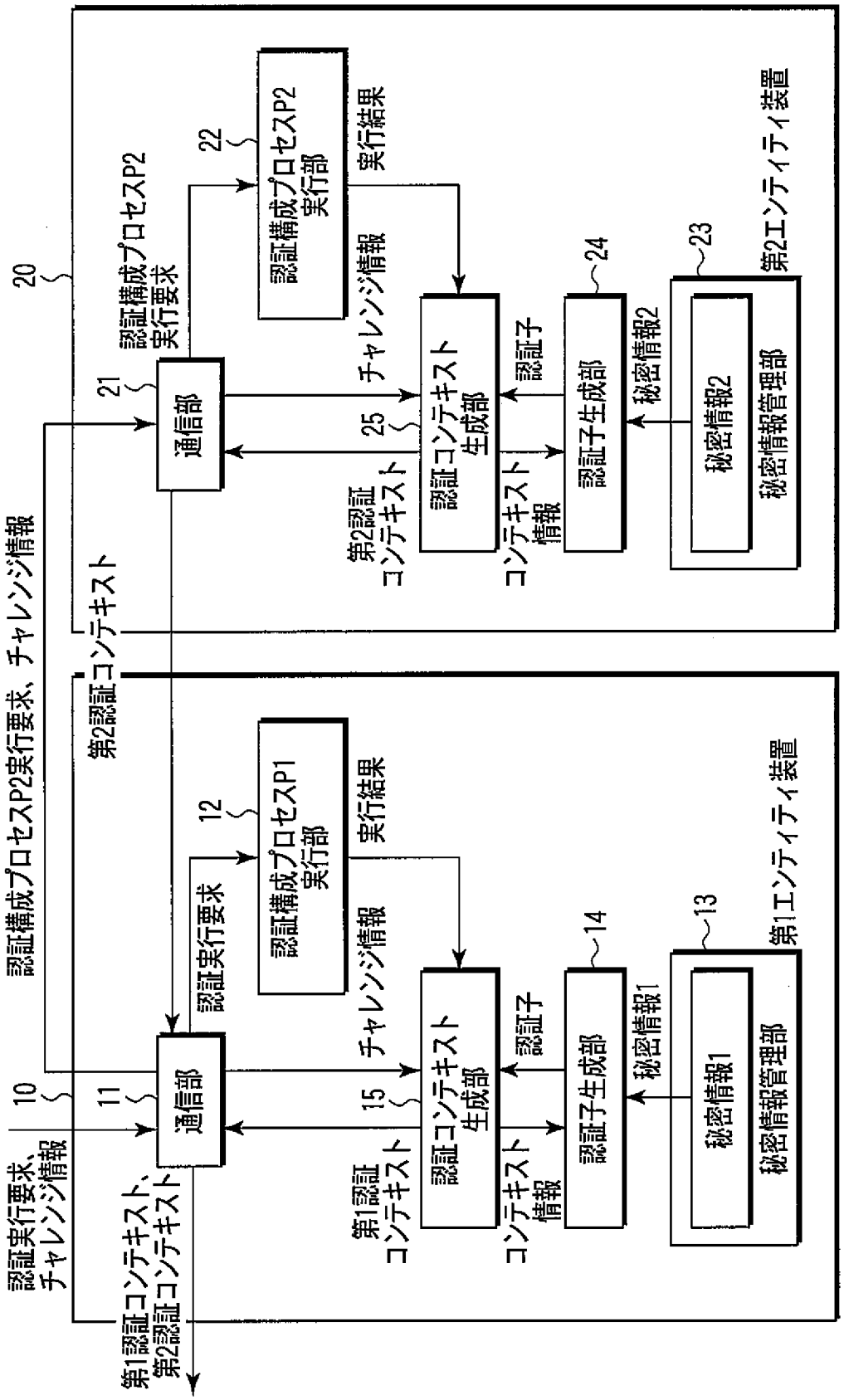
[図1]


30
認証実行要求、
チャレンジ情報
第1エンティティ装置
10
認証構成プロセスP1
通信部
第1及び第2認証
コンテキスト
(チャレンジ情報
を含む)
31
32
第2認証コンテキスト
(チャレンジ情報を
含む)
認証構成プロセスP2
実行要求、
チャレンジ情報
認証コンテキスト
検証部
検証装置
認証構成プロセスP2
20
第2エンティティ装置

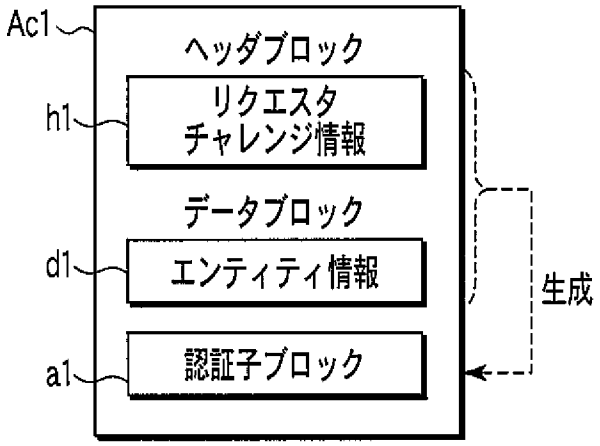
[図2]


認証プロセス実行開始
ST1~ST3
認証構成プロセスP2
ST4~ST10
認証構成プロセスP1
ST11~ST17
認証結果
ST18~ST23

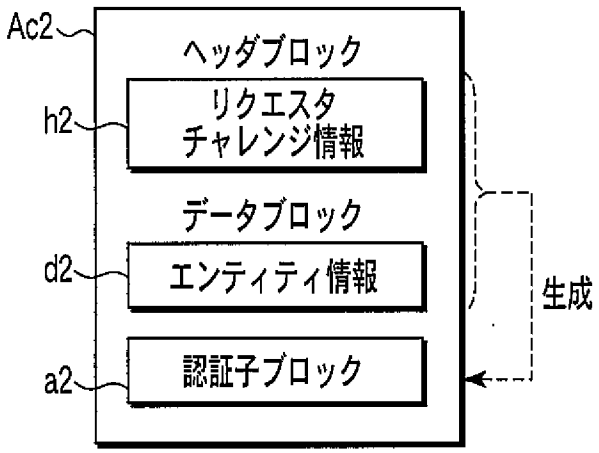
[図3]


認証構成プロセスP2実行要求、チャレンジ情報
認証実行要求、チャレンジ情報
第1認証コンテキスト、第2認証コンテキスト
10
11
通信部
認証実行要求
12
認証構成プロセスP1実行部
実行結果
チャレンジ情報
15
第1認証コンテキスト
認証コンテキスト生成部
認証子
コンテキスト情報
14
認証子生成部
秘密情報1
13
秘密情報1
秘密情報管理部
第1エンティティ装置
第2認証コンテキスト
20
認証構成プロセスP2実行要求
21
通信部
22
認証構成プロセスP2実行部
実行結果
チャレンジ情報
25
第2認証コンテキスト
認証コンテキスト生成部
認証子
コンテキスト情報
24
認証子生成部
秘密情報2
23
秘密情報2
秘密情報管理部
第2エンティティ装置

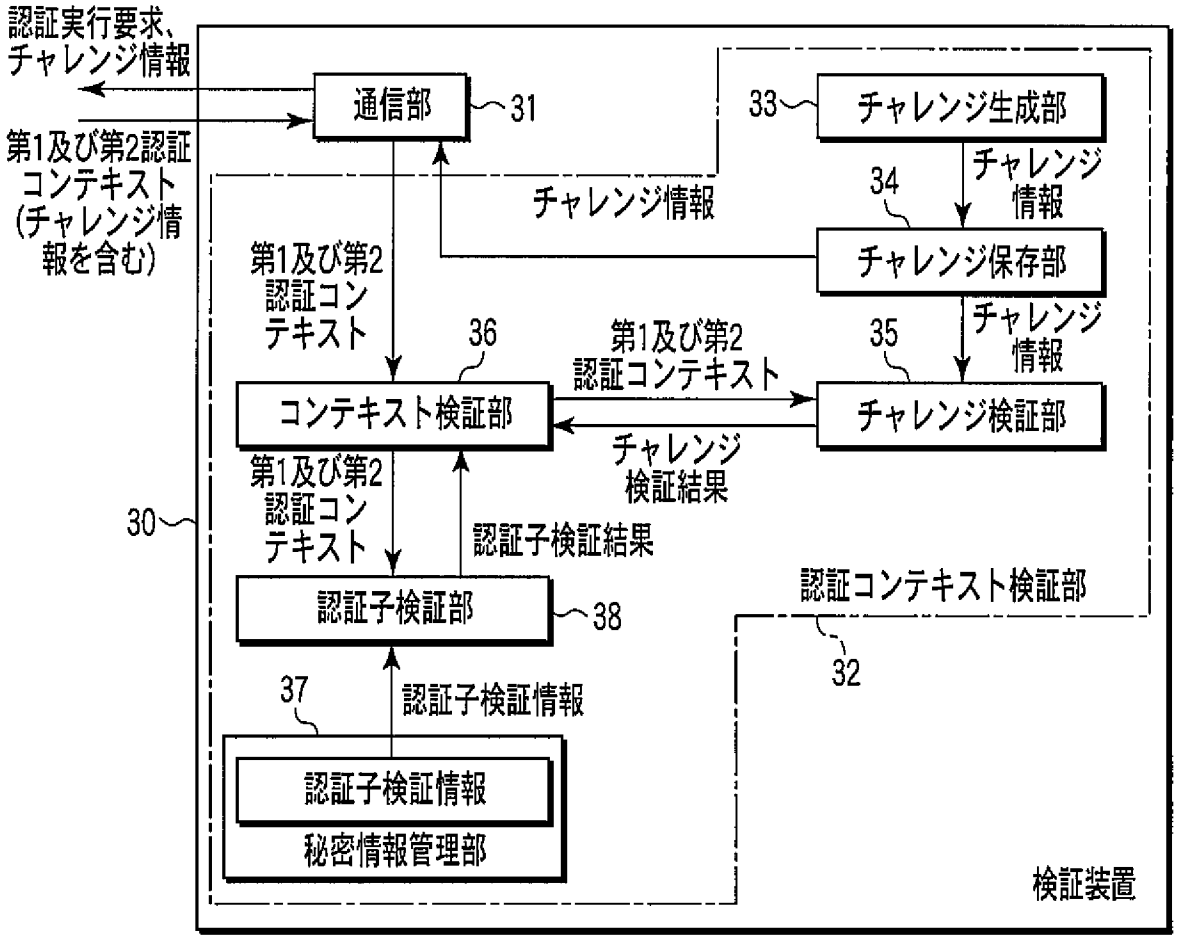
[図4A]


Ac1
ヘッダブロック
h1
リクエスタ
チャレンジ情報
データブロック
d1
エンティティ情報
a1
認証子ブロック
生成

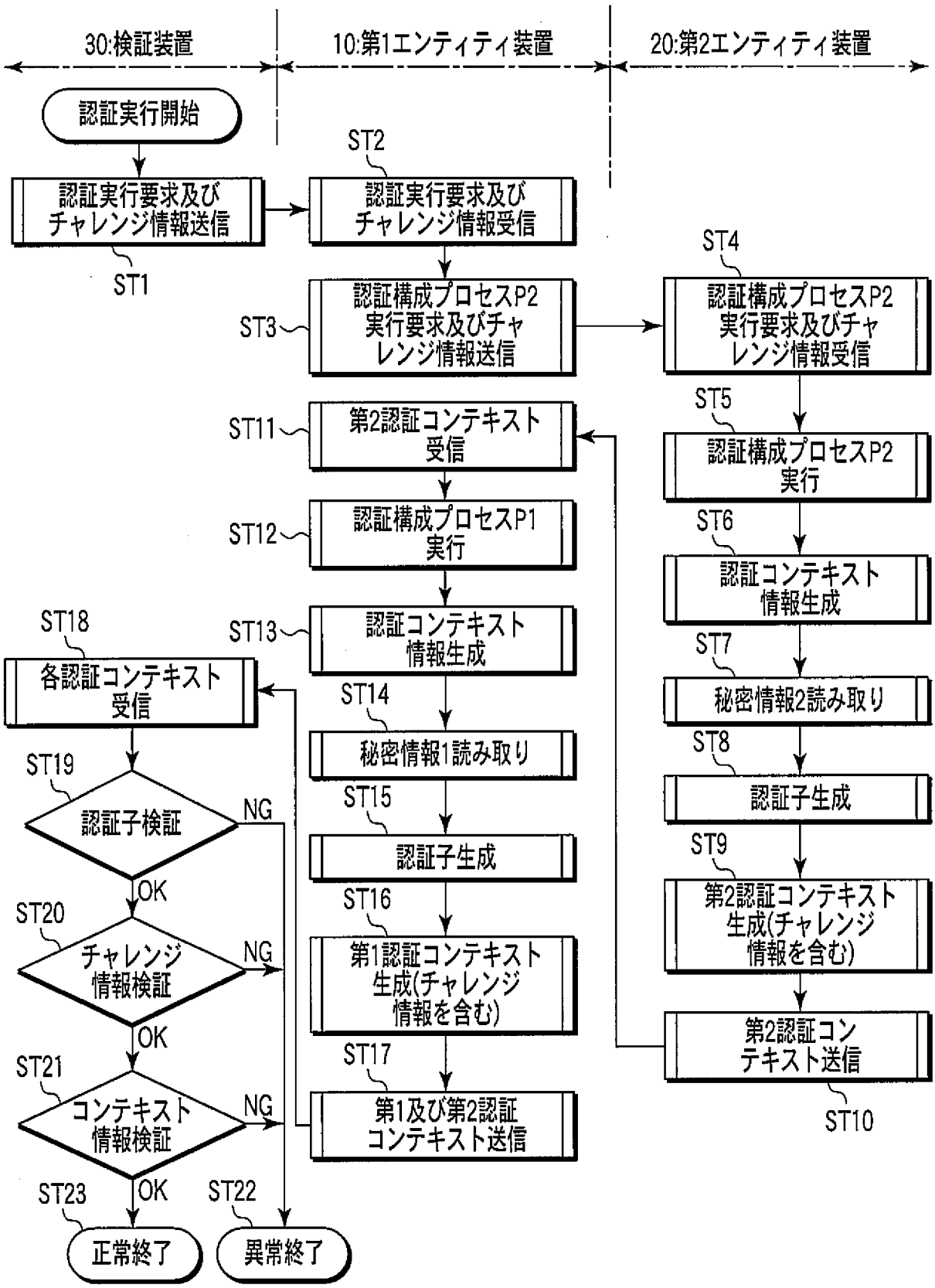
[図4B]


Ac2
ヘッダブロック
h2
リクエスタ
チャレンジ情報
データブロック
d2
エンティティ情報
a2
認証子ブロック
生成

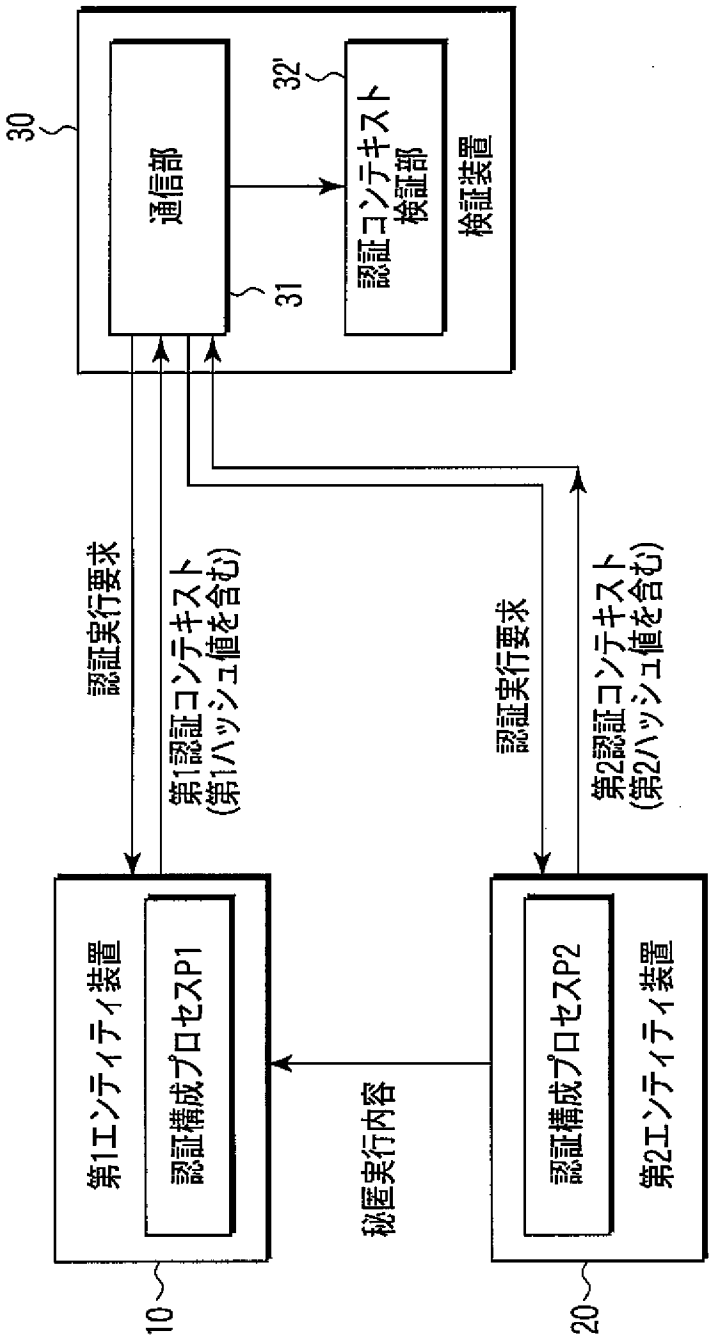
[図5]


認証実行要求、
チャレンジ情報
第1及び第2認証
コンテキスト
(チャレンジ情
報を含む)
通信部
31
33
チャレンジ生成部
チャレンジ
情報
34
チャレンジ情報
チャレンジ保存部
第1及び第2
認証コン
テキスト
36
第1及び第2
認証コンテキスト
35
チャレンジ
情報
コンテキスト検証部
チャレンジ検証部
チャレンジ
検証結果
第1及び第2
認証コン
テキスト
30
認証子検証結果
認証コンテキスト検証部
認証子検証部
38
32
37
認証子検証情報
認証子検証情報
秘密情報管理部
検証装置

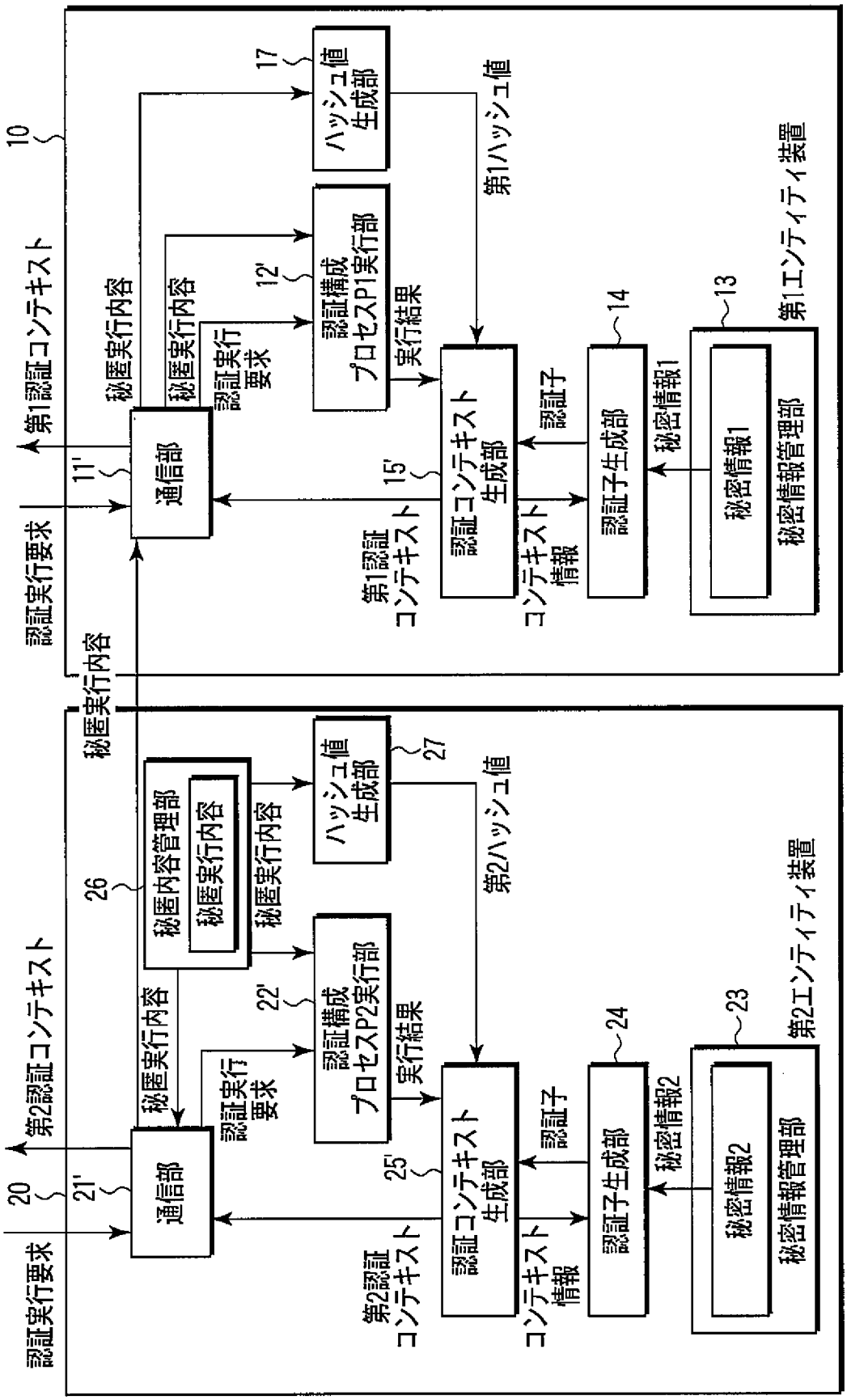
[図6]


30:検証装置
10:第1エンティティ装置
20:第2エンティティ装置
認証実行開始
認証実行要求及び
チャレンジ情報送信
ST1
ST2
認証実行要求及び
チャレンジ情報受信
ST3
認証構成プロセスP2
実行要求及びチャ
レンジ情報送信
ST4
認証構成プロセスP2
実行要求及びチャ
レンジ情報受信
ST5
認証構成プロセスP2
実行
ST6
認証コンテキスト
情報生成
ST7
秘密情報2読み取り
ST8
認証子生成
ST9
第2認証コンテキスト
生成(チャレンジ
情報を含む)
第2認証コン
テキスト送信
ST10
ST11
第2認証コンテキスト
受信
ST12
認証構成プロセスP1
実行
ST13
認証コンテキスト
情報生成
ST14
秘密情報1読み取り
ST15
認証子生成
ST16
第1認証コンテキスト
生成(チャレンジ
情報を含む)
ST17
第1及び第2認証
コンテキスト送信
ST18
各認証コンテキスト
受信
ST19
認証子検証
NG
OK
ST20
チャレンジ
情報検証
NG
OK
ST21
コンテキスト
情報検証
NG
OK
ST23
正常終了
ST22
異常終了

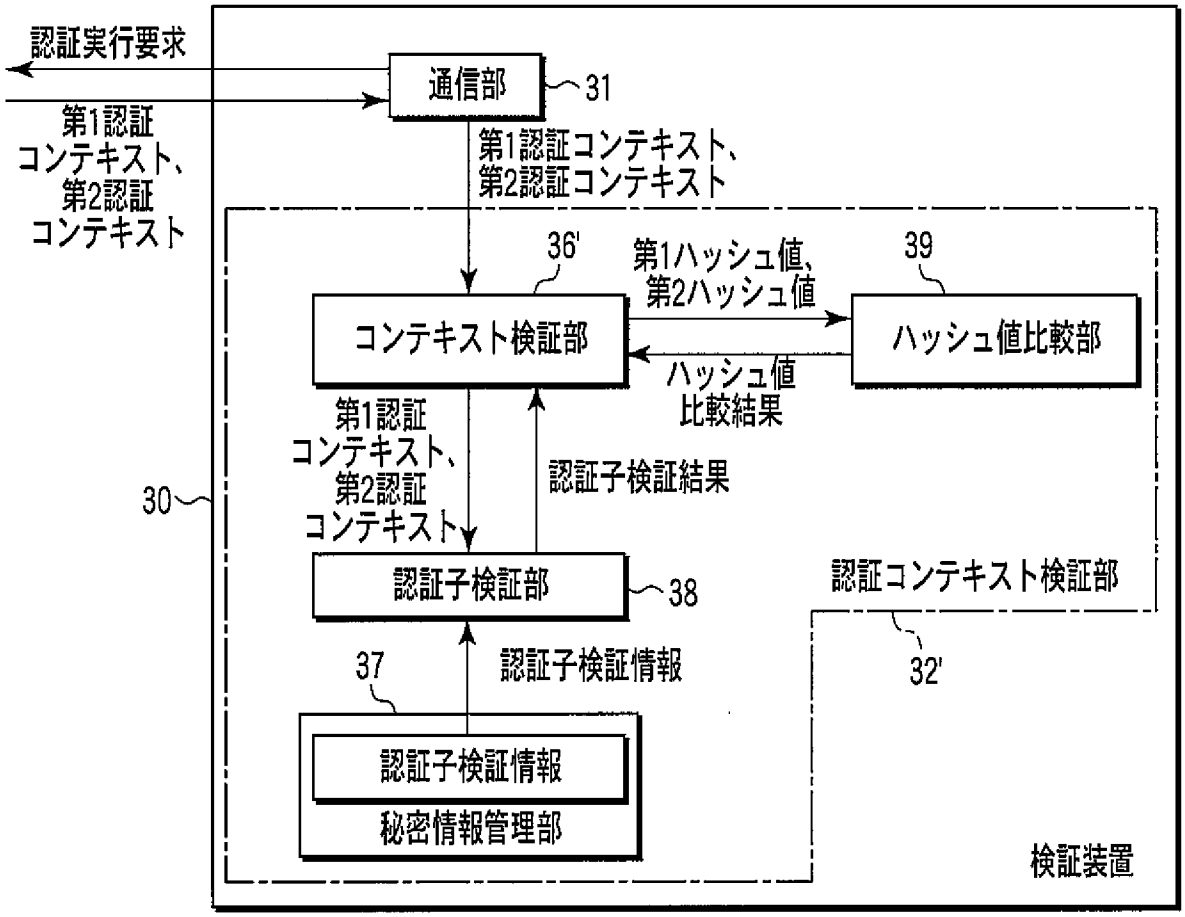
[図7]


30
通信部
31
32'
認証コンテキスト検証部
検証装置
認証実行要求
第1認証コンテキスト(第1ハッシュ値を含む)
認証実行要求
第2認証コンテキスト(第2ハッシュ値を含む)
第1エンティティ装置
認証構成プロセスP1
秘匿実行内容
認証構成プロセスP2
第2エンティティ装置
10
20

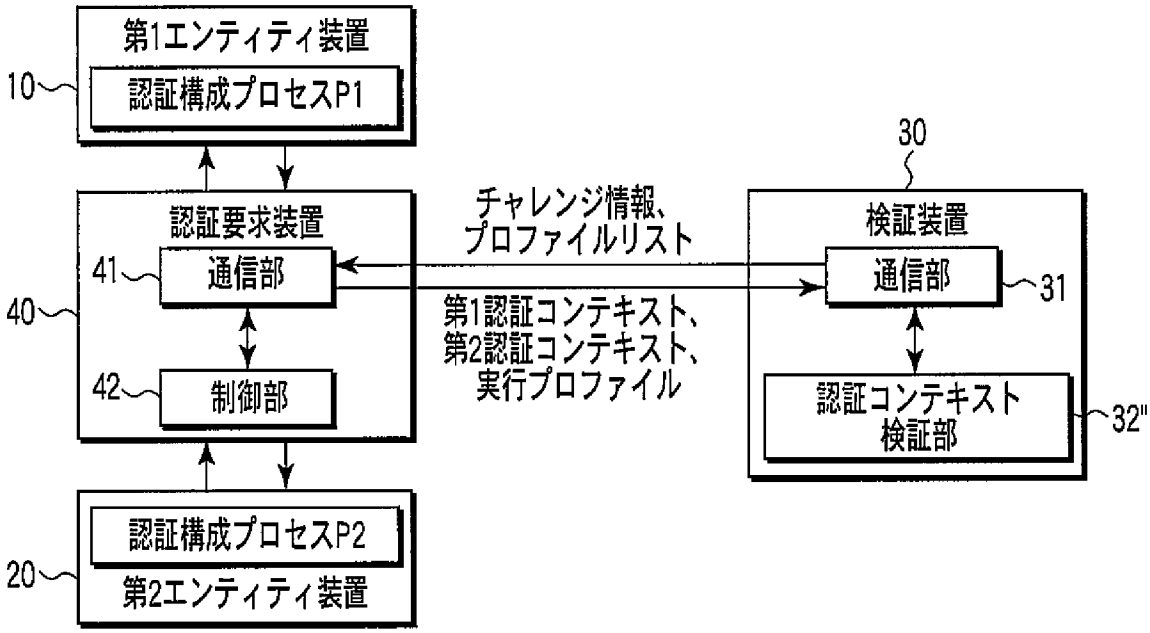
[図8]


10
第1認証コンテキスト
認証実行要求
秘匿実行内容
11'
通信部
秘匿実行内容
認証実行要求
12'
認証構成プロセスP1実行部
実行結果
17
ハッシュ値生成部
第1ハッシュ値
15'
認証コンテキスト生成部
第1認証コンテキスト
認証子
コンテキスト情報
14
認証子生成部
秘密情報1
13
秘密情報1
秘密情報管理部
第1エンティティ装置
秘匿実行内容
20
第2認証コンテキスト
認証実行要求
21'
通信部
秘匿実行内容
認証実行要求
22'
認証構成プロセスP2実行部
実行結果
26
秘匿内容管理部
秘匿実行内容
秘匿実行内容
27
ハッシュ値生成部
第2ハッシュ値
25'
認証コンテキスト生成部
第2認証コンテキスト
認証子
コンテキスト情報
24
認証子生成部
秘密情報2
23
秘密情報2
秘密情報管理部
第2エンティティ装置

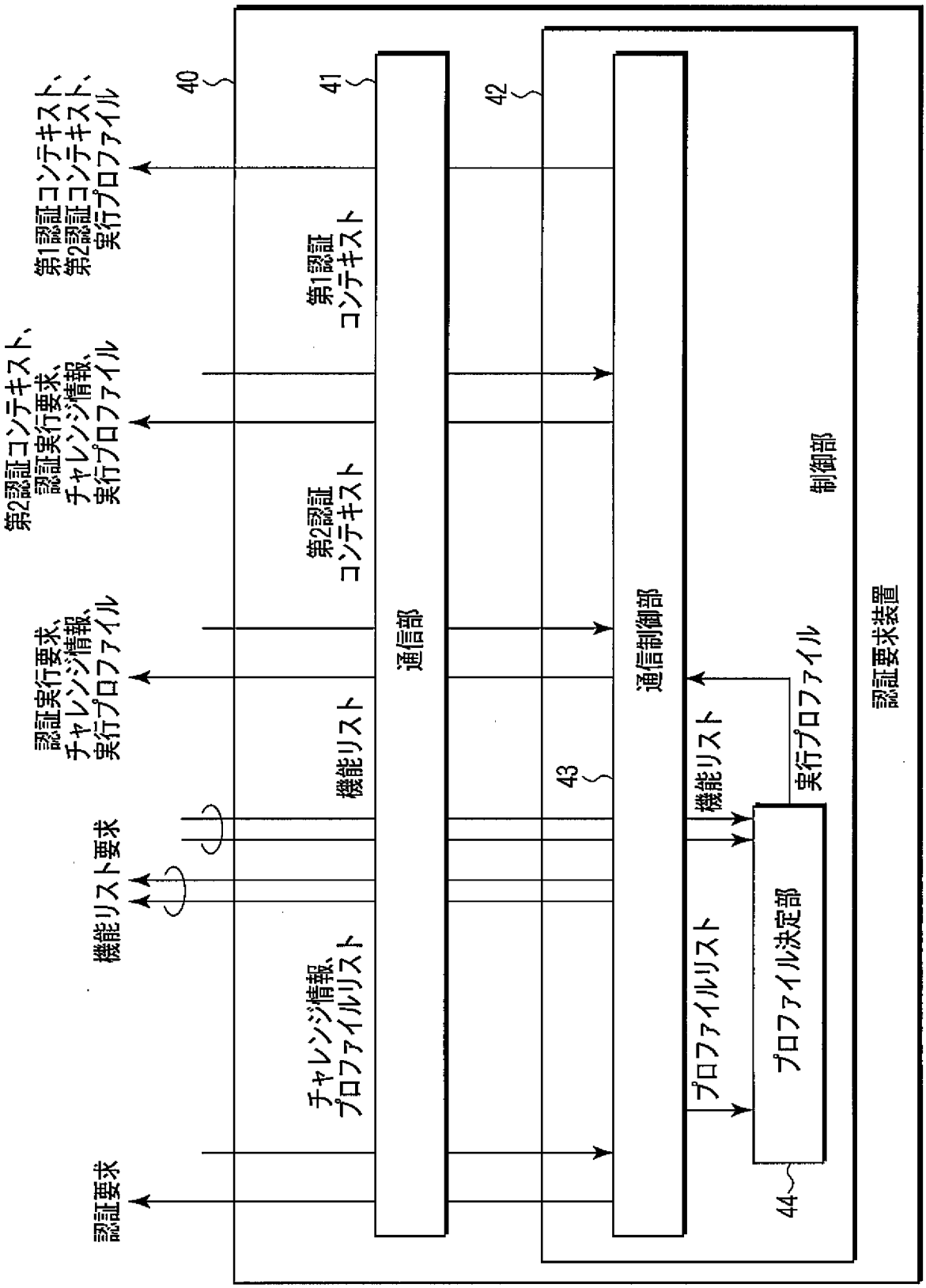
[図9]


認証実行要求
通信部
31
第1認証
コンテキスト、
第2認証
コンテキスト
第1認証コンテキスト、
第2認証コンテキスト
36'
第1ハッシュ値、
第2ハッシュ値
39
コンテキスト検証部
ハッシュ値比較部
ハッシュ値
比較結果
第1認証
コンテキスト、
第2認証
コンテキスト
認証子検証結果
30
認証子検証部
38
認証コンテキスト検証部
37
認証子検証情報
32'
認証子検証情報
秘密情報管理部
検証装置

[図10]


第1エンティティ装置
10
認証構成プロセスP1
30
認証要求装置
チャレンジ情報、
プロファイルリスト
検証装置
41
通信部
通信部
31
40
第1認証コンテキスト、
第2認証コンテキスト、
実行プロファイル
42
制御部
認証コンテキスト
検証部
32''
認証構成プロセスP2
20
第2エンティティ装置

[図11]


40
41
42
43
44
第1認証コンテキスト、
第2認証コンテキスト、
実行プロファイル
第2認証コンテキスト、
認証実行要求、
チャレンジ情報、
実行プロファイル
認証実行要求、
チャレンジ情報、
実行プロファイル
機能リスト要求
認証要求
第1認証
コンテキスト
第2認証
コンテキスト
機能リスト
チャレンジ情報、
プロファイルリスト
通信部
通信制御部
機能リスト
プロファイルリスト
実行プロファイル
プロファイル決定部
制御部
認証要求装置

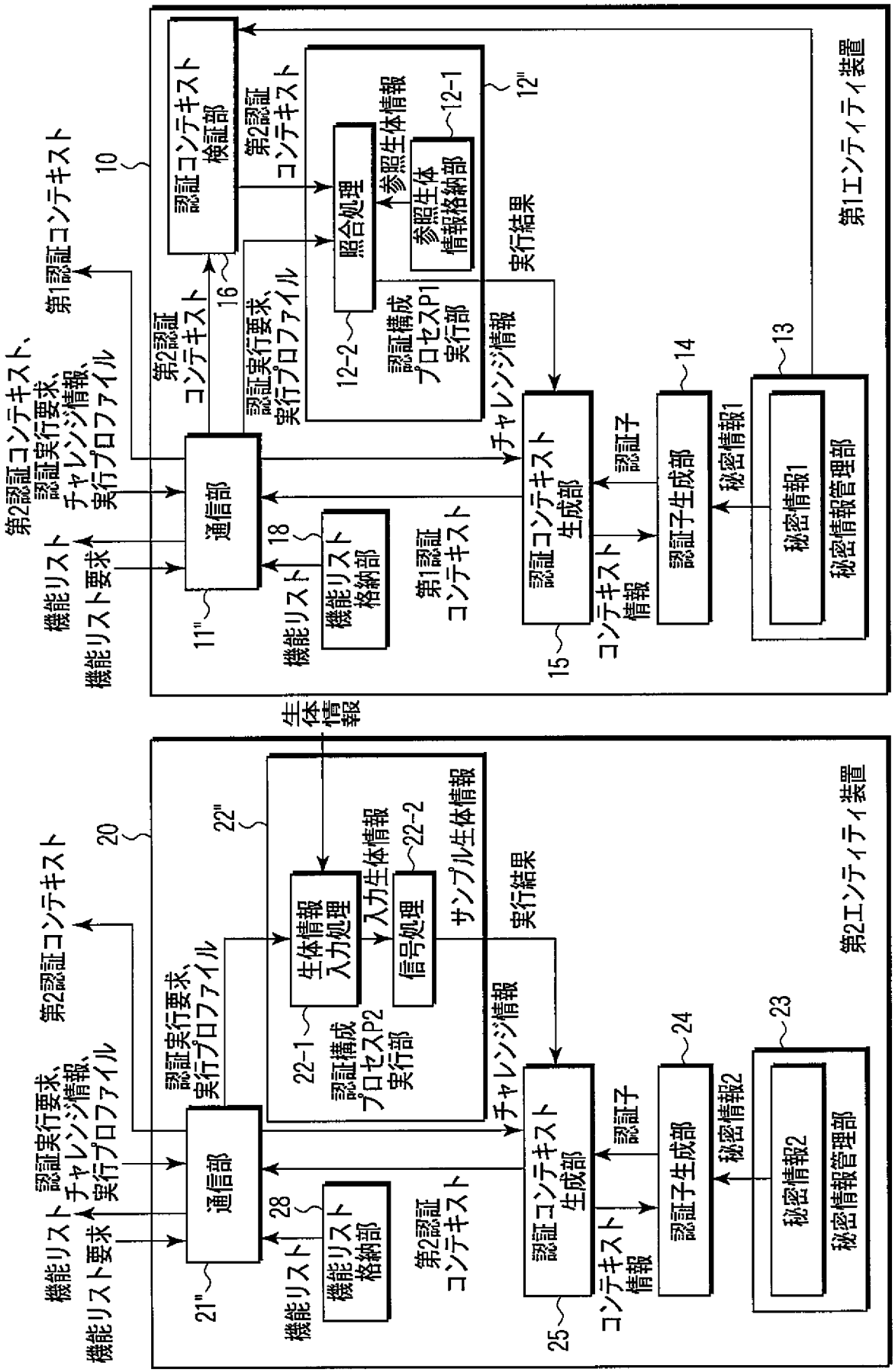
[図12]

ハッシュ値計算アルゴリズム	アルゴリズムA、アルゴリズムB、アルゴリズムC
認証子計算アルゴリズム	アルゴリズムA、アルゴリズムB
第1エンティティ装置の安全性	20～80%
第2エンティティ装置の安全性	20～80%
入力生体情報の品質	50～90点
サンプル生体情報の品質	50～90点
参照生体情報の品質	50～90点
照合の一致度	80～100%
照合アルゴリズム	アルゴリズムA、アルゴリズムB、アルゴリズムC
照合パラメータ	パラメータA、 パラメータB、 パラメータC
照合の品質	70～90点
参照生体情報の品質	50～90点

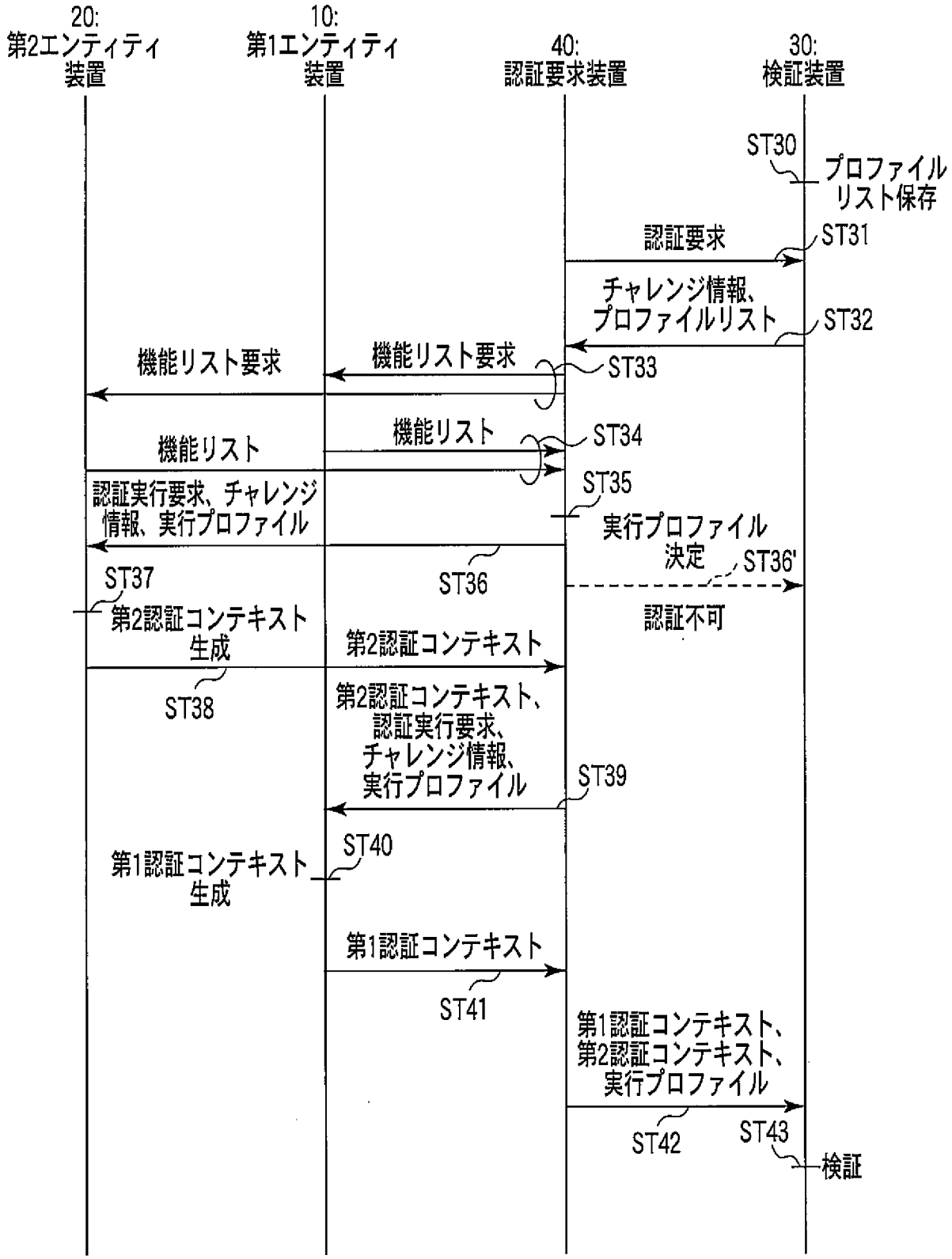
[図13]

ハッシュ値計算アルゴリズム	:A
認証子計算アルゴリズム	:B
第1エンティティ装置の安全性	:70%
第2エンティティ装置の安全性	:70%
入力生体情報の品質	:80点
サンプル生体情報の品質	:80点
参照生体情報の品質	:80点
照合の一致度	:85%
照合アルゴリズム	:C
照合パラメータ	:B
照合の品質	:80点
参照生体情報の品質	:80点

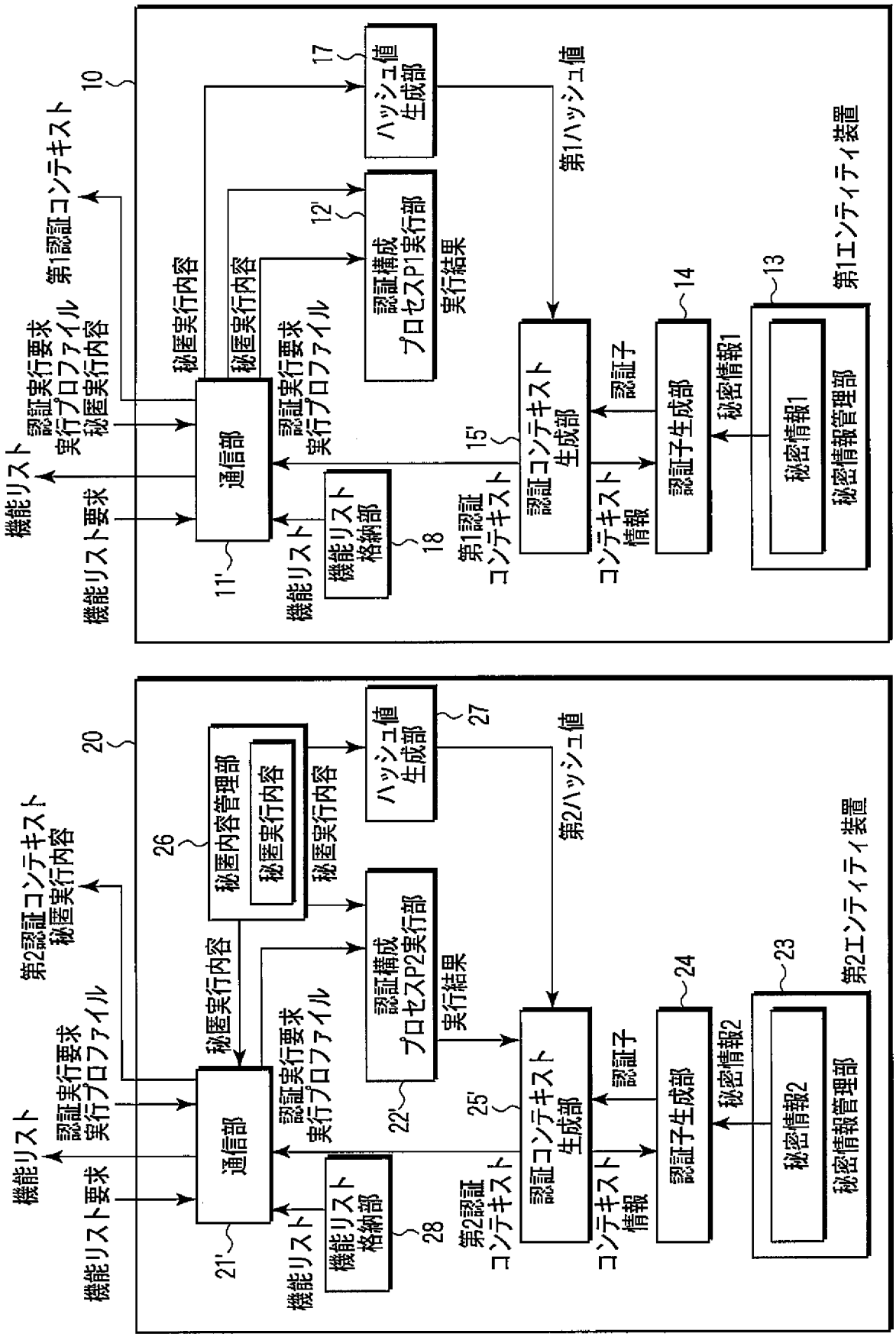
[図14]


第1エンティティ装置
第2エンティティ装置
10
11"
12"
12-1
12-2
13
14
15
16
18
20
21"
22"
22-1
22-2
23
24
25
28
認証コンテキスト検証部
第2認証コンテキスト
照合処理
参照生体情報
参照生体情報格納部
認証構成プロセスP1実行部
認証実行要求、実行プロファイル
第1認証コンテキスト
第2認証コンテキスト、認証実行要求、チャレンジ情報、実行プロファイル
機能リスト
機能リスト要求
通信部
機能リスト格納部
機能リスト
認証コンテキスト生成部
認証子
認証子生成部
秘密情報1
秘密情報管理部
コンテキスト情報
チャレンジ情報
実行結果
認証実行要求、実行プロファイル
認証実行要求、チャレンジ情報、実行プロファイル
生体情報
生体情報入力処理
入力生体情報
信号処理
サンプル生体情報
認証構成プロセスP2実行部
秘密情報2

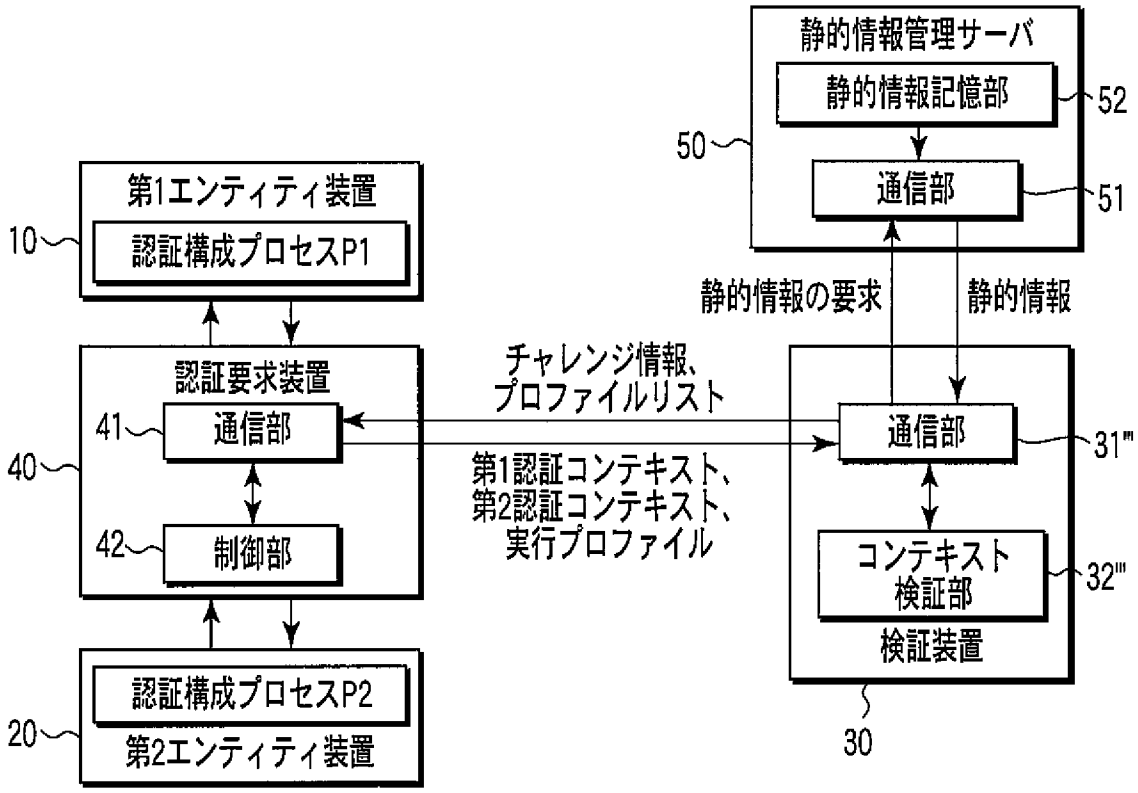
[図15]


20:
第2エンティティ
装置
10:
第1エンティティ
装置
40:
認証要求装置
30:
検証装置
ST30
プロファイル
リスト保存
認証要求
ST31
チャレンジ情報、
プロファイルリスト
ST32
機能リスト要求
機能リスト要求
ST33
機能リスト
機能リスト
ST34
ST35
認証実行要求、チャレンジ
情報、実行プロファイル
実行プロファイル
決定
ST36'
ST36
ST37
第2認証コンテキスト
生成
認証不可
第2認証コンテキスト
ST38
第2認証コンテキスト、
認証実行要求、
チャレンジ情報、
実行プロファイル
ST39
ST40
第1認証コンテキスト
生成
第1認証コンテキスト
ST41
第1認証コンテキスト、
第2認証コンテキスト、
実行プロファイル
ST42
ST43
検証

[図16]


10
第1認証コンテキスト
秘匿実行内容
認証実行要求
実行プロファイル
秘匿実行内容
機能リスト
機能リスト要求
通信部
11'
秘匿実行内容
認証実行要求
実行プロファイル
機能リスト
機能リスト格納部
18
ハッシュ値生成部
17
認証構成プロセスP1実行部
12'
実行結果
第1ハッシュ値
認証コンテキスト生成部
15'
第1認証コンテキスト
コンテキスト情報
認証子
認証子生成部
14
秘密情報1
秘密情報1
秘密情報管理部
13
第1エンティティ装置
20
第2認証コンテキスト
秘匿実行内容
認証実行要求
実行プロファイル
機能リスト
機能リスト要求
通信部
21'
秘匿実行内容
認証実行要求
実行プロファイル
機能リスト
機能リスト格納部
28
秘匿内容管理部
秘匿実行内容
26
秘匿実行内容
ハッシュ値生成部
27
認証構成プロセスP2実行部
22'
実行結果
第2ハッシュ値
認証コンテキスト生成部
25'
第2認証コンテキスト
コンテキスト情報
認証子
認証子生成部
24
秘密情報2
秘密情報2
秘密情報管理部
23
第2エンティティ装置

[図17]

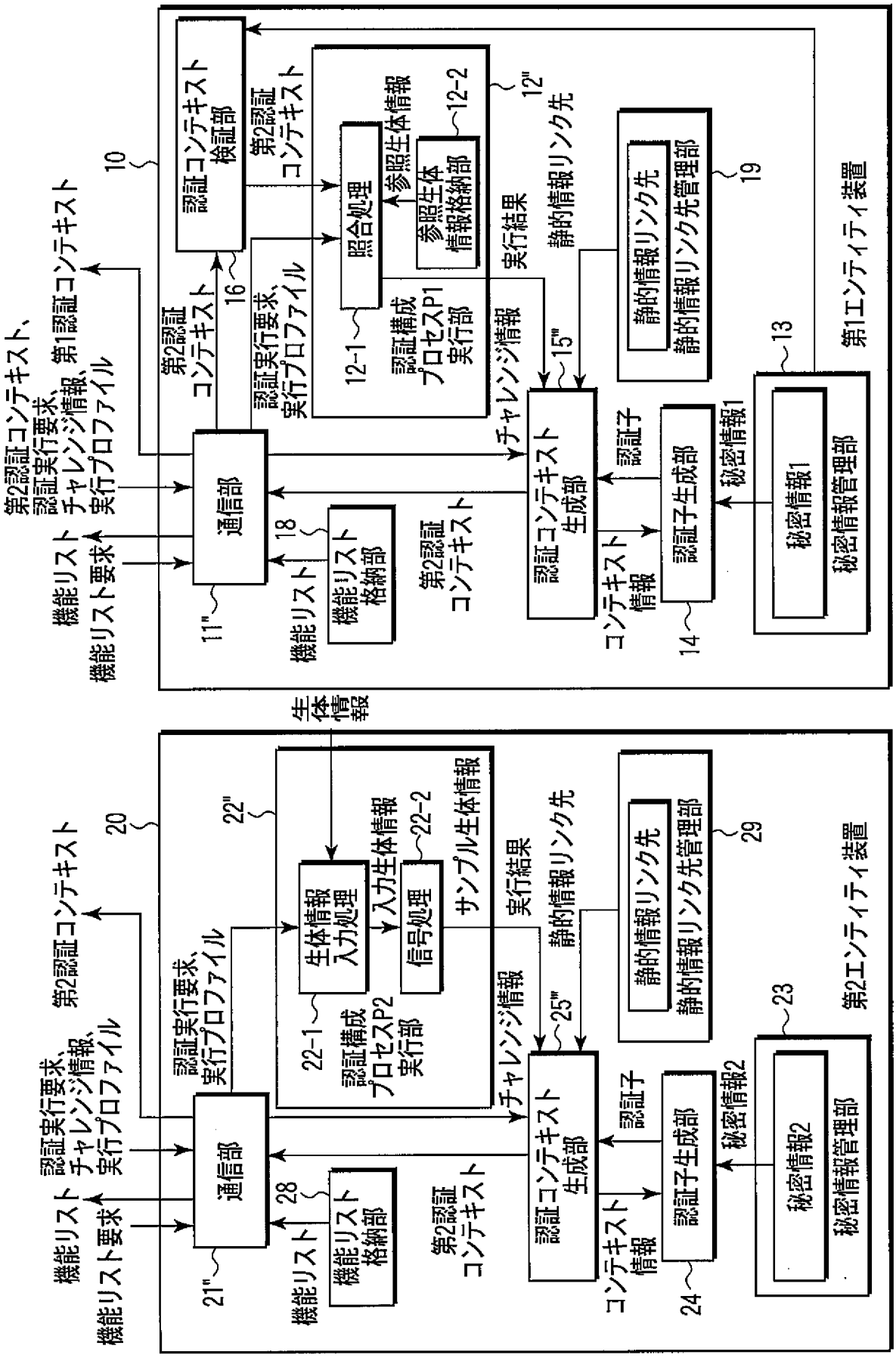


[図18]

Ct

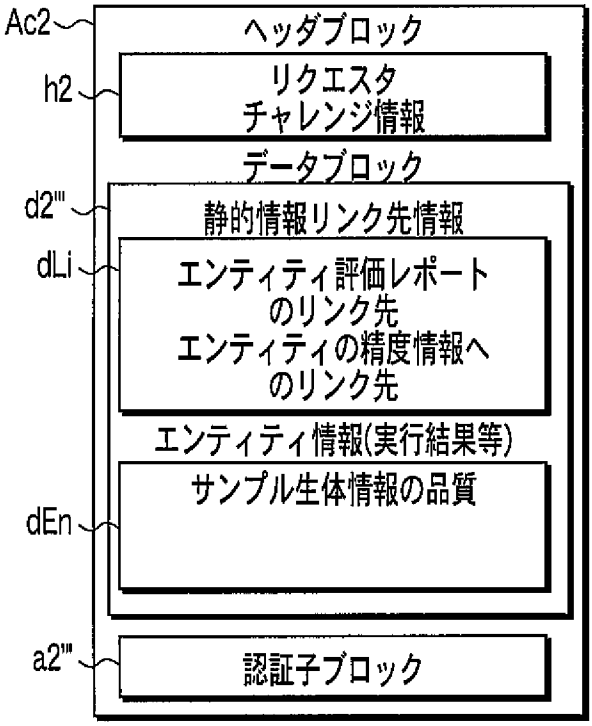
領域名	項　目	内　容
基本領域	バージョン	証明書形式のバージョン
	シリアル番号	証明書のシリアル番号
	署名アルゴリズム	発行者署名の署名アルゴリズム
	有効期限	テンプレートの有効期限
	発行者名	証明書の発行者名情報
	ハッシュアルゴリズム	テンプレートダイジェストのハッシュアルゴリズム
	テンプレートダイジェスト	テンプレートのハッシュ値
	テンプレート評価結果	テンプレートの評価結果
	テンプレート評価基準	テンプレートの評価基準
署名領域	発行者署名	基本領域を対象とした、発行者のデジタル署名

[図19]

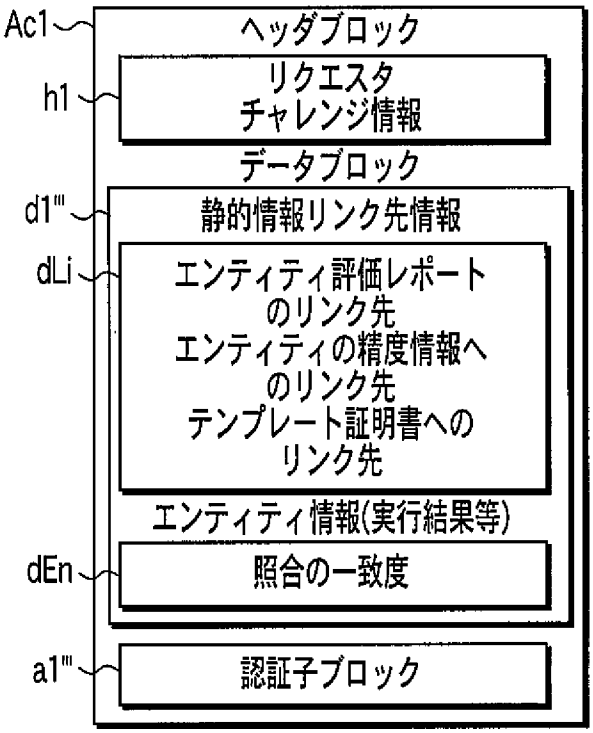


10
認証コンテキスト検証部
16
第2認証コンテキスト
照合処理
12-1
参照生体情報
参照生体情報格納部
12-2
12"
認証構成プロセスP1実行部
認証実行要求、実行プロファイル
第2認証コンテキスト
第1認証コンテキスト
第2認証コンテキスト、認証実行要求、チャレンジ情報、実行プロファイル
機能リスト
機能リスト要求
通信部
11"
18
機能リスト格納部
機能リスト
第2認証コンテキスト
チャレンジ情報
実行結果
静的情報リンク先
15"
認証コンテキスト生成部
認証子
認証子生成部
14
コンテキスト情報
秘密情報1
秘密情報1
秘密情報管理部
13
静的情報リンク先
静的情報リンク先管理部
19
第1エンティティ装置
生体情報
20
22"
生体情報入力処理
22-1
入力生体情報
信号処理
22-2
サンプル生体情報
認証構成プロセスP2実行部
認証実行要求、実行プロファイル
第2認証コンテキスト
認証実行要求、チャレンジ情報、実行プロファイル
機能リスト
機能リスト要求
通信部
21"
28
機能リスト格納部
機能リスト
第2認証コンテキスト
チャレンジ情報
実行結果
静的情報リンク先
25"
認証コンテキスト生成部
認証子
認証子生成部
24
コンテキスト情報
秘密情報2
秘密情報2
秘密情報管理部
23
静的情報リンク先
静的情報リンク先管理部
29
第2エンティティ装置

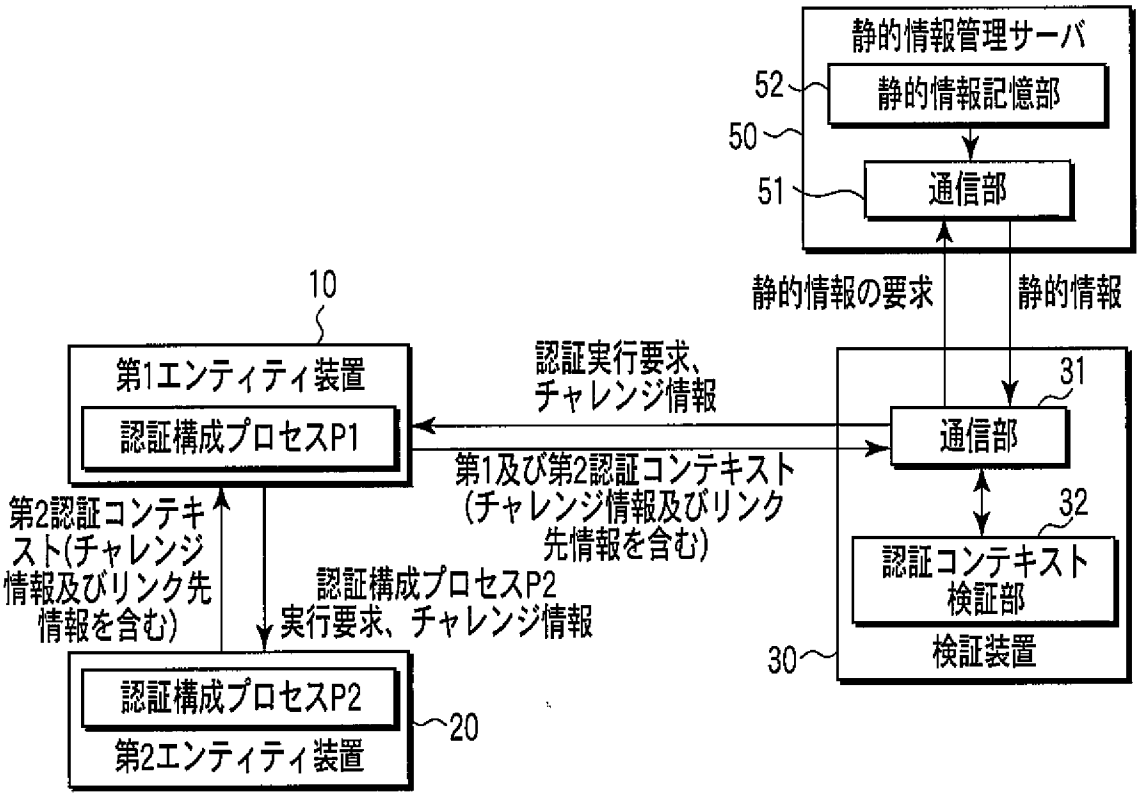
[図20A]


Ac2
ヘッダブロック
h2
リクエスタ
チャレンジ情報
データブロック
d2'''
静的情報リンク先情報
dLi
エンティティ評価レポート
のリンク先
エンティティの精度情報へ
のリンク先
エンティティ情報(実行結果等)
サンプル生体情報の品質
dEn
a2'''
認証子ブロック

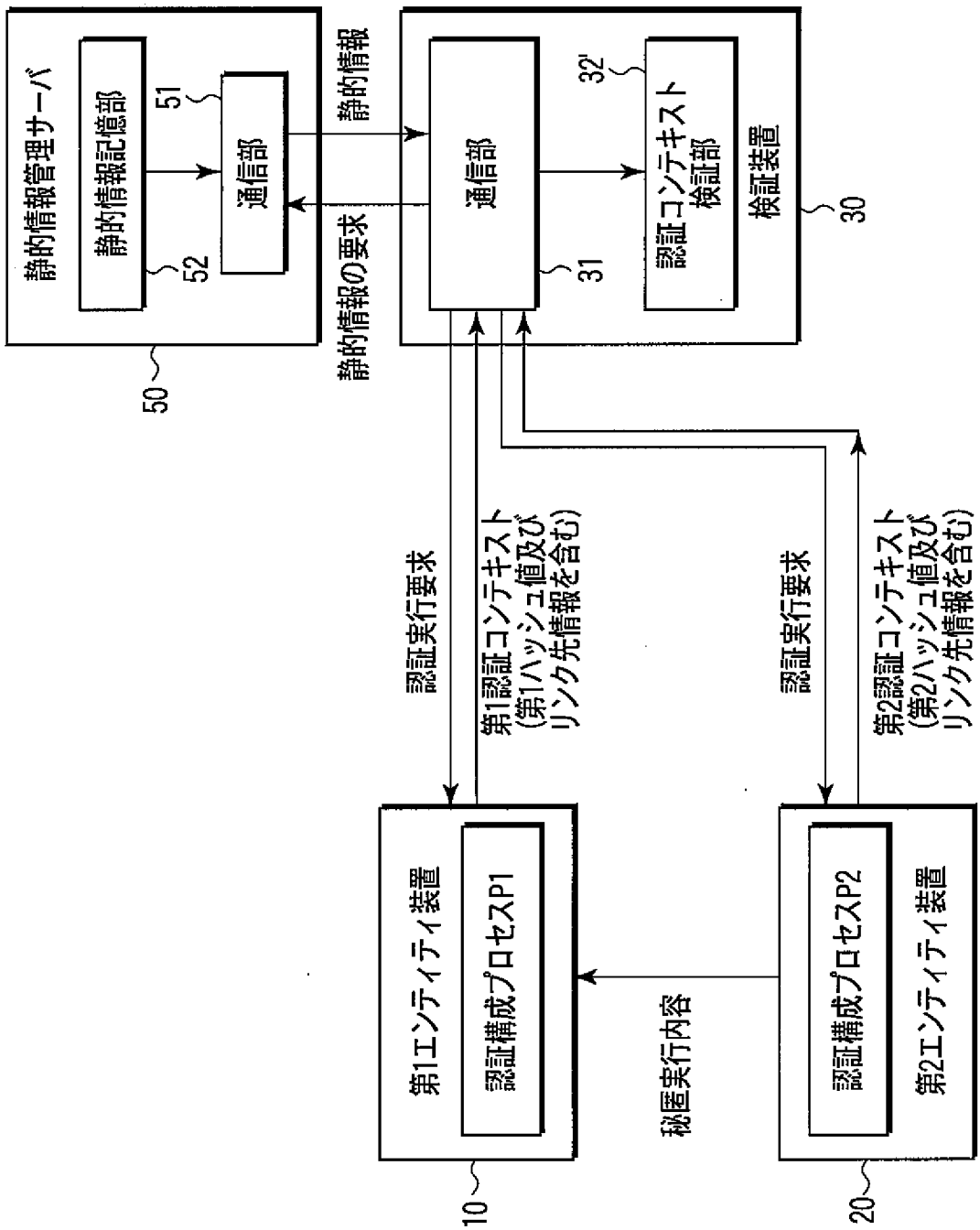
[図20B]


Ac1
ヘッダブロック
h1
リクエスタ
チャレンジ情報
データブロック
d1'''
静的情報リンク先情報
dLi
エンティティ評価レポート
のリンク先
エンティティの精度情報へ
のリンク先
テンプレート証明書への
リンク先
エンティティ情報(実行結果等)
dEn
照合の一致度
a1'''
認証子ブロック

[図21]


静的情報管理サーバ
52
静的情報記憶部
50
51
通信部
静的情報の要求
静的情報
10
第1エンティティ装置
認証構成プロセスP1
認証実行要求、
チャレンジ情報
31
通信部
第1及び第2認証コンテキスト
(チャレンジ情報及びリンク
先情報を含む)
32
認証コンテキスト
検証部
検証装置
30
第2認証コンテキスト(チャレンジ情報及びリンク先情報を含む)
認証構成プロセスP2
実行要求、チャレンジ情報
認証構成プロセスP2
第2エンティティ装置
20

[図22]


静的情報管理サーバ
静的情報記憶部
51
52
通信部
50
静的情報
静的情報の要求
通信部
31
32'
認証コンテキスト検証部
検証装置
30
認証実行要求
第1認証コンテキスト(第1ハッシュ値及びリンク先情報を含む)
認証実行要求
第2認証コンテキスト(第2ハッシュ値及びリンク先情報を含む)
第1エンティティ装置
認証構成プロセスP1
10
秘匿実行内容
認証構成プロセスP2
第2エンティティ装置
20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/313615

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G06F21/20*(2006.01)i, *G09C1/00*(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32, G06F21/20, G09C1/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-157224 A (KDDI Corp.), 31 May, 2002 (31.05.02), Full text (Family: none)	1-22
A	JP 2002-152196 A (NEC Corp.), 24 May, 2002 (24.05.02), Full text (Family: none)	1-22
A	JP 2001-202335 A (Hitachi, Ltd.), 27 July, 2001 (27.07.01), Full text (Family: none)	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 04 September, 2006 (04.09.06)	Date of mailing of the international search report 12 September, 2006 (12.09.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３１３６１５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G06F21/20(2006.01)i, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, G06F21/20, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

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

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００２－１５７２２４　Ａ（ケイディーディーアイ株式会社） ２００２．０５．３１，全文　（ファミリーなし）	１－２２
Ａ	ＪＰ　２００２－１５２１９６　Ａ（日本電気株式会社） ２００２．０５．２４，全文　（ファミリーなし）	１－２２
Ａ	ＪＰ　２００１－２０２３３５　Ａ（株式会社日立製作所） ２００１．０７．２７，全文　（ファミリーなし）	１－２２

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 ０４．０９．２００６	国際調査報告の発送日 １２．０９．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９４６９ 石田　信行 電話番号　０３－３５８１－１１０１　内線　３５４６