(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
2024年10月3日(03.10.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/201734 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *G06F 21/44* (2013.01)
H04L 9/32 (2006.01)

(21) 国際出願番号： PCT/JP2023/012602

(22) 国際出願日： 2023年3月28日(28.03.2023)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電気株式会社 (**NEC CORPORATION**) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP). 株式会社サイバーディフェンス研究所(**CYBER DEFENSE INSTITUTE,INC.**) [JP/JP]; 〒1010062 東京都千代田区神田駿河台２－５－１ Tokyo (JP).

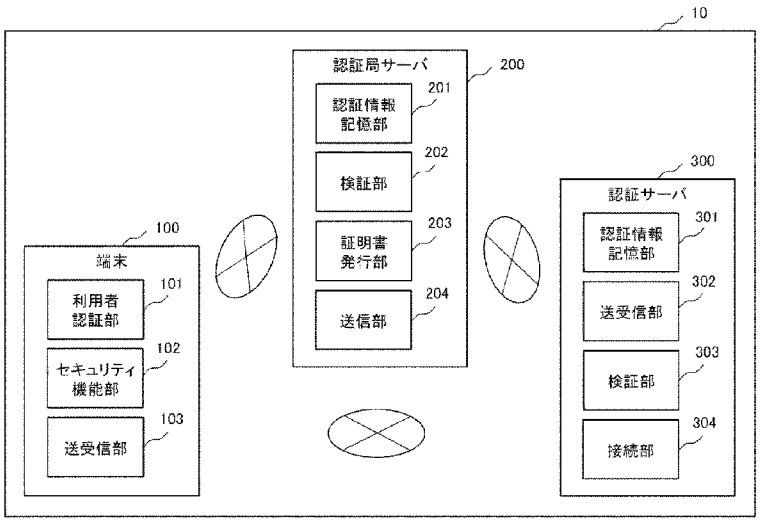
(72) 発明者: 永田 篤志 (**NAGATA Atsushi**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 富田 亨 (**TOMITA Toru**); 〒1010062 東京都千代田区神田駿河台２－５－１ 株式会社サイバーディフェンス研究所内 Tokyo (JP).

(74) 代理人: 北嶋 啓至, 外 (**KITAJIMA Hiroshi** et al.); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社 知的財産部門 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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU,

(54) **Title:** AUTHENTICATION SYSTEM, TERMINAL, AUTHENTICATION SERVER, AUTHENTICATION METHOD, AND RECORDING MEDIUM

(54) 発明の名称： 認証システム、端末、認証サーバ、認証方法、及び記録媒体



100 Terminal
101 User authentication unit
103 Security function unit
103, 302 Transceiver unit
200 Authentication station server
201, 301 Authentication information storage unit
202, 303 Verification unit
203 Certificate issuing unit
204 Transmission unit
300 Authentication server
304 Connection unit

(57) **Abstract:** An authentication system according to the present disclosure comprises a terminal and an authentication server for using a network system from the terminal. The terminal comprises: a security function means that generates a first private key corresponding to a user certificate that is linked to an endorsement key, and a second private key corresponding to a device certificate that is linked to an endorsement key, and signs prescribed data by using each of the private keys; and a transceiving means that transmits, through encrypted communication and to the authentication server, the signature data that was signed using each of the first private key and the second private key. The authentication server comprises: a verification means that verifies the signature data by using the user certificate and device certificate that were retained in advance; and a connection means that allows the terminal to connect to the network system if the user and device were able to be verified.

WO 2024/201734 A1

［続葉有］

LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能):ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

(57) 要約:本開示の認証システムは、端末と当該端末からネットワークシステムを利用するための認証サーバとを有する認証システムであって、端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、第一の秘密鍵及び第二の秘密鍵のそれぞれで署名された署名データを暗号通信により認証サーバに送信する、送受信手段と、を備え、認証サーバは、予め保持している利用者証明書及びデバイス証明書を用いて署名データを検証する、検証手段と、利用者及びデバイスを検証できた場合に、端末のネットワークシステムへの接続を可能にさせる、接続手段と、を備える。

明　細　書

発明の名称 ：

認証システム、端末、認証サーバ、認証方法、及び記録媒体

技術分野

[0001] 本開示は、認証システム、端末、認証サーバ、認証方法、及び記録媒体に関する。

背景技術

[0002] 利用者がネットワーク経由で認証システムへの認証を行う場合に、利用者や端末の情報を用いて認証する技術がある。

[0003] 特許文献１には、利用者が自身の秘密鍵で認証サーバから送信されたノンスに署名したかどうかを検証することで、利用者を認証する方法が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特表２０２２－５３０１３６号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、特許文献１に記載された発明は、認証を行う際に、利用者が入力した、ＰＩＮ（Personal Identification Number）コードをノンスとともに認証サーバに送信している。このため、認証時に用いられる認証情報の秘密が確保されていない。したがって、認証情報がネットワーク上で窃取された場合、認証サーバは利用者又は端末のなりすましの検出を行うことが困難である。

[0006] 本開示の目的の一例は、ネットワーク経由での認証において、利用者及び端末の秘密情報を保護しながら、利用者及び端末の真正性を検証することが可能な認証システムを提供することにある。

課題を解決するための手段

[0007] 本開示の一態様における認証システムは、端末と当該端末からネットワークシステムを利用するための認証サーバとを有する認証システムであって、端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、第一の秘密鍵及び第二の秘密鍵のそれぞれで署名された署名データを暗号通信により認証サーバに送信する、送受信手段と、を備え、認証サーバは、予め保持している利用者証明書及びデバイス証明書を用いて署名データを検証する、検証手段と、利用者及びデバイスを検証できた場合に、端末のネットワークシステムへの接続を可能にさせる、接続手段と、を備える。

[0008] 本開示の一態様における端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、第一の秘密鍵及び第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、送受信手段と、を備える。

[0009] 本開示の一態様における認証サーバは、認証対象の端末から受信した、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している利用者証明書及びデバイス証明書を用いて、利用者及びデバイスを検証する、検証手段と、利用者とデバイスを検証できた場合に、端末のネットワークシステムへの接続を可能にさせる、接続手段とを備える。

[0010] 本開示の一態様における認証方法は、認証サーバがネットワークシステムを利用する端末を認証する認証方法あって、端末は、エンドースメントキー

に紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、第一の秘密鍵及び第二の秘密鍵でそれぞれ署名された署名データを暗号通信により認証サーバに送信し、認証サーバは、予め保持している利用者証明書及びデバイス証明書を用いて署名データを検証し、検証できた場合に、端末のネットワークシステムへの接続を可能にさせる。

[0011] 本開示の一態様における記録媒体は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、第一の秘密鍵及び第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、ことをコンピュータに実行させるプログラムを格納する。

[0012] 本開示の一態様における記録媒体は、認証対象の端末から受信した、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している利用者証明書及びデバイス証明書を用いて検証し、検証できた場合に、端末のネットワークシステムへの接続を可能にさせる、ことをコンピュータに実行させるプログラムを格納する。

発明の効果

[0013] 本開示による効果の一例によれば、利用者の秘密情報と利用者端末の秘密情報を保護しながら、利用者及び端末の真正性を検証することが可能となる。

図面の簡単な説明

[0014] [図1]図１は、本開示における認証システムの構成を示すブロック図である。

[図2]図２は、本開示における端末、認証局サーバ及び認証サーバをコンピュ

ータ装置とその周辺装置で実現したハードウェア構成を示す図である。

[図3]図３は、本開示における認証システムの動作を示すフローチャートである。

[図4]図４は、本開示における認証システムの動作を示すフローチャートである。

発明を実施するための形態

[0015] 次に、実施形態について図面を参照して詳細に説明する。

[0016] ［第一の実施形態］

図１は、本開示における認証システム１０の構成を示すブロック図である。認証システム１０は、端末１００、認証局サーバ２００及び認証サーバ３００を有し、これらは互いにネットワークを介して接続されている。図１では、端末１００単体が図示されているが、ネットワークシステムに接続を行う複数の端末１００が存在していてもよい。ネットワークシステムとは、ネットワーク上で利用するサービス又はシステムを含む。認証システム１０は、ネットワークシステムに接続する際の利用者及び端末の真正性を検証するためのシステムである。真正性とは、例えば、なりすましの利用者や端末ではなく、本物の利用者及び端末であることを確かめるための性質を指す。

[0017] 図２は、本開示の第一の実施形態における端末１００、認証局サーバ２００及び認証サーバ３００のそれぞれを、プロセッサを含むコンピュータ装置５００で実現したハードウェア構成の一例を示す図である。図２に示されるように、端末１００、認証局サーバ２００及び認証サーバ３００は、それぞれＣＰＵ(Central Processing Unit)５０１、ＲＯＭ（Read Only Memory）５０２、ＲＡＭ（Random Access Memory）５０３等のメモリ、プログラム５０４を格納するハードディスク等の記憶装置５０５、ネットワーク接続用の通信Ｉ／Ｆ（Interface）５０８、データの入出力を行う入出力インターフェース５１１を含む。第一の実施形態において、端末１００、認証局サーバ２００及び認証サーバ３００は、バス５１２を介して各構成部と接続されている。

[0018] ＣＰＵ５０１は、ＯＳを動作させて本発明の第一の実施の形態に係る端末１００、認証局サーバ２００及び認証サーバ３００をそれぞれ制御する。また、ＣＰＵ５０１は、例えばドライブ装置５０７などに装着された記録媒体５０６からメモリにプログラムやデータを読み出す。また、ＣＰＵ５０１は、第一の実施の形態における端末１００、認証局サーバ２００及び認証サーバ３００が備える各構成部の実現手段及びこれらの一部として機能し、プログラムに基づいて後述する図３及び図４に示すフローチャートにおける処理または命令を実行する。

[0019] 記録媒体５０６は、例えば光ディスク、フレキシブルディスク、磁気光ディスク、外付けハードディスク、または半導体メモリ等である。記憶装置の一部の記録媒体は、不揮発性記憶装置であり、そこにプログラムを記録する。また、プログラムは、通信網に接続されている図示しない外部コンピュータからダウンロードされてもよい。

[0020] 入力装置５０９は、例えば、マウスやキーボード、内蔵のキーボタンなどで実現され、入力操作に用いられる。入力装置５０９は、マウスやキーボード、内蔵のキーボタンに限らず、例えばタッチパネルでもよい。出力装置５１０は、例えばディスプレイで実現され、出力を確認するために用いられる。

[0021] 以上のように、図１の端末１００、認証局サーバ２００及び認証サーバ３００は、図２に示されるコンピュータ・ハードウェアによって実現される。ただし、端末１００、認証局サーバ２００及び認証サーバ３００の各構成部の実現手段は、本明細書で説明した構成に限定されない。

[0022] ＜証明書登録＞

まず、認証に用いる利用者証明書及びデバイス証明書を認証サーバ３００に登録する方法について説明する。

[0023] （端末１００）

図１に示すように、端末１００は、ネットワークシステムを利用するためのデバイスである。図１に示すように、利用者認証部１０１と、セキュリテ

ィ機能部１０２と送受信部１０３と、を備える。

[0024] 利用者認証部１０１は、利用者を識別する識別情報を照合する。識別情報とは、静脈、指紋、手のひら、虹彩、音声、顔、等の一若しくは複数の生体情報、又は、ＰＩＮコードを含む。利用者認証部１０１は、利用者から入力された識別情報を受付する。また、利用者認証部１０１は、識別情報を格納したＩＣカード内のデータを読み取ることで、利用者の識別情報を取得してもよい。また、利用者認証部１０１は入力された識別情報と、端末１００内に格納されている利用者の識別情報とを照合し、照合できた場合に端末１００にサインインする。

[0025] セキュリティ機能部１０２は、耐タンパー性を持った記憶領域を含む。セキュリティ機能部１０２は、悪意を持った第三者による改ざんが難しい領域である。セキュリティ機能部１０２は、ハードウェア暗号モジュールで構成され、一例としては、ＴＰＭ（Trusted Platform Module）であるが、耐タンパー性を実現できる構成であればこれに限らない。ＴＰＭは、ＯＳやハードウェア、外部からの物理ハッキングに対して改ざんが難しい特性をもつため、耐タンパー性が高い。

[0026] セキュリティ機能部１０２には、端末１００の製造過程で封入されたエンドースメントキーが格納されている。エンドースメントキーは、ハードウェア暗号モジュール毎に固有の識別子が付与され、ハードウェア暗号モジュールを識別するために用いられる。

[0027] セキュリティ機能部１０２は、乱数生成回路を用いてネットワークシステムの認証のための利用者証明書に対応した第一の秘密鍵及び第一の公開鍵のペアと、デバイス証明書に対応した第二の秘密鍵及び第二の公開鍵のペアをそれぞれ生成する。利用者証明書及びデバイス証明書は、それぞれエンドースメントキーに紐づけされている。第一の秘密鍵及び第一の公開鍵のペアは、利用者の検証に利用され、第二の秘密鍵及び第二の公開鍵のペアは、端末１００の検証に利用される。秘密鍵のそれぞれは、例えば、ＡＩＫ（Attestation Identity Key）における秘密鍵であり、認証サーバ３００に格納され

る利用者証明書及びデバイス証明書とそれぞれ対になっている。各セキュリティ機能部１０２は、生成した秘密鍵のそれぞれをハードウェア暗号モジュールの保存領域に格納する。送信部１１３は、生成した公開鍵のそれぞれを認証局サーバ２００に送信する。

[0028] （認証局サーバ２００）

図１に示すように、認証局サーバ２００は、認証情報記憶部２０１と検証部２０２と証明書発行部２０３と送信部２０４を備える。

[0029] 認証情報記憶部２０１は、端末１００のエンドースメントキー証明書を格納する。エンドースメントキー証明書は、エンドースメントキーの情報を含み、端末１００又は端末１００のベンダーから受信したものである。

[0030] 検証部２０２は、端末１００から受信した第二の公開鍵に含まれるエンドースメントキーの情報を、エンドースメントキー証明書を用いて公知の方法で端末１００の実存性を検証する。検証部２０２は、端末１００の実存性を検証できた場合、第一及び第二の公開鍵を証明書発行部２０３に出力する。一方、検証部２０２は、検証できなかった場合、その旨を端末１００に通知する。

[0031] 証明書発行部２０３は、第二の公開鍵を検証できた場合、第二の公開鍵に認証局の署名生成鍵によって署名を付与してデバイス証明書を発行する。また、同様に、第一の公開鍵に認証局の署名生成鍵によって署名を付与して利用者証明書を発行する。証明書発行部２０３は、例えば、Ｘ．５０９に基づきこれらの証明書を発行する。証明書発行部２０３は、各証明書に有効期間を設定しもよい。

[0032] 送信部２０４は、発行したデバイス証明書及び利用者証明書を認証サーバ３００に送信する。なお、各証明書は、セキュリティを高めるために、所定の方法で暗号化されていてもよい。また、送信部２０４は、デバイス証明書及び利用者証明書の登録が完了したことを端末１００に通知する。

[0033] ＜認証＞

次に、認証サーバ３００に登録された利用者証明書及びデバイス証明書を

用いて、利用者及びデバイスを認証する方法を説明する。

[0034]（端末１００）

利用者認証部１０１は、利用者から入力された識別情報を受付すると、入力された識別情報と、端末１００内に格納されている利用者の識別情報とを照合し、照合できた場合に、入力された識別情報で端末１００にサインインする。また、利用者認証部１０１は、利用者及び端末１００の検証を要求する認証要求を認証サーバ３００に送信する。利用者認証部１０１は、ＳＳＬ(Secure Sockets Layer)又はＴＬＳ(Transport Layer Security)等の暗号通信を利用して認証要求を送信する。

[0035] セキュリティ機能部１０２は、所定のデータに対して、利用者証明書に対応した第一の秘密鍵及びデバイス証明書に対応した第二の秘密鍵のそれぞれの秘密鍵を用いて署名を行う。具体的に、まず、セキュリティ機能部１０２は、第一の秘密鍵又は第二の秘密鍵のいずれか一方の鍵を用いて、認証サーバ３００から送信されるノンスに対して署名し、送受信部１０３が署名データを認証サーバ３００に送信する。その後、セキュリティ機能部１０２は、認証サーバ３００から再度送信された署名済のノンスに対して、他方の秘密鍵を用いて署名を行う。

[0036] 送受信部１０３は、認証サーバ３００から暗号通信により送信されたノンスを受信する。また、それぞれの秘密鍵で署名された署名データを暗号通信で認証サーバ３００に送信する。

[0037]（認証サーバ３００）

認証サーバ３００は、認証情報記憶部３０１と送受信部３０２と検証部３０３と接続部３０４を備える。認証情報記憶部３０１は、ネットワークシステムの認証のための利用者証明書及びデバイス証明書を紐づけて格納している。これらの証明書は、認証局サーバ２００で発行されたものであり、端末１００から受信した署名データを検証するため証明書である。

[0038] 送受信部３０２は、端末１００から認証要求を受信すると、暗号通信によりノンスを端末１００に送信する。また、送受信部３０２は、いずれかの秘

密鍵で署名された署名データを受信した場合は、署名付きのノンスを端末１００に対して暗号通信により送信する。送受信部３０２は、第一及び第二の両方の秘密鍵で署名された署名データを受信した場合は、署名データを検証部３０３に出力する。

[0039] 検証部３０３は、利用者証明書及びデバイス証明書を用いて署名データを検証する。検証部３０３による検証方法は、公知の方法で行われ、例えば、各証明書で記された公開鍵を利用して署名データを復号することで利用者及びデバイスを検証する。なお、検証部３０３は、各証明書に有効期間が設定されている場合は、有効期間内であるか否かも検証する。

[0040] 接続部３０４は、利用者及びデバイスを検証できた場合、端末１００とネットワークシステム間のネットワークを制御して端末１００のネットワークシステムへの接続を可能にさせる。接続部３０４は、利用者及びデバイスの少なくともいずれかが検証ができなかった場合、その旨を端末１００に通知する。

[0041] ＜フローチャート＞

図３及び図４は、本開示における認証システム１０の動作の概要を示すフローチャートである。これらのフローチャートによる処理は、前述したプロセッサによるプログラム制御に基づいて、実行されてもよい。なお、図３のフローチャートは、利用者証明書及びデバイス証明書を認証サーバ３００に登録する際の動作であり、図４のフローチャートは、利用者及び端末１００の認証を実行する際の動作である。

[0042] まず、利用者証明書及びデバイス証明書の登録の動作を説明する。図３に示すように、まず、端末１００において、利用者認証部１０１は、利用者から入力された識別情報で端末１００にサインインする（ステップＳ１０１）。次に、セキュリティ機能部１０２は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵及び第一の公開鍵のペアと、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵及び第二の公開鍵のペアをそれぞれ生成する（ステップＳ１０２）。セキュリテ

ィ機能部１０２は、生成した第一及び第二の秘密鍵のそれぞれをセキュリティ機能部１０２に格納し、送受信部１０３は、第一及び第二の公開鍵のそれぞれを認証局サーバ２００に送信する（ステップＳ１０３）。認証局サーバ２００は、端末１００から第一及び第二の公開鍵を受信すると、検証部２０２が第二の公開鍵に含まれるエンドースメントキーを検証する（ステップＳ１０４）。検証できた場合（Ｓ１０５；ＹＥＳ）、証明書発行部２０３が、利用者証明書及びデバイス証明書を発行し（ステップＳ１０６）、送信部２０４が、認証サーバ３００に送信する（ステップＳ１０７）、また、送信部２０４は、証明書の登録が完了したことを通知する（ステップＳ１０８）。一方、検証が成功しなかった場合（Ｓ１０５；ＮＯ）、送信部２０４は、検証が失敗したことを通知する（ステップＳ１０９）。最後に、端末１００の出力装置５１０に認証失敗又は証明書の登録が完了したことを表示する（ステップＳ１１０）。以上で、認証システム１０は、利用者証明書及びデバイス証明書の登録の動作を終了する。

[0043] 次に、利用者と端末１００の認証の動作について説明する。図４に示すように、まず、端末１００の利用者認証部１０１は、利用者から入力された識別情報で端末１００にサインインし（ステップＳ１１１）、認証サーバ３００に認証要求を送信する（ステップＳ１１２）。次いで、認証サーバ３００において、送受信部３０２は、ノンスを端末１００に送信する（ステップＳ１１３）。次いで、端末１００において、セキュリティ機能部１０２は、第一の秘密鍵又は第二の秘密鍵のいずれか一方の鍵を用いてノンスに対して署名し（ステップＳ１１４）、署名データを認証サーバ３００に送信する（ステップＳ１１５）。次いで、認証サーバ３００は、いずれかの秘密鍵で署名済の署名データを端末１００に再度送信し（ステップＳ１１６）、セキュリティ機能部１０２は、他方の秘密鍵を用いてノンスに署名を行い（ステップＳ１１７）、認証サーバ３００に再度送信する（ステップＳ１１８）。

[0044] 次に、検証部３０３は、両方の秘密鍵で署名された署名データを受信すると、署名データを利用者証明書及びデバイス証明書を用いて検証する（ステ

ップＳ１１９）。検証できた場合（Ｓ１２０；ＹＥＳ）、接続部３０４は、端末１００のネットワークシステムへの接続を可能にさせる（ステップＳ１２１）。一方、検証できなかった場合（Ｓ１２０；ＮＯ）、送受信部３０２は、端末１００に認証が失敗した旨を通知し（ステップＳ１２２）、端末１００の出力装置５１０に認証が失敗したことを表示する（ステップＳ１２３）。以上で、認証システム１０は、利用者とデバイスの認証の動作を終了する。

[0045] 本実施形態では、利用者と端末１００の認証の動作において、端末１００のセキュリティ機能部１０２が、認証サーバ３００から送信されるノンスに対して、利用者証明書に対応した第一の秘密鍵及びデバイス証明書に対応した第二の秘密鍵のそれぞれの秘密鍵を用いて署名を行い、認証サーバ３００の検証部３０３が、利用者証明書及びデバイス証明書を用いて署名データを検証する。これにより、本物の利用者及びデバイスを用いてネットワークシステムにアクセスしていることを検証可能である。したがって、利用者及び端末１００のなりすましがなされていないことを検証できる。

[0046] また、本実施形態では、認証システム１０は、利用者及び端末１００に関する情報を用いずに、ノンスを各秘密鍵により署名した署名データとこれらの証明書を用いて検証を行っている。よって、被認証者となる利用者の秘密情報と端末１００の秘密情報を保護しながら、検証が可能である。

[0047] 以上より、本実施形態によれば、利用者及び端末１００の秘密情報を保護しながら、利用者及び端末の真正性を検証することが可能となる。

[0048] また、本実施形態では、利用者証明書及びデバイス証明書やこれらに対応する秘密鍵に、ハードウェア暗号モジュールを識別するエンドースメントキーが紐づけられている。これにより、端末１００の真正性の検証だけではなく、端末１００が実在していることの実存性の検証も可能である。

[0049] ［第一の実施形態の変形例］

本開示の第一の実施形態の変形例について説明する。上述した第一の実施形態では、第一の秘密鍵及び第二の秘密鍵のいずれかの一方の秘密鍵を用い

て署名を行う際にデータをやり取りする暗号通信と、他方の秘密鍵を用いて署名を行う際にデータをやり取りする暗号通信が同一であった。これに対し、各署名を行う際のデータのやり取りに別の暗号通信を用いてもよい。すなわち、セキュリティ機能部１０２は、ネットワークシステムへの接続時に認証サーバ３００から第一の暗号通信により受信したノンスに対して、第一の秘密鍵及び第二の秘密鍵のいずれかの一方の秘密鍵を用いて署名を行い、送受信部１０３を介して第一の暗号通信により署名データを認証サーバ３００に送信する。また、セキュリティ機能部１０２は、認証サーバ３００から第二の暗号通信により受信した署名データ付きのノンスに対して、他方の秘密鍵を用いて署名を行い、送受信部１０３を介して第二の暗号通信により認証サーバ３００に第一の秘密鍵及び第二の秘密鍵で署名された署名データを送信する。

[0050] また、セキュリティ機能部１０２は、ネットワークシステムへの接続時に認証サーバ３００から受信したノンスに対して、第一の秘密鍵と第二の秘密鍵とが集約された集約署名を用いて署名を行ってもよい。集約署名としては、例えば、Schnorr署名を用いることができる。この場合、署名データを送信する際のデータをやり取りする回数を減らすことができ、ネットワークの伝送負荷を低減することができる。

[0051] ［適用例］

本開示の認証システム１０を適用可能なネットワークシステムとしては、例えば、自動運転システムが挙げられる。この場合、認証システム１０は、利用者と利用者の自動車に搭載された端末１００の真正性を検証することで、利用者の認証を行う。このシステムでは、利用者が認証されると、利用者が自身の自動車で自動運転システムを利用することができる。

[0052] 本開示の認証システム１０を適用可能な他のネットワークシステムとしては、自動車のレンタルシステムが挙げられる。このネットワークシステムにおいて、利用者証明書には、有効期間に関する情報が含まれており、自動車のレンタル時間に対応した有効期間が設定されている。この場合、認証シス

テム１０は、利用者と利用者が利用する自動車に搭載された端末１００の真正性を検証するとともに、利用者証明書が有効期間か否かを検証する。このシステムによれば、利用者証明書が有効期間内であるときのみ利用者の認証がなされ、レンタルした時間内のみ自動車を運転するためのシステムへの接続が可能となる。

[0053] 以上、各実施の形態を参照して本発明を説明したが、本発明は上記実施の形態に限定されるものではない。本発明の構成や詳細には、本発明のスコープ内で当業者が理解しえる様々な変更をすることができる。例えば、複数の動作をフローチャートの形式で順番に記載してあるが、その記載の順番は複数の動作を実行する順番を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の順番は内容的に支障しない範囲で変更することができる。

[0054] 上記の実施の形態の一部または全部は、以下の付記のようにも記載されることができる。ただし、上記の実施の形態の一部または全部は、以下に限られない。

[0055] （付記１）

端末と当該端末からネットワークシステムを利用するための認証サーバとを有する認証システムであって、

前記端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、

前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により前記認証サーバに送信する、送受信手段と、を備え、

前記認証サーバは、予め保持している前記利用者証明書及び前記デバイス証明書を用いて前記署名データを検証する、検証手段と、

利用者及びデバイスを検証できた場合に、前記端末の前記ネットワークシステムへの接続を可能にさせる、接続手段と、を備える、認証システム。

[0056]（付記２）

前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから暗号通信により受信したノンスに対して、前記第一の秘密鍵及び前記第二の秘密鍵のいずれかの一方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記認証サーバに署名データを暗号通信により送信し、

前記署名データの送信後、前記認証サーバから前記暗号通信により受信した署名データ付きのノンスに対して、他方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記認証サーバに前記第一の秘密鍵及び前記第二の秘密鍵で署名された署名データを前記暗号通信により送信する、付記１に記載の認証システム。

[0057]（付記３）

前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから第一の暗号通信により受信したノンスに対して、前記第一の秘密鍵及び前記第二の秘密鍵のいずれかの一方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記第一の暗号通信により前記認証サーバに署名データを送信し、

前記署名データの送信後、前記認証サーバから第二の暗号通信により受信した署名データ付きのノンスに対して、他方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記第二の暗号通信により前記認証サーバに前記第一の秘密鍵及び前記第二の秘密鍵で署名された署名データを送信する、付記１に記載の認証システム。

[0058]（付記４）

前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから暗号通信により受信したノンスに対して、前記第一の秘密鍵と前記第二の秘密鍵とが集約された秘密鍵を用いて署名を行う、付記１に記載の認証システム。

[0059]（付記５）

前記利用者証明書は、有効期間に関する情報を含み、

前記認証サーバは、前記有効期間内にのみ、前記端末の前記ネットワークシステムへの接続を許可する、付記１～４のいずれかに記載の認証システム。

[0060]（付記６）

前記認証システムは、認証局サーバを更に含み、

前記認証局サーバは、前記端末から前記デバイス証明書の発行が要求された場合に、前記端末の実存性を検証する、検証手段と、

実存性が確認できた場合に、前記利用者証明書及び前記デバイス証明書を発行する、証明書発行手段と、を備える、付記１～５いずれかに記載の認証システム。

[0061]（付記７）

前記ネットワークシステムは、自動運転システムである、付記１～６のいずれかに記載の認証システム。

[0062]（付記８）

前記ネットワークシステムは、自動車のレンタルシステムであり、前記利用者証明書は、レンタル時間に対応した有効期間が設定されている。付記１～６のいずれかに記載の認証システム。

[0063]（付記９）

エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、

前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、送受信手段と、を備える、端末。

[0064]（付記１０）

認証対象の端末から受信した、エンドースメントキーに紐づけされた利用

者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している前記利用者証明書及び前記デバイス証明書を用いて、利用者及びデバイスを検証する、検証手段と、

利用者とデバイスを検証できた場合に、前記端末のネットワークシステムへの接続を可能にさせる、接続手段とを備える、認証サーバ。

[0065]（付記１１）

認証サーバがネットワークシステムを利用する端末を認証する認証方法あって、

前記端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、

前記第一の秘密鍵及び前記第二の秘密鍵でそれぞれ署名された署名データを暗号通信により前記認証サーバに送信し、

前記認証サーバは、予め保持している前記利用者証明書及び前記デバイス証明書を用いて前記署名データを検証し、

検証できた場合に、前記端末の前記ネットワークシステムへの接続を可能にさせる、認証方法。

[0066]（付記１２）

エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、

前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、ことをコンピュータに実行させるプログラムを格納する記録媒体。

[0067]（付記１３）

認証対象の端末から受信した、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している前記利用者証明書及び前記デバイス証明書を用いて検証し、検証できた場合に、前記端末のネットワークシステムへの接続を可能にさせる、ことをコンピュータに実行させるプログラムを格納する記録媒体。

符号の説明

[0068]

１０　認証システム
１００　端末
１０１　利用者認証部
１０２　セキュリティ機能部
１０３　送受信部
２００　認証局サーバ
２０１　認証情報記憶部
２０２　検証部
２０３　証明書発行部
２０４　送信部
３００　認証サーバ
３０１　認証情報記憶部
３０２　送受信部
３０３　検証部
３０４　接続部
５００　コンピュータ装置
５０１　ＣＰＵ
５０２　ＲＯＭ
５０３　ＲＡＭ
５０４　プログラム

５０５	記憶装置
５０６	記録媒体
５０７	ドライブ装置
５０８	通信インターフェース
５０９	入力装置
５１０	出力装置
５１１	入出力インターフェース
５１２	バス

請求の範囲

[請求項1] 端末と当該端末からネットワークシステムを利用するための認証サーバとを有する認証システムであって、

前記端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、

前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により前記認証サーバに送信する、送受信手段と、を備え、

前記認証サーバは、予め保持している前記利用者証明書及び前記デバイス証明書を用いて前記署名データを検証する、検証手段と、

利用者及びデバイスを検証できた場合に、前記端末の前記ネットワークシステムへの接続を可能にさせる、接続手段と、を備える、認証システム。

[請求項2] 前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから暗号通信により受信したノンスに対して、前記第一の秘密鍵及び前記第二の秘密鍵のいずれかの一方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記認証サーバに署名データを暗号通信により送信し、

前記署名データの送信後、前記認証サーバから前記暗号通信により受信した署名データ付きのノンスに対して、他方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記認証サーバに前記第一の秘密鍵及び前記第二の秘密鍵で署名された署名データを前記暗号通信により送信する、請求項１に記載の認証システム。

[請求項3] 前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから第一の暗号通信により受信したノンスに対し

て、前記第一の秘密鍵及び前記第二の秘密鍵のいずれかの一方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記第一の暗号通信により前記認証サーバに署名データを送信し、

前記署名データの送信後、前記認証サーバから第二の暗号通信により受信した署名データ付きのノンスに対して、他方の秘密鍵を用いて署名を行い、前記送受信手段を介して前記第二の暗号通信により前記認証サーバに前記第一の秘密鍵及び前記第二の秘密鍵で署名された署名データを送信する、請求項１に記載の認証システム。

[請求項4] 前記セキュリティ機能手段は、前記ネットワークシステムへの接続時に前記認証サーバから暗号通信により受信したノンスに対して、前記第一の秘密鍵と前記第二の秘密鍵とが集約された秘密鍵を用いて署名を行う、請求項１に記載の認証システム。

[請求項5] 前記利用者証明書は、有効期間に関する情報を含み、

前記認証サーバは、前記有効期間内にのみ、前記端末の前記ネットワークシステムへの接続を許可する、請求項１～４のいずれか一項に記載の認証システム。

[請求項6] 前記認証システムは、認証局サーバを更に含み、

前記認証局サーバは、前記端末から前記デバイス証明書の発行が要求された場合に、前記端末の実存性を検証する、検証手段と、

実存性が確認できた場合に、前記利用者証明書及び前記デバイス証明書を発行する、証明書発行手段と、を備える、請求項１～５いずれか一項に記載の認証システム。

[請求項7] 前記ネットワークシステムは、自動運転システムである、請求項１～６のいずれか一項に記載の認証システム。

[請求項8] 前記ネットワークシステムは、自動車のレンタルシステムであり、前記利用者証明書は、レンタル時間に対応した有効期間が設定されている。請求項１～６のいずれか一項に記載の認証システム。

[請求項9] エンドースメントキーに紐づけされた利用者証明書に対応した第一

の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名する、セキュリティ機能手段と、

前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、送受信手段と、を備える、端末。

[請求項10] 認証対象の端末から受信した、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している前記利用者証明書及び前記デバイス証明書を用いて、利用者及びデバイスを検証する、検証手段と、

利用者とデバイスを検証できた場合に、前記端末のネットワークシステムへの接続を可能にさせる、接続手段とを備える、認証サーバ。

[請求項11] 認証サーバがネットワークシステムを利用する端末を認証する認証方法あって、

前記端末は、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、

前記第一の秘密鍵及び前記第二の秘密鍵でそれぞれ署名された署名データを暗号通信により前記認証サーバに送信し、

前記認証サーバは、予め保持している前記利用者証明書及び前記デバイス証明書を用いて前記署名データを検証し、

検証できた場合に、前記端末の前記ネットワークシステムへの接続を可能にさせる、認証方法。

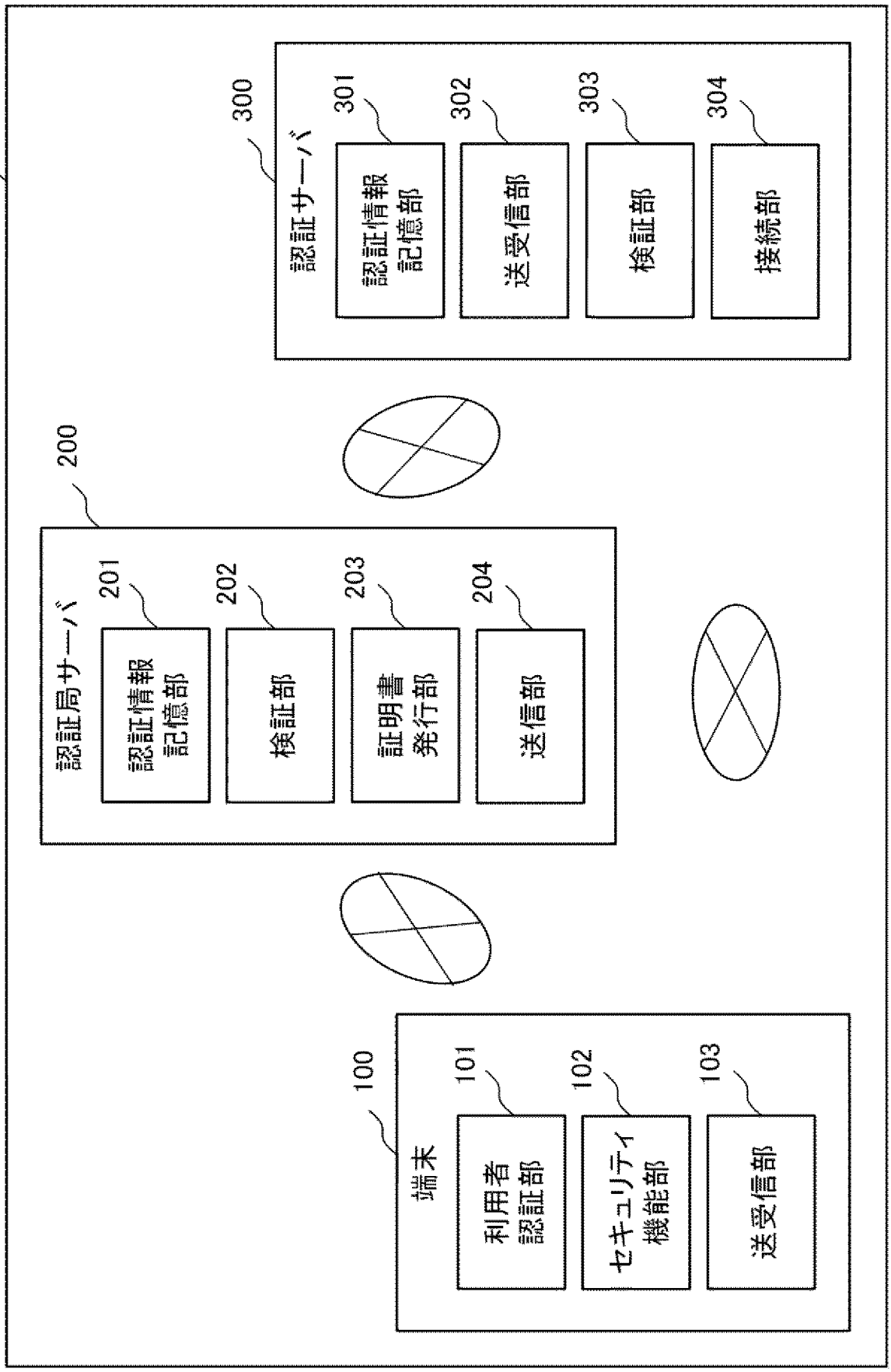
[請求項12] エンドースメントキーに紐づけされた利用者証明書に対応した第一

の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれを生成し、所定のデータに対して、それぞれの秘密鍵を用いて署名し、

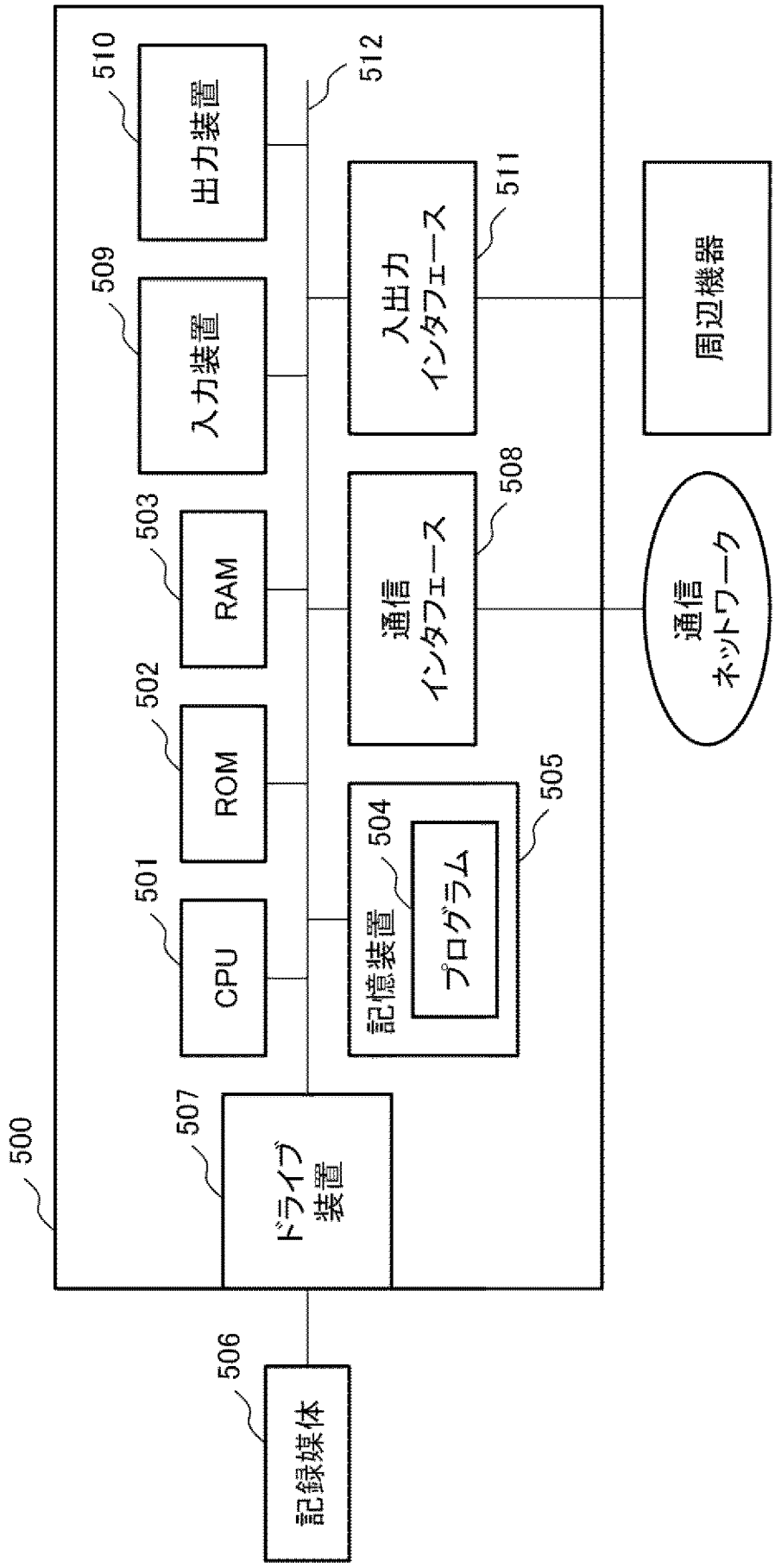
前記第一の秘密鍵及び前記第二の秘密鍵のそれぞれで署名された署名データを暗号通信により利用者及びデバイスを認証する認証サーバに送信する、ことをコンピュータに実行させるプログラムを格納する記録媒体。

[請求項13] 認証対象の端末から受信した、エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵、及び、前記エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵のそれぞれで署名された署名データについて、予め保持している前記利用者証明書及び前記デバイス証明書を用いて検証し、検証できた場合に、前記端末のネットワークシステムへの接続を可能にさせる、ことをコンピュータに実行させるプログラムを格納する記録媒体。

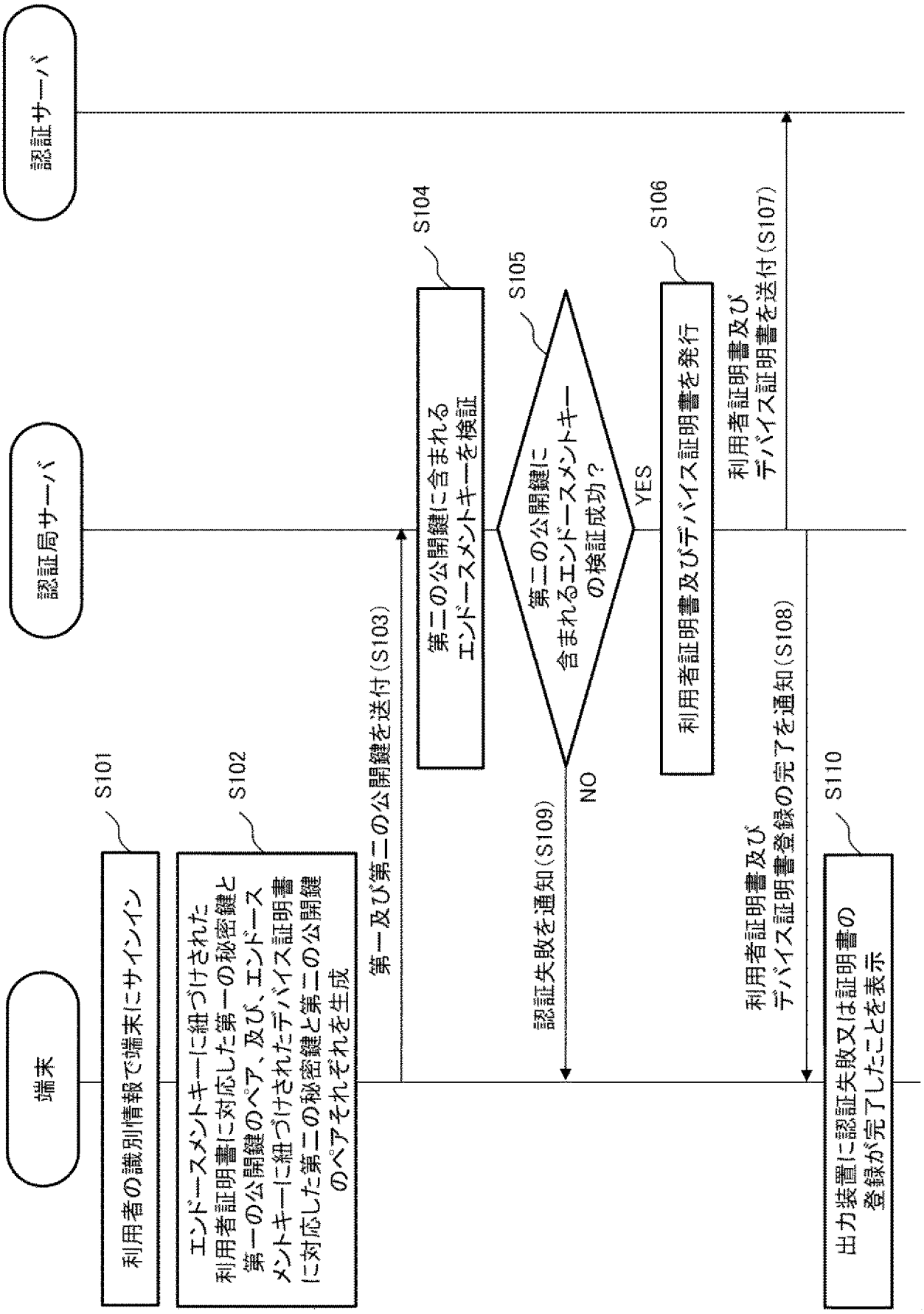
[図1]


10
300
認証サーバ
301
認証情報記憶部
302
送受信部
303
検証部
304
接続部
200
認証局サーバ
201
認証情報記憶部
202
検証部
203
証明書発行部
204
送信部
100
端末
101
利用者認証部
102
セキュリティ機能部
103
送受信部

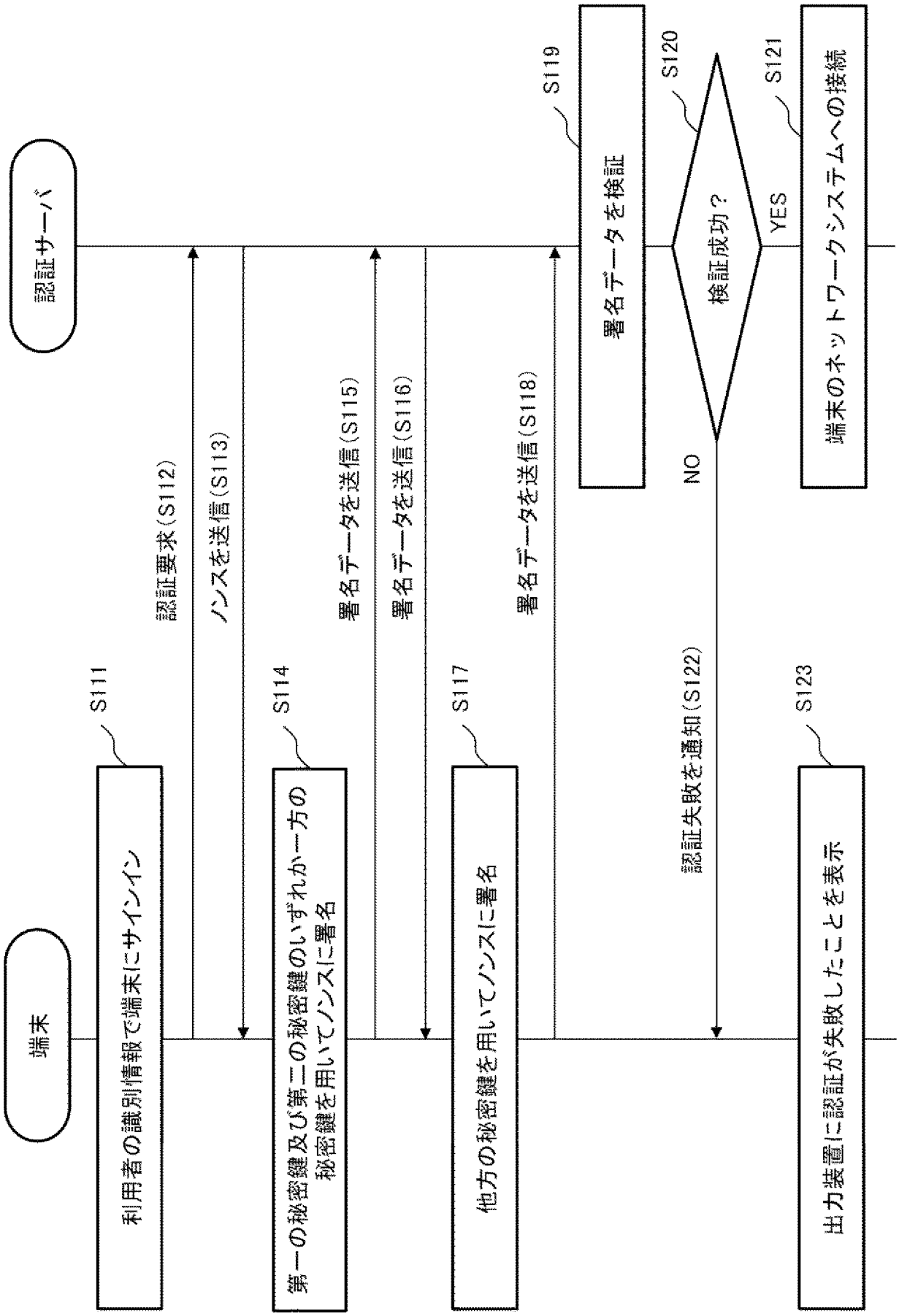
[図2]


500
506
記録媒体
507
ドライブ装置
501
CPU
502
ROM
503
RAM
509
入力装置
510
出力装置
504
記憶装置
プログラム
505
512
通信インタフェース
508
入出力インタフェース
511
通信ネットワーク
周辺機器

[図3]


端末
認証局サーバ
認証サーバ
S101
利用者の識別情報で端末にサインイン
S102
エンドースメントキーに紐づけされた利用者証明書に対応した第一の秘密鍵と第一の公開鍵のペア、及び、エンドースメントキーに紐づけされたデバイス証明書に対応した第二の秘密鍵と第二の公開鍵のペアそれぞれを生成
第一及び第二の公開鍵を送付(S103)
S104
第二の公開鍵に含まれるエンドースメントキーを検証
S105
第二の公開鍵に含まれるエンドースメントキーの検証成功？
YES
NO
S106
利用者証明書及びデバイス証明書を発行
利用者証明書及びデバイス証明書を送付(S107)
認証失敗を通知(S109)
利用者証明書及びデバイス証明書登録の完了を通知(S108)
S110
出力装置に認証失敗又は証明書の登録が完了したことを表示

[図4]


端末
認証サーバ
S111
利用者の識別情報で端末にサインイン
認証要求(S112)
ノンスを送信(S113)
S114
第一の秘密鍵及び第二の秘密鍵のいずれか一方の秘密鍵を用いてノンスに署名
署名データを送信(S115)
署名データを送信(S116)
S117
他方の秘密鍵を用いてノンスに署名
署名データを送信(S118)
S119
署名データを検証
S120
検証成功？
YES
NO
S121
端末のネットワークシステムへの接続
認証失敗を通知(S122)
S123
出力装置に認証が失敗したことを表示

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/012602

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01)i; ***H04L 9/32***(2006.01)i; ***G06F 21/44***(2013.01)i
FI: H04L9/32 200D; H04L9/32 200B; H04L9/14; G06F21/44

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)

H04L9/14; H04L9/32; G06F21/44

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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.
Y	WO 2021/049041 A1 (NTT COMMUNICATIONS CORPORATION) 18 March 2021 (2021-03-18) paragraphs [0002], [0019]-[0121], fig. 1-20	1-2, 4-13
A		3
Y	US 2020/0244469 A1 (SAFENET INC.) 30 July 2020 (2020-07-30) claims 1-3, paragraphs [0048], [0049]	1-2, 4-13
Y	JP 2021-114201 A (FUJITSU LIMITED) 05 August 2021 (2021-08-05) paragraphs [0002], [0068]	4-8
A	JP 2009-94984 A (KDDI CORPORATION) 30 April 2009 (2009-04-30) paragraphs [0006], [0022]-[0053], fig. 1-7	1-13

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
18 May 2023	**30 May 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/012602

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2021/049041 A1	18 March 2021	EP 4006866 A1 paragraphs [0002], [0019]-[0123], fig. 1-20	
US 2020/0244469 A1	30 July 2020	EP 3918768 A1	
JP 2021-114201 A	05 August 2021	US 2021/0226801 A1 paragraphs [0003], [0108] EP 3852306 A1	
JP 2009-94984 A	30 April 2009	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2023/012602

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/14(2006.01)i; H04L 9/32(2006.01)i; G06F 21/44(2013.01)i
FI: H04L9/32 200D; H04L9/32 200B; H04L9/14; G06F21/44

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

H04L9/14; H04L9/32; G06F21/44

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３年

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

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	WO 2021/049041 A1 (エヌ・ティ・ティ・コミュニケーションズ株式会社) 18.03.2021 (2021-03-18) 段落0002,0019-0121,図1-20	1-2,4-13
A		3
Y	US 2020/0244469 A1 (SAFENET INC.) 30.07.2020 (2020-07-30) 請求項1-3,段落0048-0049	1-2,4-13
Y	JP 2021-114201 A (富士通株式会社) 05.08.2021 (2021-08-05) 段落0002,0068	4-8
A	JP 2009-94984 A (ＫＤＤＩ株式会社) 30.04.2009 (2009-04-30) 段落0006,0022-0053,図1-7	1-13

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
"A" 特に関連のある文献ではなく、一般的技術水準を示すもの
"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
"O" 口頭による開示、使用、展示等に言及する文献
"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
"Y" 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
"&" 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
18.05.2023	30.05.2023

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

権限のある職員（特許庁審査官）
局　成矢 5S 1594

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/012602

引用文献	公表日	パテントファミリー文献	公表日
WO 2021/049041 A1	18.03.2021	EP 4006866 A1 段落0002,0019-0123,図1-20	
US 2020/0244469 A1	30.07.2020	EP 3918768 A1	
JP 2021-114201 A	05.08.2021	US 2021/0226801 A1 段落0003,0108 EP 3852306 A1	
JP 2009-94984 A	30.04.2009	（ファミリーなし）	