

(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
2011 年 5 月 12 日(12.05.2011)

PCT

(10) 国際公開番号
WO 2011/055486 A1

- (51) 国際特許分類:
G06F 21/24 (2006.01) G06F 21/20 (2006.01)
- (21) 国際出願番号: PCT/JP2010/005970
- (22) 国際出願日: 2010 年 10 月 5 日(05.10.2010)
- (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 2009-255908 2009 年 11 月 9 日(09.11.2009) JP
- (71) 出願人 (米国を除く全ての指定国について): 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).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 奥山玄(OKUYAMA, Gen) [JP/JP]; 〒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). 宮本善則(MIYAMOTO, Yoshinori) [JP/JP]; 〒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). 村上卓弥(MURAKAMI, Takuya) [JP/JP]; 〒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).
- (74) 代理人: 岩壁冬樹, 外(IWAKABE, Fuyuki et al.); 〒1040031 東京都中央区京橋一丁目 4 番 1 0 号

大野屋京橋ビル 6 階 サンライズ国際特許事務所 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, 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 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

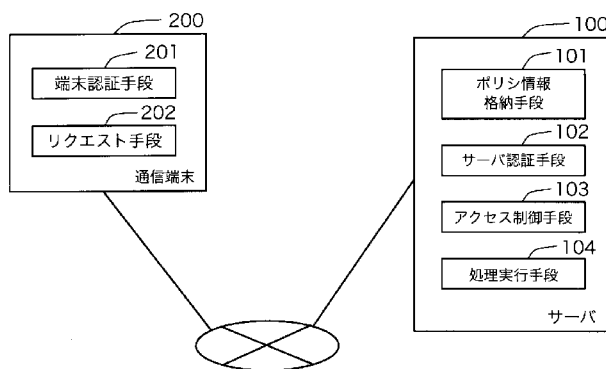
添付公開書類:

- 国際調査報告 (条約第 21 条(3))

(54) Title: ACCESS CONTROL SYSTEM, COMMUNICATION TERMINAL, SERVER, AND ACCESS CONTROL METHOD

(54) 発明の名称: アクセス制御システム、通信端末、サーバ、およびアクセス制御方法

[図14]



- 100 SERVER
101 POLICY INFORMATION STORAGE MEANS
102 SERVER AUTHENTICATION MEANS
103 ACCESS CONTROL MEANS
104 PROCESSING EXECUTION MEANS
200 COMMUNICATION TERMINAL
201 TERMINAL AUTHENTICATION MEANS
202 REQUEST MEANS

にもとづきアクセス制御を行う。

(57) Abstract: A terminal authentication means of a communication terminal associates a content item with authentication information of the content item and manages the same. When accessing a server accompanying an execution operation for a content item, a request means transmits a request including authentication information that has been associated with the content item to the server. The server receives a request from a communication terminal and authenticates the request by a server authentication means. An access control means controls access on the basis of policy information that has been stored in a policy information storage means.

(57) 要約: 通信端末の端末認証手段は、コンテンツと当該コンテンツの認証情報を対応付けて管理する。コンテンツの実行動作に伴ってのサーバにアクセスする場合に、リクエスト手段は、コンテンツに対応付けられた認証情報含むリクエストをサーバに送信する。サーバは、通信端末からのリクエストを受け、サーバ認証手段によってリクエストの認証を行う。アクセス制御手段は、ポリシー情報格納手段に格納されているポリシー情報と

明 細 書

発明の名称：

アクセス制御システム、通信端末、サーバ、およびアクセス制御方法

技術分野

[0001] 本発明は、アクセス制御システム、通信端末、サーバ、およびアクセス制御方法に関し、特に通信ネットワークを介したサービスの提供に適用することができるアクセス制御システム、通信端末、サーバ、およびアクセス制御方法に関する。

背景技術

[0002] インターネットを介して、多くのウェブサービスが提供されている。サーバ（ウェブサーバ）は、クライアント端末の要求に応じてサービスを提供する。提供するサービスは、具体的には、例えば、ウェブサイトによる情報提供、ウェブアプリケーション（アプリケーションプログラム）の提供、その他情報の提供などである。ウェブサーバには、クライアント端末ごとに表示レイアウトの変更やサービスの提供可否を決定しているものがある。

[0003] クライアント端末の判別手段として、HTTP（HyperText Transfer Protocol）のリクエストヘッダに付与されるユーザエージェント（User Agent：UA）がよく利用されている。

[0004] ウェブサーバは、UAを参照することでクライアント端末を判別できる。具体的には、使用されているウェブブラウザプログラム（以下、単にウェブブラウザやブラウザともいう）の種類や、クライアント端末の機種名を判別できる。しかし、例えば、ウェブアプリケーションのようにウェブブラウザ上で動作するアプリケーションがいずれのアプリケーションであるのかを判定することはできない。

[0005] このため、ウェブサーバは、信頼できるアプリケーションにはサービスを提供するがそれ以外には提供しない、などの判断をすることができない。そのような判断を可能にするためには、クライアント端末で動作するアプリケ

ーションからウェブサーバにアクセスする際、すなわち、例えば、クライアント端末が、搭載しているアプリケーションプログラムの制御に従って、インターネットを介してウェブサーバに接続要求を行った際、クライアント端末からウェブサーバに対して要求元アプリケーションの素性を通知する仕組みが必要となる。なお、アプリケーションの素性とは、例えば、当該アプリケーションの出所（具体的には、例えば、当該アプリケーションの作成者や、当該作成者を認証した機関）のことである。

[0006] アプリケーションの素性確認は、認証処理によって行われ、認証処理にはアプリケーションに付与されている署名を用いることが多い。認証処理では、署名に用いられた証明書が信頼できる認証機関（Certificate Authority：CA）によって発行されたものかを検証し、それをもってアプリケーションが信頼できるか否かを判断する。信頼できるCAであるか否かは、一般に、ルート証明書と呼ばれる大元の認証機関の証明書によって判断される。

[0007] そして、ウェブサーバに対してアプリケーションの素性を通知する方法として、クライアント端末が行った認証処理の結果を通知するという方法が考えられる。例えば、クライアント端末が、ウェブサーバAから送信されたSSL（Secure Sockets Layer）証明書を検証することによってウェブサーバAが提供するアプリケーションが信頼できるか否かを判定する認証処理を行う。そして、アプリケーションがアクセス先のサーバBに認証処理の結果を送信する。ウェブサーバBは、送信された認証結果にもとづいて、信頼できるアプリケーションからの接続要求であるか否かを判断し、アクセス制限（接続処理の制限）を行うことができる。

[0008] 特許文献1には、サービス提供サーバへの接続の可否を判断するアクセス制御サーバを備えたシステムが記載されている。

先行技術文献

特許文献

[0009] 特許文献1：特開2009-54086号公報（段落0009～0043、図

1)

発明の概要

発明が解決しようとする課題

[0010] ウェブブラウザが保持するルート証明書はユーザによって追加可能であるので、前述したウェブサーバにアプリケーションの素性を通知する方法では、ルート証明書等の情報がウェブサーバにとっては信頼できない情報である場合がある。しかし、そのような追加されたルート証明書によってアプリケーションの認証処理が行われた場合であっても、クライアント端末はアプリケーションを信頼できるものとして認証してしまう。すると、クライアント端末に搭載された当該アプリケーションによるウェブサーバへの要求は、信頼できるアプリケーションからの要求として当該ウェブサーバに認識されてしまうので、ウェブサーバが本来接続を許可することを意図していないアクセスが行われてしまうおそれがある。つまり、ルート証明書が追加された場合には、ウェブサーバが本来拒絶すべき接続要求が許可されてしまうおそれがある。

[0011] なお、特許文献 1 に記載されているシステムは、サービス提供サーバへの接続の可否を判断するためのアクセス制御サーバを用いるので、システムの導入および管理に費用がかかるという問題がある。また、特許文献 1 に記載されているシステムは、ユーザごとにサービス提供サーバへの接続の可否を判断しており、接続が許可されているユーザが使用するアプリケーションによって、ウェブサーバが本来接続を許可することを意図していないアクセスが行われてしまうおそれがある。

[0012] 本発明は、サーバが接続を許可することを意図していないアプリケーションからのアクセスの要求に対して、アクセスを許可しないようにすることができるアクセス制御システム、通信端末、サーバ、およびアクセス制御方法を提供することを目的とする。

課題を解決するための手段

[0013] 本発明によるアクセス制御システムは、サーバ、およびサーバに通信ネッ

トワークを介して接続される通信端末を備えたアクセス制御システムであって、通信端末は、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理する端末認証手段と、サーバにアクセスする場合に、当該コンテンツの認証情報と、サーバに要求する処理を示す要求内容情報とを含むリクエストをサーバに送信するリクエスト手段とを含み、サーバは、通信端末が送信したリクエストに含まれる認証情報および要求内容情報にもとづいて、リクエストに応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、通信端末が送信したリクエストに含まれる認証情報にもとづいてリクエストの認証を行うサーバ認証手段と、サーバ認証手段がリクエストを認証した場合に、ポリシー情報格納手段に格納されているポリシー情報と、リクエストに含まれる認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、アクセス制御手段が要求内容情報によって示される処理を実行すると決定した場合に、処理を実行する処理実行手段とを含むことを特徴とする。

[0014] 本発明による他の態様のアクセス制御システムは、サーバ、およびサーバに通信ネットワークを介して接続される通信端末を備えたアクセス制御システムであって、通信端末は、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理する端末認証手段と、サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証手段と、検証手段が認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、コンテンツの認証情報と、サーバに要求する処理を示す要求内容情報とを含むリクエストをサーバに送信するリクエスト手段とを含み、サーバは、通信端末が送信した

リクエストに含まれる認証情報および要求内容情報にもとづいて、リクエストに応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、ポリシー情報格納手段に格納されているポリシー情報と、リクエストに含まれる認証情報および要求内容情報にもとづいて、要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、アクセス制御手段が要求内容情報によって示される処理を実行すると決定した場合に、処理を実行する処理実行手段とを含むことを特徴とする。

[0015] 本発明による通信端末は、通信ネットワークを介してサーバに処理の実行を要求する通信端末であって、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報である認証情報とを対応付けて管理する認証手段と、コンテンツの認証情報およびサーバに要求する処理を示す要求内容情報を含むリクエストをコンテンツの認証情報および要求内容情報に応じて処理を実行するサーバに送信するリクエスト手段を備えたことを特徴とする。

[0016] 本発明による他の態様の通信端末は、通信ネットワークを介してサーバに処理の実行を要求する通信端末であって、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるそのコンテンツの認証情報とを対応付けて管理する認証手段と、サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証手段と、検証手段が認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、コンテンツの認証情報と、サーバに要求する処理を示す要求内容情報とを含むリクエストをコンテンツの認証情報および要求内容情報に応じて処理を実行するサーバに送信するリクエスト手段を備えたことを特徴とする。

[0017] 本発明によるサーバは、通信端末が通信ネットワークを介して送信した要求に応じて処理を実行するサーバであって、通信端末が送信した要求を示す

要求内容情報と、通信端末が処理を実行しているコンテンツの電子証明書にもとづく認証情報とにもとづいて、要求に応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、通信端末が送信した認証情報にもとづいて要求の認証を行う認証手段と、認証手段が要求を認証した場合に、ポリシー情報格納手段に格納されているポリシー情報と、認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、アクセス制御手段が要求内容情報によって示される処理を実行すると決定した場合に、処理を実行する処理実行手段とを備えたことを特徴とする。

[0018] 本発明による他の態様のサーバは、通信端末が通信ネットワークを介して送信した要求に応じて処理を実行するサーバであって、通信端末が送信した要求を示す要求内容情報と、通信端末が処理を実行しているコンテンツの電子証明書にもとづく認証情報とにもとづいて、要求に応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、ポリシー情報格納手段に格納されているポリシー情報と、認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、アクセス制御手段が要求内容情報によって示される処理を実行すると決定した場合に、処理を実行する処理実行手段とを備えたことを特徴とする。

[0019] 本発明によるアクセス制御方法は、通信端末の要求に応じてサーバが処理を実行するアクセス制御方法であって、通信端末が、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理し、サーバにアクセスする場合に、当該コンテンツの認証情報と、サーバに要求する処理を示す要求内容情報とを含むリクエストをサーバに送信し、サーバが、通信端末が送信したリクエストに含まれる認証情報にもとづいてリクエストを認証する処理を行い、リクエストを認証した場合に、リクエストに応じた処理を実

行するか否かを示すポリシー情報と、リクエストに含まれる認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定し、要求内容情報によって示される処理を実行すると決定した場合に、処理を実行することを特徴とする。

- [0020] 本発明による他の態様のアクセス制御方法は、通信端末の要求に応じてサーバが処理を実行するアクセス制御方法であって、通信端末が、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理し、サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証処理を行い、検証処理で、認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、当該コンテンツの認証情報と、サーバに要求する処理を示す要求内容情報とを含むリクエストをサーバに送信し、サーバが、リクエストに応じた処理を実行するか否かを示すポリシー情報と、リクエストに含まれる認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定し、要求内容情報によって示される処理を実行すると決定した場合に、処理を実行することを特徴とする。

発明の効果

- [0021] 本発明によれば、サーバが接続を許可することを意図していないアプリケーションからのアクセスの要求に対して、アクセスを許可しないようにすることができる。つまり、アプリケーションごとにアクセス制御をすることができる。

図面の簡単な説明

- [0022] [図1]本発明による第1の実施形態のアクセス制御システムの構成例を示すブロック図である。

[図2]アプリケーション認証処理を示すフローチャートである。

[図3]認証情報格納部に対応付けられて格納されているアプリケーション情報

と検証結果との例を示す説明図である。

[図4] リクエスト処理を示すフローチャートである。

[図5] 第 1 の実施形態のアクセス要求情報の例を示す説明図である。

[図6] リクエスト認証処理を示すフローチャートである。

[図7] ポリシ格納部に格納されているポリシの例を示す説明図である。

[図8] 本発明による第 2 の実施形態のアクセス制御システムの構成例を示すブロック図である。

[図9] 第 2 の実施形態において図 4 に示す第 1 の実施形態の（２）通信端末 2 からサーバ 3 へのリクエスト処理に追加する処理を示すフローチャートである。

[図10] 第 2 の実施形態のアクセス要求情報の例を示す説明図である。

[図11] 本実施例において、認証情報格納部に格納されたウェブサーバの URL と証明書のハッシュ値とを示す説明図である。

[図12] 本実施例において、認証情報格納部に格納されたウェブサーバの URL と証明書のハッシュ値とを示す説明図である。

[図13] 各認証機関が発行したルート証明書のハッシュ値の例を示す説明図である。

[図14] 本発明の概要を示すブロック図である。

発明を実施するための形態

[0023] 実施形態 1 .

本発明による第 1 の実施形態のアクセス制御システムについて、図面を参照して説明する。図 1 は、本発明による第 1 の実施形態のアクセス制御システムの構成例を示すブロック図である。

[0024] 図 1 に示すように、本発明による第 1 の実施形態のアクセス制御システムは、通信端末 2 とサーバ 3 とを含み、通信端末 2 にはアプリケーションサーバ 1 が接続される。なお、通信端末 2 は、サーバ 3 にも接続される。

[0025] アプリケーションサーバ 1 は、通信端末 2 に提供されるアプリケーションプログラムであるアプリケーション 1 2 が格納されたアプリケーション格納

部 1 1 を含む。アプリケーション 1 2 は、通信端末 2 によってダウンロードされる。

[0026] 通信端末 2 は、アプリケーション取得手段 2 1 と、アプリケーション格納部 2 2 と、アプリケーション認証手段 2 3 と、証明書格納部 2 4 と、認証情報格納部 2 5 と、リクエスト手段 2 6 と、アプリケーション実行手段 2 7 とを含む。

[0027] サーバ 3 は、リクエスト受付手段 3 1 と、リクエスト認証手段 3 2 と、証明書格納部 3 3 と、サービス格納部 3 4 と、アクセス制御手段 3 5 と、ポリシー格納部 3 6 とを含む。

[0028] 次に、ブロック図およびフローチャートを参照して本実施形態のアクセス制御システムの動作について説明する。

[0029] アクセス制御システムの動作は、（１）通信端末 2 が実行するアプリケーション認証処理、（２）通信端末 2 からサーバ 3 へのリクエスト処理、（３）サーバ 3 が実行するリクエスト認証処理、の 3 つの動作に分けられる。以下、本実施形態におけるそれぞれの処理について説明する。

[0030] まず、（１）通信端末 2 が実行するアプリケーション認証処理について、図面を参照して説明する。図 2 は、アプリケーション認証処理を示すフローチャートである。通信端末 2 のアプリケーション取得手段 2 1 は、アプリケーションサーバ 1 からアプリケーション 1 2 をダウンロード（DL）する（ステップ S 2 1）。

[0031] アプリケーション 1 2 に証明書が付加されている場合（ステップ S 2 2 の Yes）、アプリケーション認証手段 2 3 は、証明書検証処理（認証処理）を行う（ステップ S 2 3）。なお、証明書（電子証明書）とは、例えば、CA 等が電子的な方法で署名した電子データである。証明書には、例えば、証明書保持者名、証明書保持者の公開鍵、CA の ID、および CA による電子署名などが含まれる。

[0032] 証明書検証処理は、例えば、証明書格納部 2 4 に格納されている証明書と、アプリケーション 1 2 に付加されている証明書とが合致するか否かを判断

する処理である。なお、他の方法によって証明書検証処理が行われてもよい。

[0033] アプリケーション認証手段 23 は、ステップ S 23 における証明書検証処理で、証明書格納部 24 に格納されている証明書と、アプリケーション 12 に付加されている証明書とが合致すると判断した場合に（ステップ S 24 の Yes）、認証情報格納部 25 に検証結果として認証情報を格納する（ステップ S 25）。具体的には、アプリケーション認証手段 23 は、認証情報格納部 25 に、アプリケーション情報と認証情報とを対応付けて格納する。認証情報は、証明書格納部 24 に格納されている証明書とアプリケーション 12 に付加されている証明書とが合致すると判断された場合に、認証情報格納部 25 に検証結果として格納されるので、認証情報が認証情報格納部 25 に格納されているということは、当該認証情報に対応付けられているアプリケーション情報によって示されるアプリケーションが証明書検証処理（認証処理）で認証されたということである。

[0034] 図 3 は、認証情報格納部 25 に対応付けられて格納されているアプリケーション情報と検証結果との例を示す説明図である。図 3 に示す例では、アプリケーション情報は、アプリケーション 12 の格納場所を示す URL（Uniform Resource Locator）である。また、図 3 に示す例では、認証情報は、アプリケーション 12 に付加されていた証明書のハッシュ値である。図 3 に示す例では、アプリケーション情報は「http://appserver1/app12」である。図 3 に示す例では、認証情報であるハッシュ値は「92q8sldkfjd038u」である。そして、図 3 には、アプリケーション 12 のアプリケーション情報であるアプリケーション 12 の格納場所を示す URL と、アプリケーション 12 に付加されていた証明書のハッシュ値とが対応付けられて認証情報格納部 25 に格納されていることが示されている。本例では、認証情報は、アプリケーション 12 に付加されていた証明書のハッシュ値である。

[0035] そして、アプリケーション取得手段 21 は、ステップ S 21 の処理でアプ

リケーションサーバ1からダウンロードしたアプリケーション12をアプリケーション格納部22に格納する（ステップS26）。

[0036] 次に、（2）通信端末2からサーバ3へのリクエスト処理について説明する。図4は、リクエスト処理を示すフローチャートである。上述したステップS21の処理で通信端末2がダウンロードしたアプリケーション12のプログラム制御にもとづいて、通信端末2がサーバ3にアクセスする場合（接続要求（アクセス要求）する場合）を例に説明する。アプリケーション実行手段27が、アプリケーション格納部22に格納されているアプリケーション12の実行中に、アプリケーション12のプログラム制御にもとづいてサーバ3にアクセス要求を行う指示（以下、単にアクセス要求という）をリクエスト手段26に出力する（ステップS41）。

[0037] リクエスト手段26は、アクセス要求を受け取ると、認証情報格納部25からアプリケーション12に対応する認証情報を取得する（ステップS42）。具体的には、認証情報の取得を試みる。図3に示す例では、認証情報格納部25に、アプリケーション12のURLに対応付けられた認証情報が格納されているので（ステップS43のYes）、アプリケーション12のID（具体的には、アプリケーション12の格納場所を示すURL）をキーとして認証情報である証明書のハッシュ値を得る。リクエスト手段26は、認証情報取得後、アクセス要求に認証情報を付加し（ステップS44）、サーバ3にリクエスト（アクセス要求情報）を送信する（ステップS45）。図5は、本実施形態のアクセス要求情報の例を示す説明図である。図5に示す例では、アクセス要求情報には、要求元のアプリケーションID（アプリケーション12のURL）、要求する内容（要求内容情報）、認証情報が含まれる。図5に示す例では、アクセス要求情報は、アプリケーション12がサーバ3にdata001の送信を要求する情報である。

[0038] 次に、（3）サーバ3が実行するリクエスト認証処理について、図面を参照して説明する。図6は、リクエスト認証処理を示すフローチャートである。リクエスト受付手段31は、通信端末2からのアクセス要求（具体的には

、アクセス要求情報）を受け（ステップS 6 1）、リクエスト認証手段 3 2 にアクセス要求情報を渡し、検証を行う（ステップS 6 2）。

[0039] リクエスト認証手段 3 2 は、アクセス要求情報から認証情報を取り出し、証明書格納部 3 3 に予め格納されている証明書と合致するか否かを確認する。本例では、図 5 に示すように、アクセス要求情報に認証情報として証明書のハッシュ値が含まれているので、リクエスト認証手段 3 2 は、証明書格納部 3 3 に予め格納されている証明書のハッシュ値を計算し、計算結果のハッシュ値と認証情報によって示されるハッシュ値とが合致するか否かを確認する。

[0040] ここでは、認証情報によって示されるハッシュ値が証明書格納部 3 3 に予め格納されている認証機関 a（CA__1）によって発行された証明書のハッシュ値と合致したこととする。その後、アクセス制御手段 3 5 は、ポリシー格納部 3 6 に格納されているポリシーを参照して、アクセス可否の判定を行う（ステップS 6 3）。なお、ポリシー（ポリシー情報）とは、どの認証機関が発行した証明書を有するアプリケーションに、どのデータへのアクセスを許可するのかを示す情報である。ポリシー格納部 3 6 には、認証機関の ID（例えば、CA__1 や CA__2、CA__3）と、認証機関の ID ごとにアクセスを許可するデータ（例えば、data 001 や data 002、data 003、data 004）とが格納されている。

[0041] 図 7 は、ポリシー格納部 3 6 に格納されているポリシーの例を示す説明図である。図 7 に示す例では、認証機関 a（CA__1）が発行した証明書を有するアプリケーションに、data 001、data 002、data 003 へのアクセスを許可し、認証機関 b（CA__2）が発行した証明書を有するアプリケーションに、data 003、data 004 へのアクセスを許可し、認証機関 c（CA__3）が発行した証明書を有するアプリケーションに、data 002 へのアクセスを許可するポリシーがポリシー格納部 3 6 に格納されていることが示されている。

[0042] 本例では、アクセス要求情報に含まれるハッシュ値は認証機関 a（CA__

1) が発行した証明書のハッシュ値と合致するので、アプリケーション 12 による data 001 へのアクセスは許可されることになる（ステップ S 64 の Yes）。アクセス許可になった場合（ステップ S 64 の Yes）、リクエスト受付手段 31 は、サービス格納部 34 からデータ（data 001）を取り出し（ステップ S 65）、通信端末 2 にレスポンスを返す（ステップ S 66）。具体的には、取り出したデータ（data 001）を通信端末 2 に送信する。

[0043] 本実施形態では、通信端末 2 がアプリケーションの認証情報をサーバ 3 に送信するので、サーバ 3 がどのアプリケーション（具体的には、どの認証機関で認証されたアプリケーション）の動作にもとづく要求なのかを把握することができる。また、サーバ 3 が認証情報を検証するので、通信端末 2 が行った認証処理の正当性を確認している。さらに、サーバ 3 のポリシー格納部 36 に格納されているポリシーでアクセス制御を行うことができる。すなわち、通信端末 2 のユーザによって証明書格納部 24 に証明書が追加され、その証明書によってアプリケーションが認証されたとしても、サーバ 3 のリクエスト認証処理およびポリシーを用いたアクセス制御でアクセスを拒絶可能であるため、サーバ 3 が意図しないアクセスを行われることはない。つまり、サーバ 3 に所定の認証機関によって発行された証明書にもとづくポリシーを設定して、アプリケーションごとのアクセス制御を行うことができる。

[0044] すなわち、本実施形態では、サーバがリクエスト元のコンテンツごとにアクセス制限を行うことができる。その理由は、通信端末がリクエストにコンテンツの認証情報を付加してサーバに送信するからである。また、サーバのポリシーでアクセス制限を行うことができることである。その理由は、通信端末から送信される認証情報にもとづいて、サーバ側が、自身のポリシーで再度認証するための仕組みを有しているからである。

[0045] 実施形態 2.

本発明の第 2 の実施形態のアクセス制御システムについて、図面を参照して説明する。図 8 は、本発明による第 2 の実施形態のアクセス制御システム

の構成例を示すブロック図である。

[0046] 図 8 に示すように、本発明の第 2 の実施形態のアクセス制御システムには、図 1 に示す第 1 の実施形態における通信端末 2 に、追加証明書格納部 2 8 と検証手段 2 9 とが追加されている。また、本発明の第 2 の実施形態のアクセス制御システムにおけるサーバ 3 は、リクエスト認証手段 3 2 と証明書格納部 3 3 とを含んでいない。追加証明書格納部 2 8 には、通信端末 2 のユーザによって追加された証明書が格納される。検証手段 2 9 は、証明書検証処理で、アプリケーション 1 2 に付加されている証明書に合致する証明書が証明書格納部 2 4 に格納されている証明書であるのか否かを検証する。

[0047] 本実施形態のアクセス制御システムの動作について説明する。本実施形態では、図 2 に示す (1) 通信端末 2 が実行するアプリケーション認証処理におけるステップ S 2 3 の処理で、アプリケーション 1 2 に付加されている証明書が、証明書格納部 2 4 に格納されている証明書、または追加証明書格納部 2 8 に格納されている証明書に合致するか否かを判断する。その他の処理は図 2 に示す第 1 の実施形態の (1) 通信端末 2 が実行するアプリケーション認証処理と同様なため、説明を省略する。

[0048] 次に、本実施形態の (2) 通信端末 2 からサーバ 3 へのリクエスト処理について説明する。図 9 は、本実施形態において図 4 に示す第 1 の実施形態の (2) 通信端末 2 からサーバ 3 へのリクエスト処理に追加される処理を示すフローチャートである。

[0049] 第 1 の実施形態では、図 4 に示すステップ S 4 2 の処理で、リクエスト手段 2 6 が認証情報を取得していたが、本実施形態では、リクエスト手段 2 6 が認証情報を取得した後に、検証手段 2 9 が認証情報格納部 2 5 から認証情報を取得する (ステップ S 9 1)。

[0050] また、第 1 の実施形態では、図 4 に示すステップ S 4 3 の処理で認証情報がある場合は、認証情報を付加する処理 (ステップ S 4 4) が行われていた。しかし、第 2 の実施形態では、ステップ S 4 4 の処理を行う前に、検証手段 2 9 が認証情報の検証を行う (ステップ S 9 1)。検証手段 2 9 は、認証

情報が、（１）通信端末２が実行するアプリケーション認証処理におけるステップＳ２３の処理で、証明書格納部２４に格納されている証明書によって検証されたか否かを確認する。

[0051] 具体的には、証明書格納部２４に格納されている証明書のハッシュ値を計算し、図３に例示されているアプリケーション１２に付加されていた証明書のハッシュ値と合致するか否かを確認する。検証手段２９は、合致した場合には、証明書格納部２４に格納されている証明書によって検証されたアプリケーションからの要求であると判断する。合致しない場合は、追加証明書格納部２８に格納されている追加された証明書によって検証されたと判断する。

[0052] 証明書格納部２４に格納されている証明書によって検証されたことが判断された場合（Ｓ９２のＹｅｓ）、ステップＳ４４の処理に移行する。第１の実施形態のステップＳ４４の処理では、リクエスト手段２６が、アクセス要求に認証情報としてハッシュ値を付加したが、第２の実施形態では、リクエスト手段２６が、ステップＳ４４の処理でアクセス要求に認証機関のＩＤを付加する。図１０は、本実施形態のアクセス要求情報の例を示す説明図である。図１０に示す本実施形態のアクセス要求情報には、要求元のアプリケーションＩＤ（アプリケーション１２のＵＲＬ）、要求する内容、認証機関のＩＤが含まれる。なお、リクエスト手段２６は、証明書格納部２４に格納されている証明書から認証機関のＩＤを取得する。

[0053] 次に、本実施形態の（３）サーバ３が実行するリクエスト認証処理について説明する。第１の実施形態では、図６に示すステップＳ６２でアクセス要求情報の検証処理を行っていたが、本実施形態では、ステップＳ６１の処理後にステップＳ６３の処理に移行し、ステップＳ６２の処理は行われない。すなわち、図１０に示すように、サーバ３には、通信端末２から送信される認証情報に認証機関のＩＤが含まれるので、ステップＳ６１の処理後にはステップＳ６３のアクセス可否判定に移行する。その後の処理は、第１の実施の形態と同様であるので、説明を省略する。

- [0054] 本実施の形態では、通信端末 2 において、もともとインストールされている（予め認証情報格納部 2 5 に格納されている）証明書と追加された（追加証明書格納部 2 8 に格納されている）証明書とが分けて管理されている。そして、アプリケーションの証明書のハッシュ値がもともとインストールされている証明書のハッシュ値と合致した場合には、認証機関の ID がサーバ 3 に送信されるように構成されている。このため、通信端末 2 がサーバ 3 にアクセスする際、サーバ 3 は、アクセス元のアプリケーションがもともとインストールされている証明書によって認証されているか否かを判断することができる。従って、第 1 の実施形態と異なり、サーバ 3 側でリクエスト認証処理を行う必要がない。よって、サーバ 3 の処理負担を軽減することができる。
- [0055] なお、本実施形態は、第 1 の実施形態においてサーバ 3 側で管理している証明書（証明書格納部 3 3 に格納されている証明書）が通信端末 2 で管理している証明書（証明書格納部 2 4 に格納されている証明書）と同一であることが前提である。
- [0056] 以下に、本発明の他の実施形態について述べる。以上に述べた第 1 の実施形態では、図 2 に示すステップ S 2 5 の処理で、認証情報格納部 2 5 に証明書のハッシュ値を格納した。このハッシュ値は、独自のハッシュ関数を用いて証明書からハッシュ値を計算してもよいし、証明書に格納されているフィンガープリントを使用してもよい。さらに、証明書に格納されている暗号化フィンガープリントを複合したものを使用してもよい。
- [0057] さらに、第 1 の実施形態では、通信端末 2 からサーバ 3 に送信される認証情報は、証明書のハッシュ値としていたが、これに限らない。すなわち、証明書そのものを送信してもよい。
- [0058] さらに、第 1 の実施形態では、図 6 に示すステップ S 6 2 において、サーバ 3 のリクエスト認証手段 3 2 は、通信端末 2 からのリクエストがあったときに証明書格納部 3 3 に格納されている証明書のハッシュ値を計算していたがこれに限られない。すなわち、リクエスト認証手段 3 2 が、証明書格納部

33に格納されている証明書のハッシュ値を予め計算しておき、リクエストがあった際は、比較だけ行うように構成されていてもよい。

[0059] さらに、第1の実施形態では、通信端末2からサーバ3へのリクエスト前に、リクエスト手段26が認証情報格納部25からリクエスト元のアプリケーションに対応した認証情報を取得していたがこれに限られない。すなわち、リクエスト手段26がリクエスト元のアプリケーションに対応した認証情報を取得できればよい。例えば、リクエスト元のアプリケーションに対応した証明書を取得するような `getCertificate()` 関数などのAPI (Application Programming Interface) があり、これをリクエスト手段26が発行することで証明書を取得し、その証明書からハッシュ値を計算し、サーバ3に送信する、といった流れであってもよい。この方法によれば、通信端末2が行うアプリケーション認証処理時に認証結果を認証情報格納部25に格納する必要はない。

[0060] さらに、第1の実施形態および第2の実施形態では、サーバ3の証明書格納部33に格納されている証明書は更新されないことが前提であったが、これに限られない。また、更新された証明書を通信端末2に通知し、通信端末2において証明書格納部24に格納された証明書を更新する手段が設けられていてもよい。この場合、通信端末2に証明書更新手段を設け、サーバ3から通知、または通信端末2が定期的にポーリングし、証明書格納部24に格納されている証明書を更新する仕組みが設けられていてもよい。

[0061] さらに、第2の実施形態では、図8に示したように証明書格納部24と追加証明書格納部28とが分けられていたが、同じ格納部であってもよく、論理的に分かれていればよい。すなわち、通信端末2からサーバ3にリクエストを送信する前に、検証手段29によってもともとインストールされていた証明書によってアプリケーションが検証されているか否かがわかるように構成されていればよい。

[0062] さらに、第1の実施形態および第2の実施形態では、通信端末2がサーバ3にリクエストを送信する際、図5に例示したようにアプリケーションID

も送信していたが、これに限られない。すなわち、認証情報、つまり誰にお墨付きをもらったアプリケーションであるのかという認証機関の情報がアクセス要求情報に含まれていれば、アプリケーションIDは送信されなくてもよい。

- [0063] さらに、第1の実施形態および第2の実施形態では、図6に示すステップS63のアクセス可否判定において、図7に例示したCAのIDとアクセス可能データとの対応付けテーブルが用いられていたが、対応付けの組み合わせはこれに限られない。すなわち、URLとアクセス可能データとの対応付けであってもよいし、CAのIDとURLとアクセス可能データとの組合せであってもよい。

実施例

- [0064] 次に、具体的な実施例を用いて本発明によるアクセス制御システムの動作を説明する。本実施例では、通信端末（通信端末2）が、搭載しているウェブブラウザの起動中にウェブサーバ（アプリケーションサーバ1）に格納されているウェブアプリケーションを実行し、サーバ（サーバ3）に格納されているデータにアクセスする場合を例に説明する。
- [0065] まず、（1）通信端末2が行うアプリケーション認証処理について説明する。通信端末2のユーザは、ウェブブラウザを用いてウェブサーバ（アプリケーションサーバ1）にアクセスする（接続処理を行う）。ウェブサーバのURLが「https」で始まる場合には、SSL通信が行われることが示されており、ウェブサーバと通信端末2との間で証明書のやり取りが行われる。
- [0066] 具体的には、アプリケーション認証手段23が、例えば、ウェブサーバが信頼できる認証機関によってウェブアプリケーションが承認されているかを、アプリケーションサーバ1から送信された証明書と、証明書格納部24に格納されているルート証明書とを用いて確認する。本実施例では、アプリケーションサーバ1が信頼されていることを前提とし、認証情報格納部25にアプリケーションサーバ1のURLとルート証明書のハッシュ値とが対応付

けられて格納されているとする。図 11 は、本実施例において、認証情報格納部 25 に格納されたウェブサーバの URL と証明書のハッシュ値とを示す説明図である。図 11 に示すように、本実施例では、認証情報格納部 25 には、ウェブサーバの URL である「https: appserver1. com」と、ルート証明書のハッシュ値である「3 j l s d k 0 d l 0 3 j 0 8 1 7 e u b」とが格納されている。

[0067] ルート証明書を用いたウェブアプリケーションの確認後、ウェブサイトの HTML (HyperText Markup Language) ファイルを表示する。この HTML ファイルにウェブアプリケーションが組み込まれている場合、そのブラウザの起動中にウェブアプリケーションが実行される。具体的には、アプリケーション格納部 22 に格納されたウェブアプリケーションをアプリケーション実行手段 27 が実行する。

[0068] 次に、(2) 通信端末 2 からサーバ 3 へのリクエスト処理について説明する。ウェブアプリケーションは、サーバ 3 の API を発行する（具体的には、例えば、API キーを発行する）ことで、サーバ 3 のサービス格納部 34 に格納されたデータのリクエストを行う。これは例えば、「call (http: // appserver3. com? getData ("data001"))」などの API を発行することで、サーバ 3 に「data001」の送信を要求する。

[0069] ウェブアプリケーションが本 API を発行すると、リクエスト手段 26 はこれを検知する（具体的には、例えば、リクエスト手段 26 は、ウェブアプリケーションのプログラム制御にもとづいてアプリケーション実行手段 27 が API キーを発行したことを検知する）。そして、認証情報格納部 25 からリクエスト元のウェブアプリケーション（実際にはウェブアプリケーション配信元のサーバ。つまりアプリケーションサーバ 1）に対応した認証情報を取り出す。リクエスト手段 26 は、この認証情報を付加して、サーバ 3 にリクエスト（具体的には、例えば、アクセス要求情報）を送信する。図 12 は、HTTP リクエストヘッダに認証情報を付加する例を示す説明図である

。図 1 2 に示す例では、リクエスト元アプリケーションの情報として「`referrer`」を設定し、認証情報として「`x-cert-hash`」を設定している。

[0070] 次に、(3) サーバ 3 が実行するリクエスト認証処理について説明する。リクエスト受付手段 3 1 が通信端末 2 からのリクエストを受けた際（例えば、通信端末 2 が送信したアクセス要求情報を受信した際）、リクエスト認証手段 3 2 は、HTTP ヘッダから認証情報を取得する。HTTP ヘッダから認証情報を取得する方法には、例えば、「`getHTTPHeader(“referrer”)`」などの API を呼び出し、リクエスト元のウェブアプリケーションの情報と認証情報とを取得する方法がある。リクエスト認証手段 3 2 は、取得した認証情報と証明書格納部 3 3 に格納されている証明書とが合致するか否か検証する。

[0071] 図 1 3 は、各認証機関が発行したルート証明書のハッシュ値の例を示す説明図である。本実施例では、図 1 3 に示すように証明書のハッシュ値が予め計算されていることとし、各ハッシュ値が証明書の発行元の CA の ID と対応付けられていることとする。これによると、通信端末 2 が送信した認証情報によって示されるハッシュ値と CA__1 のハッシュ値とが合致するため、リクエスト元のアプリケーション（を格納しているアプリケーションサーバ 1）が確かに CA__1 によって承認されていることがわかる。

[0072] ここで合致しない場合には、通信端末 2 は、リクエスト元のアプリケーション（アプリケーションサーバ 1 に格納されているアプリケーション）は信頼できるアプリケーションであると認識するが、サーバ 3 は（サーバ 3 のポリシーでは）、それ（アプリケーションサーバ 1 に格納されているアプリケーション）は信頼できないアプリケーションである、と認識する。例えば、通信端末 2 において、ユーザによって追加された証明書（追加証明書）によってアプリケーションが認証されると、そのように（通信端末 2 が送信した認証情報によって示されるハッシュ値と CA__1 のハッシュ値とが合致しない）なると考えられる。つまり、リクエスト（具体的には、例えば、アクセス

要求情報)に追加証明書のハッシュ値が付与されて送信されると、サーバ側にはこの証明書は存在しない(例えば、サーバ3の証明書格納部33に格納されていない)ので、リクエスト認証の段階で、リクエストに付与されている証明書と自身が保持する証明書が合致しない、という結果になる。

[0073] 認証処理を終えると、アクセス制御手段35は、CA__1(によって発行された証明書を有するアプリケーション)に対するポリシーを確認する。これは、前述した図7に示したように、CA__1が発行した証明書を有するアプリケーションに、data001へのアクセスを許可するポリシーがポリシー格納部36に格納されているため、アクセス権があると判断される。その後、リクエスト受付手段31は、サービス格納部34に格納されているdata001を取り出し、HTTPのレスポンスに追加し、通信端末2に返す(送信する)。

[0074] なお、本実施例は、ウェブアプリケーションを対象としていたが、これに限らない。例えば、JAVA(登録商標)アプリケーションなどにも適用できる。JAVAアプリケーションのダウンロード時にその実行環境であるJAVAVM(JAVA Virtual Machine)がアプリケーションの認証を行い、アプリケーションとアプリケーションに対応付けられた証明書を管理する。JAVAアプリケーションからサーバにデータの送信要求があった際は、JAVAVMがそれを検知し、リクエストに対応する証明書のハッシュ値を付加してサーバに送信することで実現できる。

[0075] 本発明は、その他のアプリケーションにも適用できる。すなわち、機器固有のネイティブアプリケーションや、スクリプト言語で作成されたアプリケーションなどにも適用できる。また、アプリケーションに限らず、コンテンツにも適用できる。すなわち、HTMLファイルなどにも適用できる。HTMLファイルの場合は、自身のタグ(Aタグなど)でイメージファイルを読み込む際、他サイトにリンクが貼られている場合がある。その他サイトにおいて、どのHTMLファイルからアクセスされたのかを判断し、イメージファイルの提供に関するアクセス制御を行う、などに利用できる。

- [0076] 次に、本発明の概要について説明する。図 14 は、本発明の概要を示すブロック図である。図 14 に示すように、本発明によるアクセス制御システムは、サーバ（図 1 に示されたサーバ 3 に相当） 100 と通信端末（図 1 に示された通信端末 2 に相当） 200 とを備える。そして、通信端末 200 は、端末認証手段（図 1 に示されたアプリケーション認証手段 23 に相当） 201、およびリクエスト手段（図 1 に示されたリクエスト手段 26 に相当） 202 を含む。また、サーバ 100 は、ポリシー情報格納手段（図 1 に示されたポリシー格納部 36 に相当） 101、サーバ認証手段（図 1 に示されたリクエスト認証手段 32 に相当） 102、アクセス制御手段（図 1 に示されたアクセス制御手段 35 に相当） 103 および処理実行手段（図 1 に示されたリクエスト受付手段 34 に相当） 104 を含む。
- [0077] 端末認証手段 201 は、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、認証処理で認証したコンテンツと、認証処理で認証されたことを示し、電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理する。
- [0078] リクエスト手段 202 は、コンテンツの実行動作に伴ってサーバ 100 にアクセスする場合に、当該コンテンツの認証情報と、サーバ 100 に要求する処理を示す要求内容情報とを含むリクエストをサーバ 100 に送信する。
- [0079] ポリシー情報格納手段 101 は、通信端末 200 が送信したリクエストに含まれる認証情報および要求内容情報にもとづいて、リクエストに応じた処理を実行するか否かを示すポリシー情報を予め格納する。
- [0080] サーバ認証手段 102 は、通信端末 200 が送信したリクエストに含まれる認証情報にもとづいてリクエストの認証を行う。
- [0081] アクセス制御手段 103 は、サーバ認証手段 102 がリクエストを認証した場合に、ポリシー情報格納手段 101 に格納されているポリシー情報と、リクエストに含まれる認証情報および要求内容情報とにもとづいて、要求内容情報によって示される処理を実行するか否かを決定する。
- [0082] 処理実行手段 104 は、アクセス制御手段 103 が要求内容情報によって

示される処理を実行すると決定した場合に、処理を実行する。

[0083] そのような構成により、通信端末 200 のリクエスト手段 202 がコンテンツの認証情報をサーバ 100 に送信するので、サーバ 100 がどのコンテンツ（具体的には、どの認証機関で認証されたコンテンツ）の動作にもとづく要求なのかを把握することができる。そして、サーバ 100 のアクセス制御手段 103 がポリシー情報格納手段 101 に格納されているポリシー情報にもとづいて当該要求に応じた処理を実行するか否かを決定するので、サーバ 100 のポリシー情報格納手段 101 に格納されているポリシー情報にもとづいてアクセス制御を行うことができる。よって、例えば、通信端末 200 のユーザによって証明書が追加され、その証明書によってコンテンツが認証されていたとしても、サーバ 100 のポリシー情報にもとづいてアクセスを拒絶可能であるため、サーバ 100 が意図しないアクセスを行われることはない。つまり、サーバ 100 に所定の認証機関によって発行された証明書にもとづくポリシーを設定して、コンテンツごとにアクセス制御を行うことができる。

[0084] 上記の各実施形態には、以下のようなアクセス制御システムも開示されている。

[0085] 端末認証手段 201 が、コンテンツの電子証明書のハッシュ値、フィンガープリント、または電子証明書自体を当該コンテンツの認証情報として当該コンテンツに対応付けて管理するアクセス制御システム。

[0086] 検証手段が、コンテンツの認証処理で用いられた電子証明書が予め記憶手段に記憶されている電子証明書に合致するか否かを検証するアクセス制御システム。そのような構成によれば、通信端末 200 がサーバ 100 にアクセスする際、サーバ 100 は、アクセス元のコンテンツがもともとインストールされている証明書によって認証されているか否かを判断することができる。よって、サーバ 100 側で認証処理を行う必要がなくなり、サーバ 100 の処理負担を軽減することができる。

[0087] 端末認証手段によってコンテンツに対応付けて管理される当該コンテンツの認証情報には、コンテンツの電子証明書の発行元の ID が含まれているア

クセス制御システム。コンテンツとしてアプリケーションプログラムを扱うアクセス制御システム。

[0088] 通信端末 200 が検証手段（図 8 に示された検証手段 29 に相当）を含み、サーバ 100 がサーバ認証手段 102 を含まない構成が開示されている。

[0089] 検証手段が、サーバ 100 にアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証するように構成されている通信端末。

[0090] そのような構成によれば、前述した効果に加えて、通信端末 200 側で、コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証するので、サーバ 100 側で認証処理を行う必要がない。よって、サーバ 100 の処理負担を軽減することができる。

[0091] 以上、実施形態及び実施例を参照して本願発明を説明したが、本願発明は上記実施形態および実施例に限定されるものではない。本願発明の構成や詳細には、本願発明のScope内で当業者が理解し得る様々な変更をすることができる。

[0092] この出願は、2009 年 11 月 9 日に提出された日本特許出願 2009-255908 を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用の可能性

[0093] 本発明を、PC や携帯電話機などの通信機器からウェブサービスを利用する際のアクセス制限に適用できる。

請求の範囲

[請求項1]

サーバと、前記サーバに通信ネットワークを介して接続される通信端末とを含むアクセス制御システムであって、

前記通信端末は、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理する端末認証手段と、

前記サーバにアクセスする場合に、当該コンテンツの認証情報と、前記サーバに要求する処理を示す要求内容情報とを含むリクエストを前記サーバに送信するリクエスト手段とを含み、

前記サーバは、前記通信端末が送信したリクエストに含まれる認証情報および要求内容情報にもとづいて、前記リクエストに応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、

前記通信端末が送信したリクエストに含まれる前記認証情報にもとづいてリクエストの認証を行うサーバ認証手段と、

前記サーバ認証手段が前記リクエストを認証した場合に、前記ポリシー情報格納手段に格納されているポリシー情報と、前記リクエストに含まれる認証情報および要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、

前記アクセス制御手段が前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する処理実行手段とを含む

ことを特徴とするアクセス制御システム。

[請求項2]

端末認証手段は、コンテンツの電子証明書のハッシュ値を当該コンテンツの認証情報として当該コンテンツに対応付けて管理する

請求項 1 記載のアクセス制御システム。

[請求項3] 端末認証手段は、コンテンツの電子証明書のフィンガープリントを当該コンテンツの認証情報として当該コンテンツに対応付けて管理する

請求項 1 記載のアクセス制御システム。

[請求項4] 端末認証手段は、コンテンツの電子証明書を当該コンテンツの認証情報として当該コンテンツに対応付けて管理する

請求項 1 記載のアクセス制御システム。

[請求項5] サーバ認証手段は、リクエストに含まれる認証情報によって示される電子証明書と、予め記憶手段に記憶されている電子証明書とが合致した場合に、前記リクエストを認証する

請求項 1 から請求項 4 のうちいずれか 1 項記載のアクセス制御システム。

[請求項6] サーバと、前記サーバに通信ネットワークを介して接続される通信端末とを含むアクセス制御システムであって、

前記通信端末は、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理する端末認証手段と、

前記サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証手段と、

前記検証手段が認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、コンテンツの認証情報と、前記サーバに要求する処理を示す要求内容情報とを含むリクエストを前記サーバに送信するリクエスト手段とを含み、

前記サーバは、前記通信端末が送信したリクエストに含まれる認証

情報および要求内容情報にもとづいて、前記リクエストに応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、

前記ポリシー情報格納手段に格納されているポリシー情報と、前記リクエストに含まれる認証情報および要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、

前記アクセス制御手段が前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する処理実行手段とを含む

ことを特徴とするアクセス制御システム。

[請求項7] 検証手段は、コンテンツの認証処理で用いられた電子証明書が予め記憶手段に記憶されている電子証明書に合致するか否かを検証する請求項6記載のアクセス制御システム。

[請求項8] 端末認証手段によってコンテンツに対応付けて管理される当該コンテンツの認証情報には、コンテンツの電子証明書の発行元のIDが含まれている

請求項6記載のアクセス制御システム。

[請求項9] コンテンツは、アプリケーションプログラムである
請求項1から請求項8のうちいずれか1項記載のアクセス制御システム。

[請求項10] 通信ネットワークを介してサーバに処理の実行を要求する通信端末であって、

前記コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもとづく情報である認証情報とを対応付けて管理する認証手段と、

前記コンテンツの認証情報およびサーバに要求する処理を示す要求

内容情報を含むリクエストを前記コンテンツの認証情報および前記要求内容情報に応じて処理を実行するサーバに送信するリクエスト手段とを備えた

ことを特徴とする通信端末。

[請求項11] 通信ネットワークを介してサーバに処理の実行を要求する通信端末であって、

コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもとづく情報であるそのコンテンツの認証情報とを対応付けて管理する認証手段と、

前記サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証手段と、

前記検証手段が認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、コンテンツの認証情報と、前記サーバに要求する処理を示す要求内容情報とを含むリクエストを前記コンテンツの認証情報および前記要求内容情報に応じて処理を実行する前記サーバに送信するリクエスト手段とを備えた

ことを特徴とする通信端末。

[請求項12] 検証手段は、コンテンツの認証処理で用いられた電子証明書が予め記憶手段に記憶されている電子証明書に合致するか否かを検証する

請求項11記載の通信端末。

[請求項13] 通信端末が通信ネットワークを介して送信した要求に応じて処理を実行するサーバであって、

前記通信端末が送信した要求を示す要求内容情報と、前記通信端末が処理を実行しているコンテンツの電子証明書にもとづく認証情報とにもとづいて、前記要求に応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、

前記通信端末が送信した認証情報にもとづいて要求の認証を行う認証手段と、

認証手段が前記要求を認証した場合に、前記ポリシー情報格納手段に格納されているポリシー情報と、前記認証情報および前記要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、

前記アクセス制御手段が前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する処理実行手段とを備えた

ことを特徴とするサーバ。

[請求項14]

通信端末が通信ネットワークを介して送信した要求に応じて処理を実行するサーバであって、

前記通信端末が送信した要求を示す要求内容情報と、前記通信端末が処理を実行しているコンテンツの電子証明書にもとづく認証情報とにもとづいて、前記要求に応じた処理を実行するか否かを示すポリシー情報を予め格納するポリシー情報格納手段と、

前記ポリシー情報格納手段に格納されているポリシー情報と、前記認証情報および前記要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定するアクセス制御手段と、

前記アクセス制御手段が前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する処理実行手段とを備えた

ことを特徴とするサーバ。

[請求項15]

通信端末の要求に応じてサーバが処理を実行するアクセス制御方法であって、

前記通信端末が、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもと

づく情報であるコンテンツの認証情報とを対応付けて管理し、

前記サーバにアクセスする場合に、当該コンテンツの認証情報と、前記サーバに要求する処理を示す要求内容情報とを含むリクエストを前記サーバに送信し、

前記サーバが、前記通信端末が送信したリクエストに含まれる前記認証情報にもとづいてリクエストを認証する処理を行い、

前記リクエストを認証した場合に、前記リクエストに応じた処理を実行するか否かを示すポリシー情報と、前記リクエストに含まれる認証情報および要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定し、

前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する

ことを特徴とするアクセス制御方法。

[請求項16]

サーバは、リクエストに含まれる認証情報によって示される電子証明書と、予め記憶手段に記憶されている電子証明書とが合致した場合に、前記リクエストを認証する

請求項15記載のアクセス制御方法。

[請求項17]

通信端末の要求に応じてサーバが処理を実行するアクセス制御方法であって、

前記通信端末が、コンテンツに付加されている電子証明書を用いて当該コンテンツの認証処理を行い、前記認証処理で認証したコンテンツと、前記認証処理で認証されたことを示し、前記電子証明書にもとづく情報であるコンテンツの認証情報とを対応付けて管理し、

前記サーバにアクセスする場合に、当該コンテンツの認証処理で用いられた電子証明書が所定の電子証明書であるか否かを検証する検証処理を行い、

前記検証処理で、前記認証処理で用いられた電子証明書が所定の電子証明書であると判断した場合に、当該コンテンツの認証情報と、前

記サーバに要求する処理を示す要求内容情報とを含むリクエストを前記サーバに送信し、

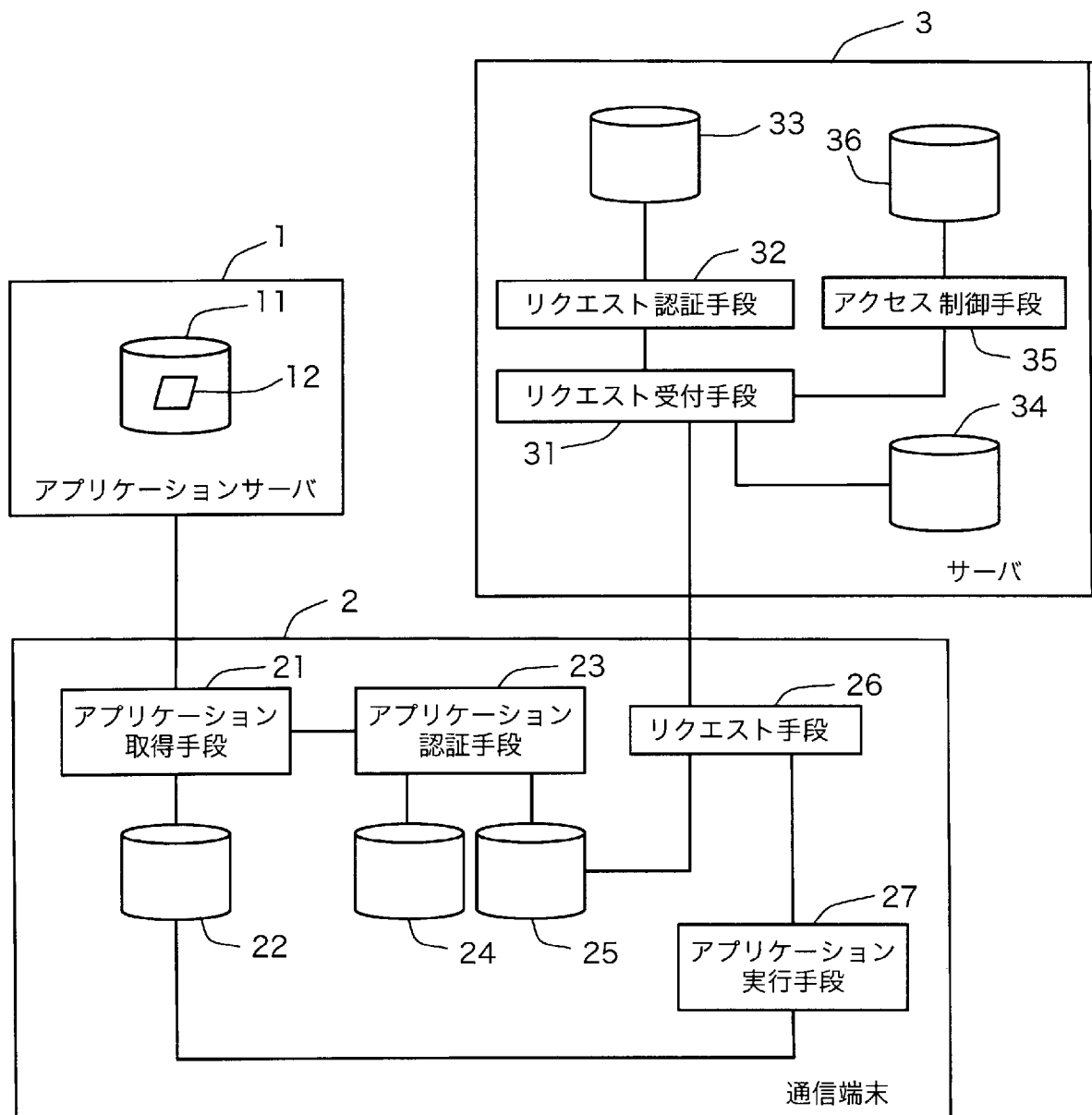
前記サーバが、前記リクエストに応じた処理を実行するか否かを示すポリシー情報と、前記リクエストに含まれる認証情報および要求内容情報とにもとづいて、前記要求内容情報によって示される処理を実行するか否かを決定し、

前記要求内容情報によって示される処理を実行すると決定した場合に、前記処理を実行する

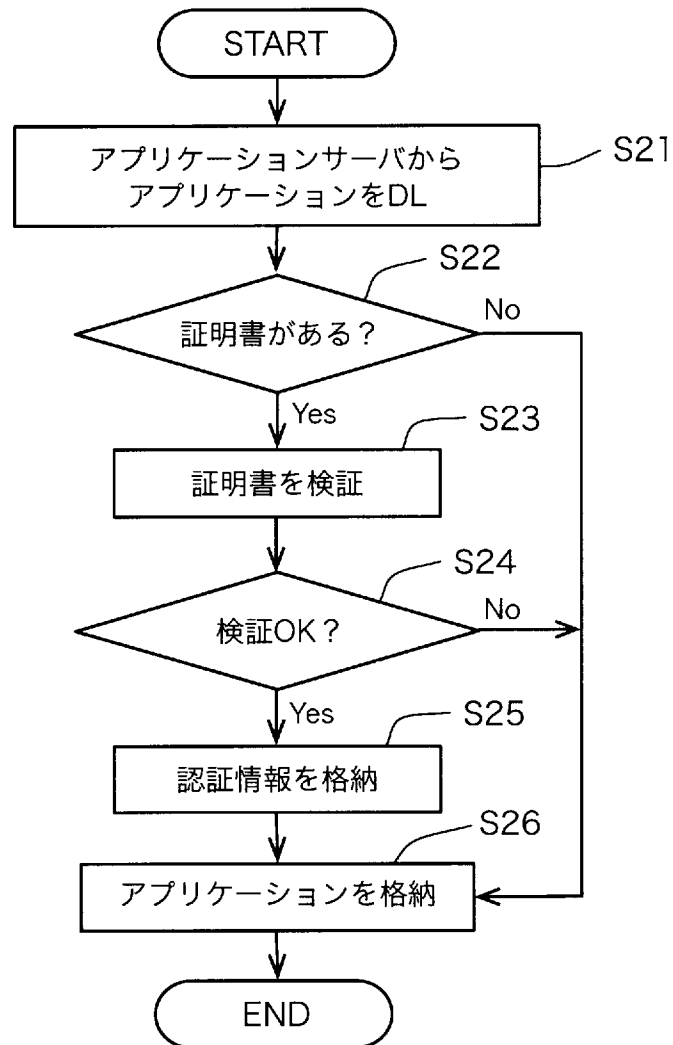
ことを特徴とするアクセス制御方法。

[請求項18] 検証処理で、コンテンツの認証処理で用いられた電子証明書が予め記憶手段に記憶されている電子証明書に合致するか否かを検証する請求項17記載のアクセス制御方法。

[図1]



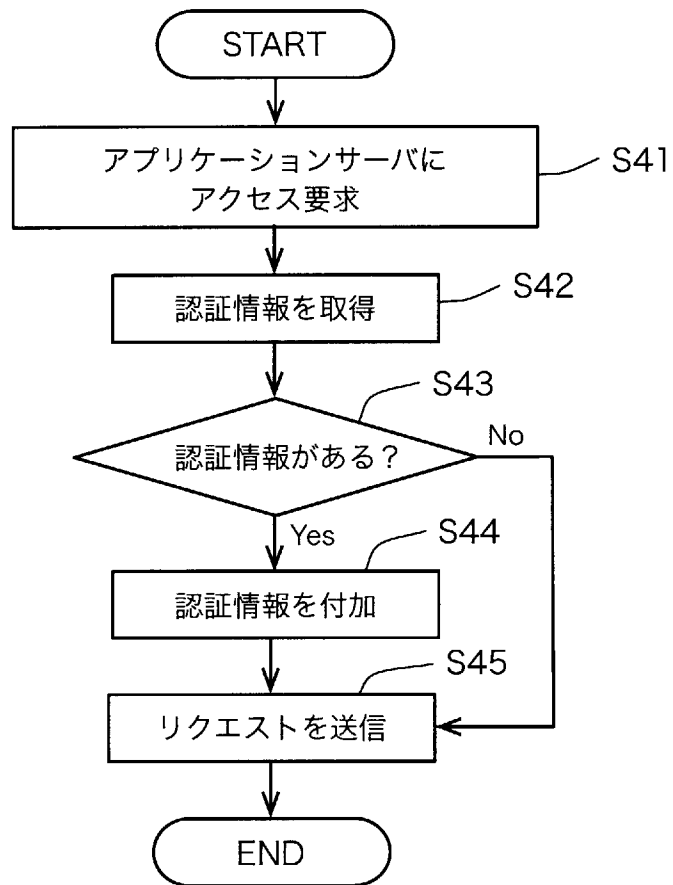
[図2]



[図3]

アプリケーションURL	証明書ハッシュ値
http://appserver1/app12	92q8sldkfjd038u

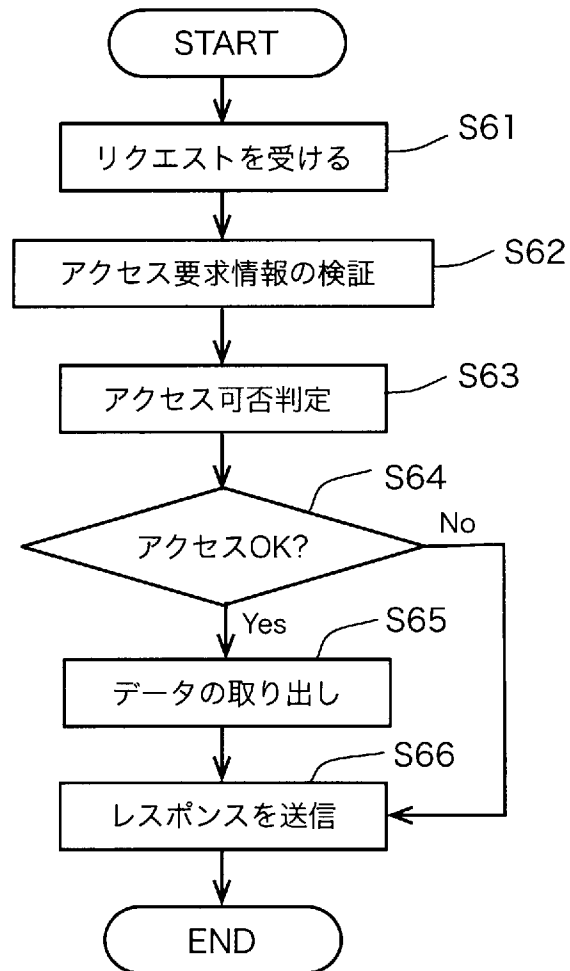
[図4]



[図5]

アプリケーションID	要求内容	認証情報
http://appserver1/app12	data001	92q8sldkfjd038u

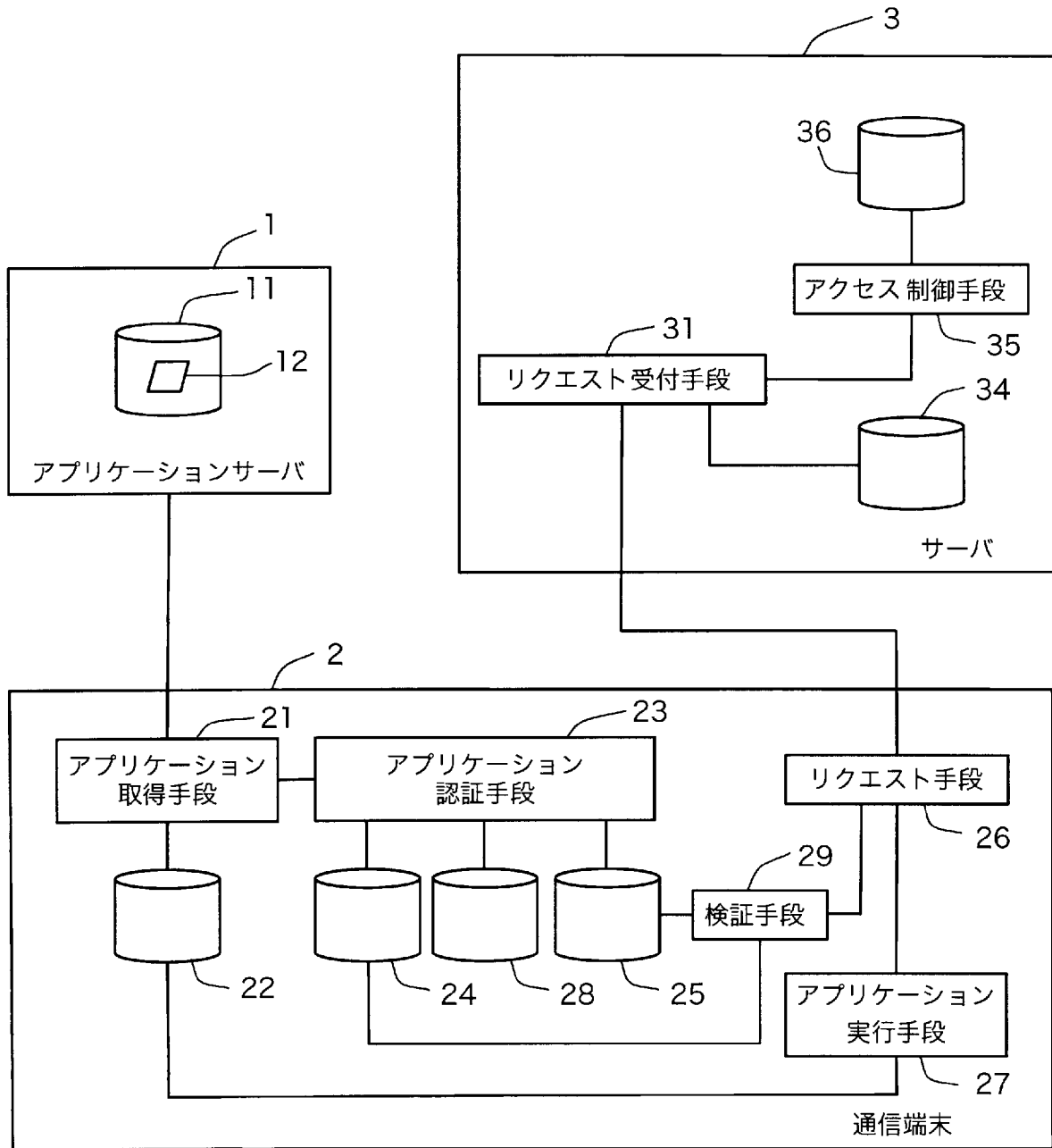
[図6]



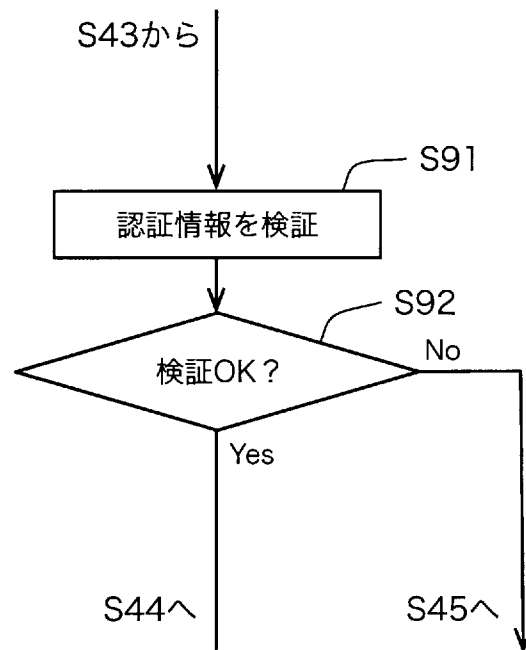
[図7]

CAのID	アクセス可能データ
CA__1	data001, data002, data003
CA__2	data003, data004
CA__3	data002

[図8]



[図9]



[図10]

アプリケーションID	要求内容	CAのID
http://appserver1/app12	data001	CA_1

[図11]

WebサーバURL	証明書ハッシュ値
https://appserver1.com	3jlsdk0dl03j0817eub

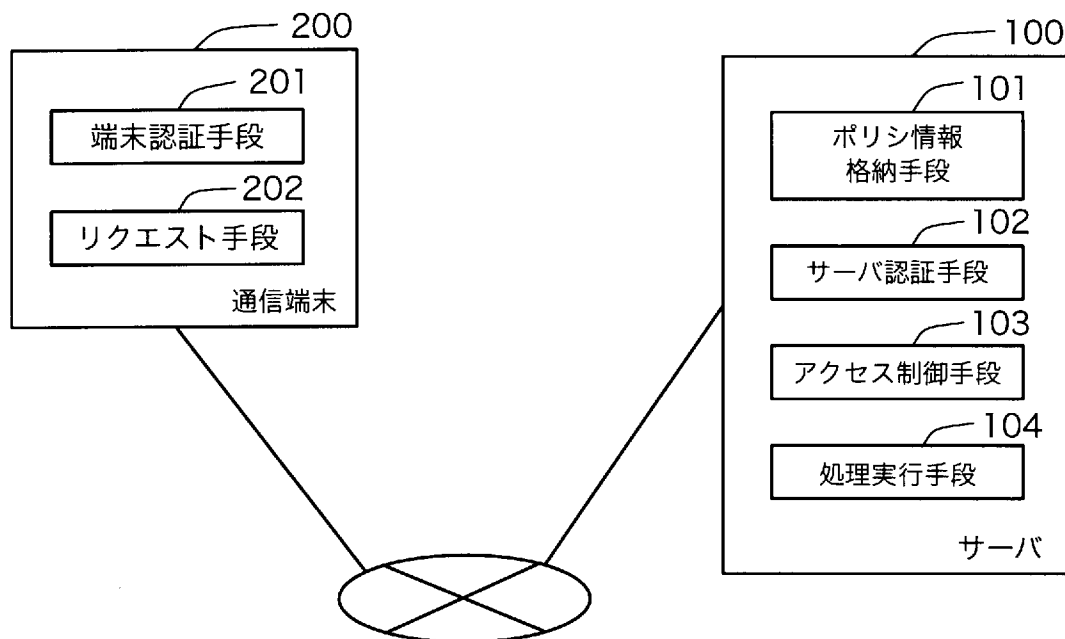
[図12]

```
GET method=getData&value=data001/HTTP1.1
host: appserver3.com
...
referer: https://appserver1.com
x-cert-hash: 3jlsdk0dl03j0817eub
```

[図13]

CAのID	ハッシュ値
CA__1	3jlsdk0dl03j0817eub
CA__2	sd203dk06nvo3iso2
CA__3	l82k5eneoi3c8el31v

[図14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/005970

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24 (2006.01) i, G06F21/20 (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)

G06F21/24, G06F21/20

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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 A	JP 2004-507848 A (ContentGuard Holdings, Inc.), 11 March 2004 (11.03.2004), paragraphs [0029] to [0046] & US 7073199 B1 & WO 2002/019628 A1	1, 9-10, 13-15 2-8, 11-12, 16-18
Y A	Hiroshi MARUYAMA, Hisashi KOJIMA, "Tokushu Internet, On Security of Signed Java and ActiveX Codes", Computer Software, vol.16, no.4, 15 July 1999 (15.07.1999), vol.16, no.4, pages 23 to 32	1, 9-10, 13-15 2-8, 11-12, 16-18
A	WO 2006/001524 A1 (NEC Corp.), 05 January 2006 (05.01.2006), entire text; all drawings & US 2009/0205037 A1	1-18

☒ 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
08 December, 2010 (08.12.10)

Date of mailing of the international search report
21 December, 2010 (21.12.10)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/005970

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-128313 A (NEC Corp.), 24 May 2007 (24.05.2007), entire text; all drawings (Family: none)	1-18

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/24(2006.01)i, G06F21/20(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（I P C））

Int.Cl. G06F21/24, G06F21/20

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 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 A	JP 2004-507848 A（コンテンツガード ホールディングス インコーポレイテッド）2004.03.11, 段落[0029]-[0046] & US 7073199 B1 & WO 2002/019628 A1	1, 9-10, 13-15 2-8, 11-12, 16-18
Y A	丸山 宏、児島 尚, 特集インターネット 主に J a v a 及び A c t i v e X におけるコード署名の安全性に関する考察, コンピュータソフトウェア VOL. 1 6 NO. 4, 1999.07.15, 第16巻 第4号, p.23-p.32	1, 9-10, 13-15 2-8, 11-12, 16-18

☒ 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

0 8 . 1 2 . 2 0 1 0

国際調査報告の発送日

2 1 . 1 2 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

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）

本郷 彰

5 S

4 2 2 5

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	WO 2006/001524 A1 (日本電気株式会社) 2006.01.05, 全文、全図 & US 2009/0205037 A1	1-18
A	JP 2007-128313 A (日本電気株式会社) 2007.05.24, 全文、全図 (フ ァミリーなし)	1-18