(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
2006 年3 月30 日 (30.03.2006)

PCT

(10) 国際公開番号
WO 2006/033150 A1

(51) 国際特許分類[7]: H04L 9/32, G06F 15/00

(21) 国際出願番号: PCT/JP2004/013920

(22) 国際出願日: 2004 年9 月24 日 (24.09.2004)

(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 (米国を除く全ての指定国について): エムブイピー株式会社 (MVP, INC.) [JP/JP]; 〒1030025 東京都中央区日本橋茅場町２丁目３番６号 Tokyo (JP).

(71) 出願人 および
(72) 発明者: 川北 潤 (KAWAKITA, Jun) [JP/JP]; 〒1030025 東京都中央区日本橋茅場町２丁目３番６号 エムブイピー株式会社内 Tokyo (JP).

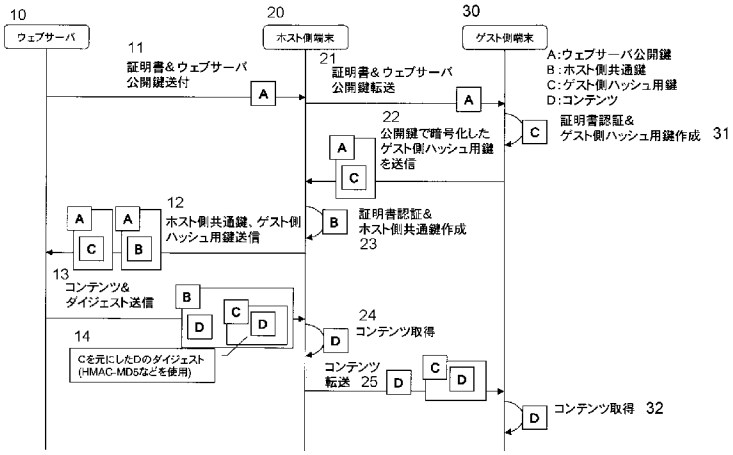
(74) 代理人: 生田 哲郎, 外 (IKUTA, Tetsuo et al.); 〒1060032 東京都港区六本木１丁目９番９号 六本木ファーストビル７階 生田・名越法律特許事務所 Tokyo (JP).

(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, 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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,

[続葉有]

(54) Title: DATA COMMUNICATION METHOD

(54) 発明の名称: データ通信方法



10 WEB SERVER
11 SEND CERTIFICATE & WEB SERVER PUBLIC KEY
12 TRANSMIT HOST SIDE COMMON KEY AND GUEST SIDE HASH KEY
13 TRANSMIT CONTENTS AND DIGEST
14 DIGEST (USING HMAC-MD5) OF D BASED ON C
20 HOST SITE TERMINAL
21 TRANSFER CETIFICATE & WEB SERVER PUBLIC KEY
22 TRANSMIT GUEST SIDE HASH KEY ENCRYPTED WITH PUBLIC KEY
23 AUTHENTICATE CERTIFICATE AND CREATE HOST SIDE COMMON KEY
24 ACQUIRE CONTENTS
25 TRANSFER CONTENTS
30 GUEST SIDE TERMINAL
A WEB SERVER PUBLIC KEY
B HOST SIDE COMMON KEY
C GUEST SIDE HAS KEY
D CONTENTS
31 AUTHENTICATE CERTIFICATE AND CREATE GUEST SIDE HASH KEY
32 ACQUIRE CONTENTS

(57) Abstract: A data communication method capable of executing a synchronizing process at two or more computer terminals while ensuring security. A server certificate and a public key are transmitted through a host side terminal to a guest side terminal. This guest side terminal authenticates the server and encrypts a guest side hash key to be used in a hash function and the hash function with the public key. A web server decrypts the hash key and the hash function, and then creates a digest of the contents with the guest side hash key and transmits the digest through the host side terminal to the guest side terminal. The guest side terminal receives the contents received from the host side terminal and that digest, and compares that digest and a digest created from the received contents thereby to ensure the security when the synchronizing process is executed.

(57) 要約: 二以上のコンピュータ端末で同期処理を実行する場合に、セキュリティを確保しながら同期処理を実行することが可能なデータ通信方法を提供することを目的とする。 ホスト側端末を介してサーバ証明書と公開鍵をゲスト側端末に送信することで、ゲスト側端末はサーバを認証し、ゲスト側端末がハッシュ関数で用いるゲスト側ハッシュ用鍵と前記ハッシュ関数とを公開鍵で暗号化して、それをウェブサーバで復号化した後、ウェブサーバが当該ゲスト側ハッシュ用鍵で当該コンテンツのダイジェストを作成してそれをホスト側端末を介してゲスト側端末に送信し、ゲスト側端末

[続葉有]

WO 2006/033150 A1

NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, IT, LU, 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。

ではホスト側端末から受信したコンテンツとダイジェストとを受信し、そのダイジェストと、受信したコンテンツから作成したダイジェストとを比較することによって、同期処理を実行する際に、セキュリティを確保することが出来る、データ通信方法である。