

(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
2013 年 3 月 28 日(28.03.2013)



(10) 国際公開番号
WO 2013/042634 A1

- (51) 国際特許分類:
H04L 12/56 (2006.01)
- (21) 国際出願番号: PCT/JP2012/073711
- (22) 国際出願日: 2012 年 9 月 14 日(14.09.2012)
- (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 2011-204487 2011 年 9 月 20 日(20.09.2011) 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): 森田 陽一郎(MORITA, Yoichiro) [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). 中江 政行(NAKAE, Masayuki) [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). 山形 昌也(YAMAGATA, Masaya) [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). 佐々木 貴之(SASAKI, Takayuki) [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). 下西 英之(SHIMONISHI, Hideyuki) [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). 園田 健太郎(SONODA, Kentaro) [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). 波多野 洋一(HATANO, Yoichi) [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).

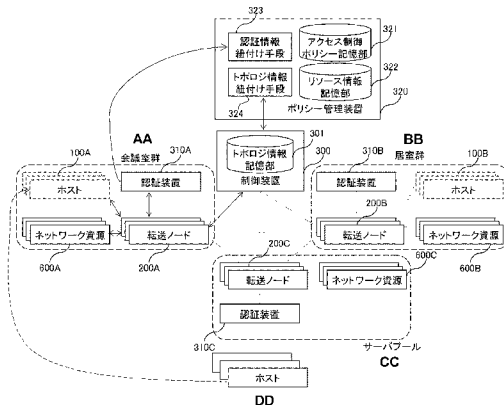
- (74) 代理人: 加藤 朝道(KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜 3 丁目 2 0 番 1 2 号加藤内外特許事務所内 Kanagawa (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA,

[続葉有]

(54) Title: COMMUNICATION SYSTEM, POLICY MANAGEMENT DEVICE, COMMUNICATION METHOD, AND PROGRAM

(54) 発明の名称: 通信システム、ポリシー管理装置、通信方法およびプログラム

[図1]



100A, 100B, DD Host
200A, 200B, 200C Forwarding node
300 Control device
301 Topology information recording unit
310A, 310B, 310C Authentication device
320 Policy management device
321 Access control policy recording unit
322 Resource information recording unit
323 Authentication information tying means
324 Topology information tying means
600A, 600B, 600C Network resources
AA Conference room group
BB Living room group
CC Server pool

(57) Abstract: The present invention updates access control in real time when the connection state of an apparatus or a user changes frequently. The present invention is provided with: an authentication device that authenticates a user who is using a host connected to a forwarding node; and a policy management device that holds an access control policy that, using an identifier of the user or the forwarding node, specifies a host that is the subject of access control, and the policy management device ties together the identifier of the host that is the subject of access control and the identifier of the user using the host or the forwarding node to which the host is connected. The forwarding node transmits to the policy management device the set of the identifiers of the selfsame forwarding node and the host connected to the selfsame forwarding node, the authentication device transmits to the policy management device the set of the identifiers of the user and the host connected to the forwarding node, when the host connected to the forwarding node is the subject of access control, the policy management device notifies a control device of the contents of access control, and the control device generates a processing rule in accordance with the notification and sets the processing rule to the forwarding node.

(57) 要約:

[続葉有]

WO 2013/042634 A1



BB, BG, BH, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

MZ, NA, RW, SD, SL, 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, 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:

- (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,

— 国際調査報告 (条約第 21 条(3))

機器やユーザの接続状態が頻繁に変化する場合にリアルタイムにアクセス制御を更新する。転送ノードに接続されたホストを使用するユーザを認証する認証装置と、転送ノードまたはユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持し、アクセス制御対象のホストの識別子とホストが接続された転送ノードまたはホストを使用するユーザの識別子とを紐付けるポリシー管理装置とを備え、転送ノードは自身に接続されたホストおよび自身の識別子の組をポリシー管理装置に送信し、認証装置は転送ノードに接続されたホストおよびユーザの識別子の組をポリシー管理装置に送信し、ポリシー管理装置は転送ノードに接続されたホストがアクセス制御対象である場合、アクセス制御の内容を制御装置に通知し、制御装置は該通知に応じて処理規則を生成して転送ノードに設定する。