

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2007 年 10 月 18 日 (18.10.2007)

PCT

(10) 国際公開番号
WO 2007/116605 A1

- (51) 国際特許分類:
H04L 12/66 (2006.01) G06F 21/20 (2006.01)
G06F 13/00 (2006.01) H04L 12/28 (2006.01)
- (21) 国際出願番号: PCT/JP2007/052322
- (22) 国際出願日: 2007 年 2 月 9 日 (09.02.2007)
- (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2006-093261 2006 年 3 月 30 日 (30.03.2006) 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 (米国についてののみ): 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). 伊

藤 正史 (ITO, Masashi) [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).
奥山 嘉昭 (OKUYAMA, Yoshiaki) [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).

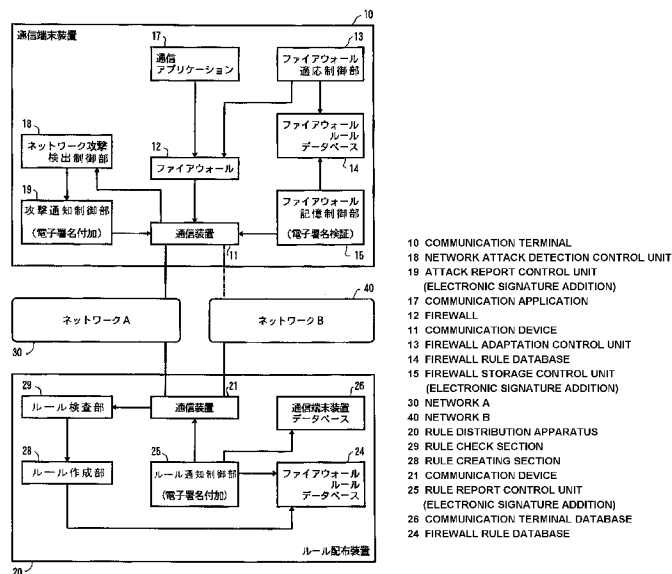
(74) 代理人: 宮崎 昭夫, 外 (MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂 1 丁目 9 番 2 0 号 第 1 6 興和ビル 8 階 Tokyo (JP).

(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, GT, 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, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[続葉有]

(54) Title: COMMUNICATION TERMINAL, RULE DISTRIBUTION APPARATUS AND PROGRAM

(54) 発明の名称: 通信端末装置、ルール配布装置およびプログラム



(57) Abstract: A communication terminal (10) comprises a communication device (11) for connection to a network and a firewall (12) functioning according to the firewall rule, a rule storage section (14) for holding the network identification information and the firewall rule in association with each other, a rule storage control unit (15) for storing the firewall rule received from a rule distribution apparatus (20) in association with the network identification information to which the rule is applied in the rule storage section (14) and a firewall control unit (13) for detecting and monitoring the network identification information and when identification information is newly detected or altered, reading the firewall rule associated with the detected or altered identification information from the rule storage section (14) to set it to the firewall (12) or to update it.

[続葉有]

WO 2007/116605 A1



(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).

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。

添付公開書類:

— 国際調査報告書

(57) 要約: 通信端末装置 10 は、ネットワークに接続するための通信装置 11 と、ファイアウォールルールに従って機能するファイアウォール 12 とを備え、ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部 14 と、ルール配布装置 20 から受信されるファイアウォールルールを適用すべきネットワークの識別情報に対応付けてルール記憶部 14 に記憶するルール記憶制御部 15 と、ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出又は変化すると当該検出又は変化した識別情報に対応付けられているファイアウォールルールをルール記憶部 14 から読み出してファイアウォール 12 に設定又は更新するファイアウォール制御部 13 とを有する。

明 細 書

通信端末装置、ルール配布装置およびプログラム

技術分野

- [0001] 本発明は、ファイアウォールを備えた通信端末装置、及び通信端末装置のプログラムに関する。また、ファイアウォールルールを各通信端末装置へ配布するルール配布装置、及びルール配布装置のプログラムに関する。

背景技術

- [0002] 近年、携帯電話網、無線LAN(Local Area Network)をはじめとする無線ネットワークの普及に伴い、移動端末装置を用いて多種多様なネットワークに接続するというユースケースが増大している。
- [0003] 多種多様なネットワークに端末を接続する場合、悪意を持った攻撃者によりネットワーク経由で端末が攻撃される恐れが高くなる。これを防御するために、端末内にパーソナルファイアウォール(以下ファイアウォール)機能を実装する方法がある。ファイアウォールは、端末とネットワークの間の通信を監視し、必要な通信のみを通過させ、不要な通信を遮断する。これにより、ネットワーク側からの不正な通信や攻撃を防御することができる。
- [0004] 従来、ファイアウォール機能は、おもにパーソナルコンピュータ上のソフトウェアとして実装されることが多く、携帯電話のような移動体通信端末装置に実装されることはあまりなかった。しかし、移動体通信端末装置は、セキュリティレベルの異なるネットワークを頻繁に切り替えて接続するため、移動体通信端末装置のファイアウォールには、あまり移動を想定していないパーソナルファイアウォールよりもさらに高度な機能が要求される。具体的には、ネットワークが切り替わったときに、切り替え先のネットワークのセキュリティレベルに応じてファイアウォールルールを迅速に切り替える必要がある。
- [0005] また、携帯電話のような移動体端末装置の利用者の多くは、ファイアウォールの設定などに精通していないので、ファイアウォールの設定を、携帯電話サービスの提供者が設定することが望まれる。特に、新種のコンピュータウィルスやワームが発生した

場合には、特定の攻撃が短時間のうちに増加するため、各通信端末装置のファイアウォールに速やかに攻撃を防御するためのルールを適用し、攻撃を未然に防御する必要がある。

[0006] (1)特開2004-094723号公報(特許文献1)には、ユーザのシステムがサービス提供会社のシステムに対してファイアウォールの設定変更データを要求すると、提供会社のシステムがユーザのシステムへ変更データを送信して、ファイアウォールの設定を変更することが記載されている。

[0007] (2)特開2005-191721号公報(特許文献2)には、無線LANネットワーク検出部が検出したネットワーク識別子に対応するネットワーク設定情報を持っていない場合に、当該無線LANに接続するための無線部とは異なる無線部を用いてディレクトリサーバにアクセスして当該無線LANのネットワーク設定情報をダウンロードして登録する機能を備えた無線端末装置が記載されている。

[0008] (3)特開2005-031720号公報(特許文献3)には、ユーザ毎にファイアウォールルールを記憶しており、接続に応じてファイアウォールルールを切り換えるファイアウォール装置が記載されている。

特許文献1:特開2004-094723号公報

特許文献2:特開2005-191721号公報

特許文献3:特開2005-031720号公報

発明の開示

発明が解決しようとする課題

[0009] 特許文献1や2に記載の設定変更方式は、何れも、ユーザからの要求に応じてサービス提供者が更新データを返す方式であるため、例えば、新種のコンピュータウィルスやワームが発生した場合等のように、緊急に各通信端末装置のファイアウォールルールを更新する必要性が生じたような場合に対応できない。従来方式で上記のような緊急事態に対応するためには、常時ユーザ側からポーリングを繰り返している必要があり、ネットワークの負荷が増大する。また、たいていは緊急事態ではないことに鑑みると、通信の大部分が無駄となってしまう。

[0010] 本発明は、新種のコンピュータウィルス等が発生したような緊急事態でも、各通信端

末装置のファイアウォールルールを速やかに更新できるようにすることを目的とする。

[0011] また、従来は、通信端末装置が攻撃を受けている場合、サービス提供者が、その事実や攻撃パターン或いは攻撃を受けているネットワークを速やかに知る手法が無い。このため例えば新種のネットワーク攻撃への対応も後手になりがちである。

[0012] 本発明は、ネットワーク攻撃を速やかに検出してファイアウォールルール更新等の対応を適時にとり得るようにすることを目的とする。

課題を解決するための手段

[0013] 本発明は、下記[1]～[11]のように構成される。

[0014] [1]構成1:

ネットワークに接続するための通信装置と、設定されているファイアウォールルールに従ってネットワークと自装置との間のデータの通過と遮断を制御するファイアウォールと、を備えた通信端末装置であって、

ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、

所定のルール配布装置から受信されるファイアウォールルールを、当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて前記ルール記憶部に記憶するルール記憶制御部と、

ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部と、

を有することを特徴とする通信端末装置。

[0015] [2]構成2:

構成1に於いて、

前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールにネットワークの識別情報が対応付けられている場合は当該識別情報をファイアウォールルールに対応付けて前記ルール記憶部に記憶し、前記ファイアウォールルールにネットワークの識別情報が対応付けられていない場合は前記ファイアウォール

ール制御部が検出している識別情報を前記ファイアウォールルールに対応付けて前記ルール記憶部に記憶する、

ことを特徴とする通信端末装置。

[0016] [3]構成3:

構成1に於いて、

前記ファイアウォール制御部は、前記ルール記憶部にファイアウォールルールとネットワークの識別情報が対応付けて記憶されると、当該識別情報を現在検出している識別情報と比較して、両者が合致する場合は当該識別情報に対応付けられたファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定されているファイアウォールルールを当該読み出したファイアウォールルールに更新する、

ことを特徴とする通信端末装置。

[0017] [4]構成4

構成1に於いて、

前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールであることを所定の電子署名を検証することで確認する、

ことを特徴とする通信端末装置。

[0018] [5]構成5:

構成1に於いて、さらに、

前記通信装置で受信されるデータを監視して所定のパターンに合致するネットワーク攻撃を検出する攻撃検出部と、

前記攻撃検出部がネットワーク攻撃を検出すると、該ネットワーク攻撃のパターン情報と前記ファイアウォール制御部が検出している識別情報とを対応付けて当該パターン情報と当該識別情報とを所定のルール配布装置へ宛てて送信する攻撃通知部と、

を有することを特徴とする通信端末装置。

[0019] [6]構成6:

構成5に於いて、

前記攻撃通知部は、前記ネットワーク攻撃のパターン情報に所定のルール配布装置が要求する電子署名を付して、当該パターン情報と前記識別情報とを送信する、ことを特徴とする通信端末装置。

[0020] [7]構成7:

ネットワークに接続するための通信装置を備えたルール配布装置であって、

ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、

管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部と、

前記ルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報を当該ファイアウォールルールに対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部と、

を有することを特徴とするルール配布装置。

[0021] [8]構成8:

構成7に於いて、

前記ルール通知部は、所定の電子署名を付して前記ファイアウォールルールと前記識別情報とを送信する、

ことを特徴とするルール配布装置。

[0022] [9]構成9:

構成7に於いて、

通信端末装置から受信されるネットワーク攻撃のパターン情報とネットワーク識別情報に基づいて、当該識別情報が対応付けられているファイアウォールルールで当該ネットワーク攻撃に対応可能か否かを調べるルール検査部と、

前記ルール検査部が対応不可と認定した場合は当該ネットワーク攻撃に対応可能なファイアウォールルールを作成するルール作成部と、

を更に有し、

前記ルール通知部は、前記ルール作成部が作成したファイアウォールルールに当

該ネットワークの識別情報を対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信する、

ことを特徴とするルール配布装置。

[0023] [10]構成10:

ネットワークに接続するための通信装置と、設定されているファイアウォールルールに従ってネットワークと自コンピュータとの間のデータの通過と遮断を制御するファイアウォールと、を備えたコンピュータを、

ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部に、所定のルール配布装置から受信されるファイアウォールルールを、当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて記憶するルール記憶制御部、

ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部、

として機能させるためのプログラム。

[0024] [11]構成11:

ネットワークに接続するための通信装置を備えたコンピュータを、

管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部、

ネットワークの識別情報とファイアウォールルールを対応付けてネットワーク毎に保持しているルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報を当該ファイアウォールルールに対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部、

として機能させるためのプログラム。

発明の効果

[0025] 構成1の通信端末装置は、ネットワークに接続するための通信装置と、設定されて

いるファイアウォールルールに従ってネットワークと自装置との間のデータの通過と遮断を制御するファイアウォールと、を備えた通信端末装置であって、ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、所定のルール配布装置から受信されるファイアウォールルールを当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて前記ルール記憶部に記憶するルール記憶制御部と、ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部と、を有する。このため、新種のコンピュータウィルス等が発生したような緊急事態でも、サービス提供者側からの更新データを受け入れてファイアウォールルールを速やかに更新することができる。

[0026] 構成2の通信端末装置は、構成1に於いて、前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールにネットワークの識別情報が対応付けられている場合は当該識別情報をファイアウォールルールに対応付けて前記ルール記憶部に記憶し、前記ファイアウォールルールにネットワークの識別情報が対応付けられていない場合は前記ファイアウォール制御部が検出している識別情報を前記ファイアウォールルールに対応付けて前記ルール記憶部に記憶する。このため、構成1が奏する効果に加えて、ネットワークの識別情報の対応付けについての具体的構成を与えることができる効果がある。

[0027] 構成3の通信端末装置は、構成1に於いて、前記ファイアウォール制御部は、前記ルール記憶部にファイアウォールルールとネットワークの識別情報が対応付けて記憶されると、当該識別情報を現在検出している識別情報と比較して、両者が合致する場合は当該識別情報に対応付けられたファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定されているファイアウォールルールを当該読み出したファイアウォールルールに更新する。このため、構成1が奏する効果に加えて、現在接続中のネットワークに関してファイアウォールルールが更新された場合は、直ちに、更新後のファイアウォールルールを設定できる効果がある。

- [0028] 構成4の通信端末装置は、構成1に於いて、前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールであることを所定の電子署名を検証することで確認する。このため、構成1が奏する効果に加えて、正規のファイアウォールルールの更新であることを確認できる効果がある。
- [0029] 構成5の通信端末装置は、構成1に於いて、さらに、前記通信装置で受信されるデータを監視して所定のパターンに合致するネットワーク攻撃を検出する攻撃検出部と、前記攻撃検出部がネットワーク攻撃を検出すると、該ネットワーク攻撃のパターン情報と前記ファイアウォール制御部が検出している識別情報とを対応付けて当該パターン情報と当該識別情報とを所定のルール配布装置へ宛てて送信する攻撃通知部と、を有する。このため、サービス提供者(ルール配布装置)は、各通信端末装置から受信される情報により、新種のネットワーク攻撃を速やかに検出してそのネットワーク攻撃に対応することができる。
- [0030] 構成6の通信端末装置は、構成5に於いて、前記攻撃通知部は、所定のルール配布装置が要求する電子署名を付して前記パターン情報と前記識別情報とを送信する。このため、サービス提供者(ルール配布装置)は、構成5が奏する効果に加えて、正規の通知であることを確認可能にする効果がある。
- [0031] 構成7のルール配布装置は、ネットワークに接続するための通信装置を備えたルール配布装置であって、ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部と、前記ルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報を当該ファイアウォールルールに対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部と、を有する。このため、新種のコンピュータウイルス等が発生したような緊急事態でも、各通信端末装置のファイアウォールルールを速やかに更新させることができる。
- [0032] 構成8のルール配布装置は、構成7に於いて、前記ルール通知部は、所定の電子署名を付して当該ファイアウォールルールと当該識別情報とを送信する。このため、

構成7が奏する効果に加えて、正規の更新であることを確認可能にする効果がある。

[0033] 構成9のルール配布装置は、構成7に於いて、通信端末装置から受信されるネットワーク攻撃のパターン情報とネットワーク識別情報に基づいて、当該識別情報が対応付けられているファイアウォールルールで当該ネットワーク攻撃に対応可能か否かを調べるルール検査部と、前記ルール検査手段が対応不可と認定した場合は当該ネットワーク攻撃に対応可能なファイアウォールルールを作成するルール作成部とを更に有し、前記ルール通知部は、前記ルール作成部が作成したファイアウォールルールに当該ネットワークの識別情報を対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信させる。このため、新種のネットワーク攻撃を各通信端末装置からの情報に基づいて速やかに検出して、ファイアウォールルール更新等の対応を適時にとり得るようにすることができる。

[0034] 構成10は、ネットワークに接続するための通信装置と、設定されているファイアウォールルールに従ってネットワークと自コンピュータとの間のデータの通過と遮断を制御するファイアウォールと、を備えたコンピュータを、ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部に、所定のルール配布装置から受信されるファイアウォールルールを、当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて記憶するルール記憶制御部、ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部、として機能させるためのプログラムである。このため、コンピュータを構成1の装置として機能させるためのプログラムを提供することができる。

[0035] 構成11は、ネットワークに接続するための通信装置を備えたコンピュータを、管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部、ネットワークの識別情報とファイアウォールルールを対応付けてネットワーク毎に保持しているルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報に対応付

けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部、として機能させるためのプログラムである。このため、コンピュータを構成7の装置として機能させるためのプログラムを提供することができる。

図面の簡単な説明

[0036] [図1]図1は、実施の形態の通信端末装置10とルール配布装置20を示した機能ブロック図である。

[図2]図2は、通信端末装置10のファイアウォールルールデータベース14と、ルール配布装置のファイアウォールルールデータベース24に保持されるルールテーブルの構成を示した説明図である。

符号の説明

- [0037]
- 10 通信端末装置
 - 11 通信装置
 - 12 ファイアウォール
 - 13 ファイアウォール適応制御部(ファイアウォール制御部)
 - 14 ファイアウォールルールデータベース(ルール記憶部)
 - 15 ファイアウォール記憶制御部(ファイアウォール制御部)
 - 18 ネットワーク攻撃検出制御部(攻撃検出部)
 - 19 攻撃通知制御部(攻撃通知部)
 - 20 ルール配布装置
 - 21 通信装置
 - 24 ファイアウォールルールデータベース(ルール記憶部)
 - 25 ルール通知制御部(ルール通知部)
 - 26 通信端末装置データベース
 - 28 ルール作成部(ルール作成部)
 - 29 ルール検査部(ルール検査部)

発明を実施するための最良の形態

[0038] 図面を参照して本発明の実施の形態を説明する。図1は、本発明の実施の形態の通信端末装置10およびルール配布装置20の構成を示すブロック図である。図1に

において、通信端末装置10は、ネットワークA30やネットワークB40に接続してネットワークサービスを受けるための通信端末装置である。

[0039] ネットワーク30、ネットワーク40としては、インターネット、イントラネット、無線LANスポット、家庭内LAN、店舗内LANなど、さまざまなネットワークが想定される。

[0040] 通信端末装置10は、通信装置11を使用してネットワーク30やネットワーク40に接続する。この際、通信端末装置10は、例えば有線LAN(Local Area Network)、無線LAN、公衆電話網、携帯電話網、PHS(Personal Handy-phone System)、IrDA(Infrared Data Association)、Bluetooth、シリアル通信等によって、ネットワーク30やネットワーク40に接続する。通信に使用するプロトコルは、TCP/IPである。

[0041] ファイアウォール12は、通信装置11を使用してネットワーク30やネットワーク40と通信する際に、不要な通信を遮断することで通信端末装置10の外部からの攻撃を防御するための手段である。具体的には、ファイアウォール12は、通信装置11を通過するTCP/IPのパケットの内容を確認し、不必要なパケットを廃棄することで不正な通信を遮断する。ファイアウォール12には、どのような種別の通信を遮断すべきかというファイアウォールルールが設定されている。ファイアウォールルールは、ファイアウォール適応制御部13によりファイアウォールルールデータベース14から読み出されて、ファイアウォール12設定される。ファイアウォール適応制御部13は、現在接続されているネットワーク(図1ではネットワーク30)の識別子を検出し、該識別子に対応するファイアウォールルールをファイアウォールルールデータベース14から読み出してファイアウォール12に設定する。

[0042] このため、ファイアウォールルールデータベース14内には、ファイアウォールルールが、図2(a)のルールテーブルに示すように、ネットワークの識別子に対応付けてネットワーク毎に保持されている。ネットワークの識別子としては、セルラ網の識別名(アクセスポイント名)、無線LANのESS-ID(Extended Service Set Identifier)、ネットワークのIPアドレスなどが使用できる。

[0043] 本発明では、ファイアウォールルールは、サービス提供側である配布装置20によって指定される。即ち、ルール配布装置20のルール通知制御部25が、ファイアウォールルールを管理しており、必要に応じて、管理下の各通信端末装置10のアドレスを

通信端末装置データベース26から読み出して、そのアドレスを用いてファイアウォールルールを配布する。本実施の形態では、ルール配布装置20は、ネットワーク30とネットワーク40とに共通に設けられているが、これに代えて、ルール配布装置20は、ネットワーク毎に設けられてもよい。

- [0044] 図1では、ファイアウォールルールは、ネットワーク30またはネットワーク40を使用して通信端末装置10に配布される。通信端末装置10では、ファイアウォール記憶制御部15が、通信装置11を経由して、このファイアウォールルールを受信して、このファイアウォールルールをファイアウォールルールデータベース14に登録する。ファイアウォールルールには電子署名が付与されており、ファイアウォールルール記憶制御部15内の署名検証制御部(電子署名検証部)が、この署名を検証する。
- [0045] ファイアウォールルールを、実際に通信するネットワークとは異なるネットワークから受信するように構成することも可能である。たとえば、無線LANを使って通信する際に、無線LANに対するファイアウォールルールを、携帯電話網の電子メールなどを用いて受信するように構成することも可能である。
- [0046] ネットワーク攻撃の検出と通知について述べる。
- [0047] 通信端末装置10は、前述の構成に加えて、ネットワーク攻撃検出制御部18と攻撃通知制御部19を更に有し、攻撃通知制御部19は電子署名付加機能を備えている。
- [0048] ネットワーク攻撃検出制御部18は、通信装置11に対して行われるネットワーク攻撃を検出する。これは一般的にはIDS(Intrusion Detection System, 侵入検知システム)と呼ばれるもので、通信パケットの内容がネットワーク攻撃パケットのパターンと一致するかどうかを、両者を比較することによって判定して、攻撃を検出するものである。
- [0049] 攻撃通知制御部19は、ネットワーク攻撃検出制御部18が攻撃を検出すると、その報告をルール配布装置20のルール検査部29へ送信する。この報告には、攻撃通知制御部19の電子署名付加機能が電子署名を付加している。
- [0050] ルール配布装置20のルール検査部29は、ネットワーク攻撃パケットのパターンや度数等を調べ、必要に応じて当該ネットワークに対応付けるべきファイアウォールルールをルール作成部28に作成／修正させ、ファイアウォールルールデータベース2

4のデータを更新する。ルール検査部29は、電子署名の検証も行なう。

[0051] 次に、動作を説明する。

[0052] 通信端末装置10の電源が投入されると、通信端末装置10は通信装置11を使用してネットワークに接続する。ここでは、通信端末装置10がネットワーク30に接続された場合を述べる。通信端末装置10がネットワーク30に接続されると、通信アプリケーション17が通信を開始する。この時、ファイアウォール12は、不必要な通信を遮断するように動作する。また、ファイアウォール記憶制御部15は、ルール配布装置20からのファイアウォールルールをいつでも受信できるように、待機状態に入る。

[0053] ルール配布装置20でファイアウォールルールが更新されると、ルール配布装置20のルール通知制御部25は、当該更新されたファイアウォールルールを、ネットワークを経由して通信端末装置10へ送信する。ここでは、ルール通知制御部25は、ネットワーク30を経由して通信端末装置10へファイアウォールルールを送信したものとする。

[0054] このとき、ルール通知制御部25は、ファイアウォールルールを電子メールに添付して送信したり、通信端末装置10内のファイアウォールルール記憶制御部15へ、直接、ファイアウォールルールのIPパケットを送信することで、ファイアウォールルールを配布するといった方式が考えられる。

[0055] 通信端末装置10では、ファイアウォールルール記憶制御部15が、当該ファイアウォールルールを、通信装置11経由で受信する。ファイアウォールルール記憶制御部15は、当該受信したファイアウォールルールの電子署名を、電子署名検証部を用いて検証する。この電子署名検証部は、ルール配布装置20のサーバ証明書或いは電子証明局の証明書を保持しており、これを用いて電子署名を検証する。検証の結果、正等な電子署名が付与されていない場合には、ファイアウォールルール記憶制御部15は、当該ファイアウォールルールを破棄する。

[0056] 一方、検証の結果、正当な電子署名が付されていた場合は、ファイアウォールルール記憶制御部15は、当該ファイアウォールルールを、ファイアウォールルールデータベース14に格納する。このとき、ファイアウォールルールにネットワークの識別子が付与されている場合は、ファイアウォールルール記憶制御部15は、この識別子と対応

づけてファイアウォールルールをファイアウォールルールデータベース14に格納する。このようにすることで、ネットワーク別にファイアウォールルールを設定することができる。また、ネットワーク識別子が付されていなかった場合は、ファイアウォールルール記憶制御部15は、ファイアウォールルールを受信したネットワーク、すなわちこの例ではネットワーク30を識別子として、これに対応付けてファイアウォールルールをファイアウォールルールデータベース14に格納する。こうすることで、現在接続中のネットワークに対応したファイアウォールルールを設定することができる。このように処理する構成は、ルール配布装置20がネットワーク毎にそれぞれ設けられている場合に有用である。

[0057] 新しく格納されたファイアウォールルールが、現在接続中のネットワークに対するルールである場合には、例えば、ファイアウォールルールデータベース14にファイアウォールルールとネットワークの識別情報が対応付けて記憶され、ファイアウォール適用制御部13が、その識別情報を現在検出している識別情報と比較して両者が合致する場合には、次に、ファイアウォール適応制御部13が、当該新しく格納されたファイアウォールルールをファイアウォールルールデータベース14から読み出して、ファイアウォール12に設定されているファイアウォールルールを、当該読み出したファイアウォールルールに更新する。ファイアウォール12は、以後、当該更新されたファイアウォールルールにしたがって通信の遮断処理を行う。

[0058] 通信端末装置10が、接続先のネットワークを切り換えた場合について説明する。

[0059] 通信装置11が接続先のネットワークをネットワーク30からネットワーク40に切り替えと、ファイアウォールルール適応制御部13が、その切換を検出し、ネットワーク40の識別子に対応付けられているファイアウォールルールをファイアウォールルールデータベース14から読み出して、ファイアウォール12に設定されているファイアウォールルールを、当該読み出したファイアウォールルールに更新する。以後、ファイアウォール12は、この切換後のファイアウォールルールにしたがって通信の遮断を行う。

[0060] このようにして、接続先のネットワークに適合するファイアウォールルールを動的に切り替える制御が行なわれる。

[0061] ネットワーク攻撃の検出時の動作について説明する。

- [0062] 通信端末装置10がネットワークに接続されると、ネットワーク攻撃検出制御部18が起動される。ネットワーク攻撃検出制御部18は、通信装置11を通過するパケットを精査して、攻撃パケットの特徴(所定のパターン)と一致しているものを探す。一致しているパケットが発見されると、攻撃通知制御部19は、そのパケット(ネットワーク攻撃のパターン情報)に、電子署名付加機能を用いて電子署名を付加して、ネットワーク経由で、電子署名が付加されたパケットをルール配布装置20のルール検査部29へ送信する。この時、攻撃通知制御部19は、攻撃が検出されたネットワークを指す識別子も対応付けて送信する。なお、電子署名付加機能では、ルール配布装置20が要求する電子署名が付加される。
- [0063] ルール配布装置20のルール検査部29は、ネットワーク攻撃の報告が受信されると、まず、電子署名を検証し、不正なものであれば当該報告を破棄する。一方、正当なものであった場合は、ルール検査部29は、この報告を受け入れ、この情報に応じて各ネットワークにおける攻撃の統計を取る。たとえば、ルール検査部29は、ネットワーク30ではTCPの80番ポートに対する攻撃が全通信端末装置の20%に対して発生している、といった統計を取る。
- [0064] ルール配布装置20のルール作成部28は、上記の情報を利用してファイアウォールルールを効果的に作成することができる。作成したファイアウォールルールは、ファイアウォールルールデータベース24に記録されて、ルール通知制御部25によって各通信端末装置10に配布される。なお、ファイアウォールルールを、人間が上記の統計情報を監視して手動で更新するようにしてもよく、ルール作成部28が自動的に更新するようにしてもよい。
- [0065] 実施の形態の効果について述べる。
- [0066] 上述した実施の形態では、ルール配布装置20が、通信端末装置10へファイアウォールルールを送信して更新させ得るため、ルール配布装置20が各通信端末装置10を集中管理しやすく、新種のコンピュータウィルス等が発生したような緊急事態でも、ファイアウォールルールを迅速に配布することができる。
- [0067] また、各通信端末装置10がファイアウォールルールを要求してダウンロードする方式に比べると、本方式では、ルール配布装置20がファイアウォールルールを各通信

端末装置10へ送信するため、全体の通信量を削減できる。また、ルール配布装置20の負荷も低減できる。

[0068] また、各通信端末装置10は、接続先のネットワークに応じてファイアウォールルールを動的に切り替えることができるので、ネットワークのセキュリティ状態に応じた最適なファイアウォール設定を使用することができる。

[0069] また、本実施の形態では、各通信端末装置10から送信されて来る攻撃に関する情報をルール配布装置20のルール検査部29が調べて、各通信端末装置10がどのネットワークでどのような攻撃を受けているか、すなわちネットワーク毎にどのような攻撃が発生しているかという情報を収集することができるため、これにより、ネットワーク毎に最適なファイアウォールのファイアウォールルールを手動あるいは自動的に更新し、迅速に端末に配布することができる。

[0070] なお、通信端末装置10は、プログラムにしたがって動作するコンピュータでもよい。このコンピュータは、通信装置11とファイアウォール12とファイアウォールルールデータベース14とを備える。また、このコンピュータは、そのプログラムを実行することによって、ファイアウォール記憶制御部15、ファイアウォール適用制御部13、ネットワーク攻撃検出制御部18および攻撃通知制御部19として機能する。

[0071] また、ルール配布装置20は、プログラムにしたがって動作するコンピュータでもよい。このコンピュータは、通信装置21とファイアウォールルールデータベース24とを備える。また、このコンピュータは、そのプログラムを実行することによって、ルール検査部29とルール作成部28とルール通知制御部25として機能する。

[0072] 以上説明した実施形態において、図示した構成は単なる一例であって、本発明はその構成に限定されるものではない。

請求の範囲

- [1] ネットワークに接続するための通信装置と、設定されているファイアウォールルールに従ってネットワークと自装置との間のデータの通過と遮断を制御するファイアウォールと、を備えた通信端末装置であって、
- ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、
- 所定のルール配布装置から受信されるファイアウォールルールを当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて前記ルール記憶部に記憶するルール記憶制御部と、
- ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部と、
- を有する通信端末装置。
- [2] 前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールにネットワークの識別情報が対応付けられている場合は当該識別情報をファイアウォールルールに対応付けて前記ルール記憶部に記憶し、前記ファイアウォールルールにネットワークの識別情報が対応付けられていない場合は前記ファイアウォール制御部が検出している識別情報を前記ファイアウォールルールに対応付けて前記ルール記憶部に記憶する、
- 請求の範囲1に記載の通信端末装置。
- [3] 前記ファイアウォール制御部は、前記ルール記憶部にファイアウォールルールとネットワークの識別情報が対応付けて記憶されると、当該識別情報を現在検出している識別情報と比較して、両者が合致する場合は当該識別情報に対応付けられたファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定されているファイアウォールルールを当該読み出したファイアウォールルールに更新する、
- 請求の範囲1に記載の通信端末装置。

- [4] 前記ルール記憶制御部は、所定のルール配布装置から受信されるファイアウォールルールであることを所定の電子署名を検証することで確認する、
請求の範囲1に記載の通信端末装置。
- [5] 前記通信装置で受信されるデータを監視して所定のパターンに合致するネットワーク攻撃を検出する攻撃検出部と、
前記攻撃検出部がネットワーク攻撃を検出すると、該ネットワーク攻撃のパターン情報に前記ファイアウォール制御部が検出している識別情報を対応付けて当該パターン情報と当該識別情報とを所定のルール配布装置へ宛てて送信する攻撃通知部と、
をさらに有する
請求の範囲1に記載の通信端末装置。
- [6] 前記攻撃通知部は、前記ネットワーク攻撃のパターン情報に所定のルール配布装置が要求する電子署名を付して送信する、
請求の範囲5に記載の通信端末装置。
- [7] ネットワークに接続するための通信装置を備えたルール配布装置であって、
ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部と、
管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部と、
前記ルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報を当該ファイアウォールルールに対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部と、
を有するルール配布装置。
- [8] 前記ルール通知部は、所定の電子署名を付して前記ファイアウォールルールと前記識別情報とを送信する、
請求の範囲7に記載のルール配布装置。
- [9] 通信端末装置から受信されるネットワーク攻撃のパターン情報とネットワーク識別情報に基づいて、当該識別情報が対応付けられているファイアウォールルールで当該

ネットワーク攻撃に対応可能か否かを調べるルール検査部と、

前記ルール検査部が対応不可と認定した場合は当該ネットワーク攻撃に対応可能なファイアウォールルールを作成するルール作成部と、

を更に有し、

前記ルール通知部は、前記ルール作成部が作成したファイアウォールルールに当該ネットワークの識別情報を対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信する、

請求の範囲7に記載のルール配布装置。

- [10] ネットワークに接続するための通信装置と、設定されているファイアウォールルールに従ってネットワークと自コンピュータとの間のデータの通過と遮断を制御するファイアウォールと、を備えたコンピュータを、

ネットワークの識別情報とファイアウォールルールとを対応付けてネットワーク毎に保持しているルール記憶部に、所定のルール配布装置から受信されるファイアウォールルールを当該ファイアウォールルールを適用すべきネットワークの識別情報に対応付けて記憶するルール記憶制御部、

ネットワークの識別情報を検出して監視するとともに該識別情報が新たに検出され又は変化すると当該検出され又は変化した識別情報に対応付けられているファイアウォールルールを前記ルール記憶部から読み出して前記ファイアウォールに設定し又は更新するファイアウォール制御部、

として機能させるためのプログラム。

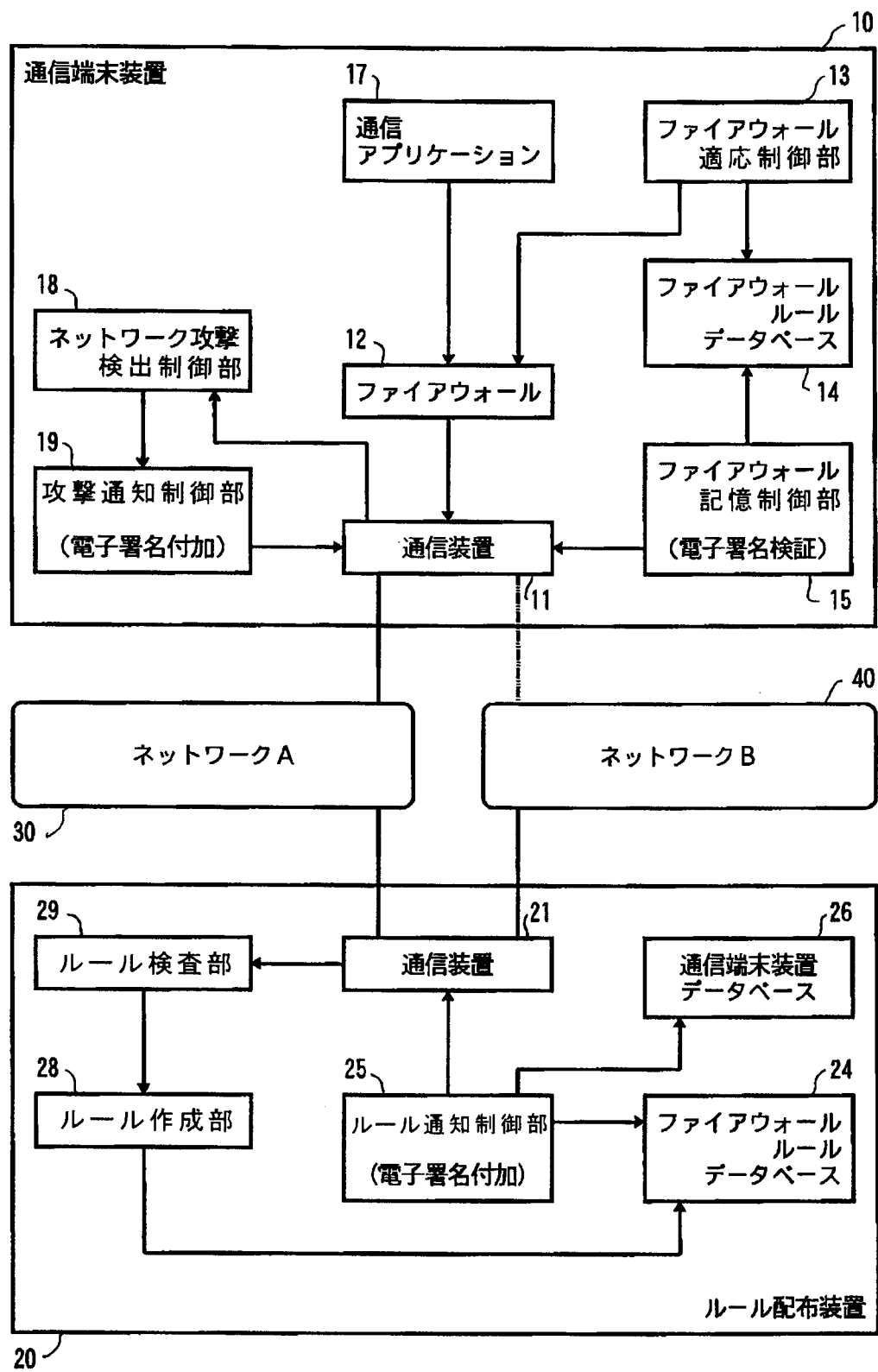
- [11] ネットワークに接続するための通信装置を備えたコンピュータを、

管理下にある通信端末装置のデータ送信先情報を通信端末装置毎に保持している端末装置記憶部、

ネットワークの識別情報とファイアウォールルールを対応付けてネットワーク毎に保持しているルール記憶部からファイアウォールルールを読み出して、必要に応じて当該ファイアウォールルールの適用対象のネットワークの識別情報を当該ファイアウォールルールに対応付けて、当該ファイアウォールルールと当該識別情報とを管理下の通信端末装置へ宛てて送信するルール通知部、

として機能させるためのプログラム。

[図1]



[図2]

(a) ルールテーブル

識別子	ファイアウォールルール
ネットワーク A	HTTP通信及びVoLP通信以外全て遮断
ネットワーク B	全て許可
ネットワーク C	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/052322

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/66(2006.01)i, G06F13/00(2006.01)i, G06F21/20(2006.01)i, H04L12/28(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)

H04L12/66, G06F13/00, G06F21/20, H04L12/28

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	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

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	Ikuo SAITO, "Uwasa no Taiketsu 07, Internet Security soft Sen", ASAHI Personal Computing, No.358, 01 May, 2004 (01.05.04), pages 58 to 63, page 76, 'Norton Internet Security 2004'	1-11
Y	Akiharu KONISHI, "Network no Kyoi kara PC o Mamore Teppeki Security no Hoteishiki, Phase 2 Hakai Katsudo o Osaekomu Technique, Sogo Security Soft o donyu suru", DOS/V magazine, Vol.13, No.2, 01 February, 2004 (01.02.04), pages 75 to 76, page 60, right column, line 5 to page 61, right column, the last line	1-11

☒ 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
02 March, 2007 (02.03.07)

Date of mailing of the international search report
13 March, 2007 (13.03.07)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2007/052322

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-273936 A (Kabushiki Kaisha Fasuto Torasuto), 26 September, 2003 (26.09.03), Page 4, right column, line 20 to page 6, left column, line 17 (Family: none)	1-11
A	JP 2004-266483 A (NEC Corp.), 24 September, 2004 (24.09.04), Claim 1 (Family: none)	1-11

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04L12/66(2006.01)i, G06F13/00(2006.01)i, G06F21/20(2006.01)i, H04L12/28(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. H04L12/66, G06F13/00, G06F21/20, H04L12/28

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	1971-2007年
日本国実用新案登録公報	1996-2007年
日本国登録実用新案公報	1994-2007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
Y	斎藤 幾郎, 噂の対決07 インターネット・セキュリティーソフト 戦, A S A H I パソコン, No. 358, 2004. 05. 01, p. 58-63 76 ページ「Norton Internet Security 2004」	1-11
Y	小西 晃治, ネットワークの脅威からPCを守れ 鉄壁セキュリティー の方程式 P h a s e 2 破壊活動を抑え込むテクニック 総合セ キュリティーソフトを導入する, D O S / V m a g a z i n e , Vol. 13, No. 2, 2004. 02. 01, p. 75-76 60 ページ右欄5行~61 ページ右欄最終行	1-11

☒ 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

02.03.2007

国際調査報告の発送日

13.03.2007

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)

衣嶋 文彦

5 X

9199

電話番号 03-3581-1101 内線 3596

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 請求の範囲の番号
Y	JP 2003-273936 A (株式会社ファーストトラスト) 2003. 09. 26, 4 ページ右欄 20 行～6 ページ左欄 17 行 (ファミリーなし)	1-11
A	JP 2004-266483 A (日本電気株式会社) 2004. 09. 24, 請求項 1 (ファミリーなし)	1-11