【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年8月11日(2005.8.11)

【公開番号】特開2003-85059(P2003-85059A)
【公開日】平成15年3月20日(2003.3.20)
【出願番号】特願2002-68762(P2002-68762)
【国際特許分類第７版】
　Ｇ０６Ｆ　13/00
　Ｇ０６Ｆ　15/00
　Ｈ０４Ｌ　12/46
　Ｈ０４Ｌ　12/66
【ＦＩ】
　Ｇ０６Ｆ　13/00　　３５１Ｚ
　Ｇ０６Ｆ　15/00　　３３０Ａ
　Ｈ０４Ｌ　12/46　　Ｅ
　Ｈ０４Ｌ　12/66　　Ｂ

【手続補正書】
【提出日】平成17年1月27日(2005.1.27)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、
　前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、
　前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、
　前記データ処理部は、
　　少なくとも前記通信データを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、
　　前記ユーザ識別データを認証する認証機能部と、
　　前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証機能部で認証を受けた使用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理機能部と、
　　前記ディレクトリ管理機能部で前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定機能部とを含む、ファイアウォール装置。
【請求項２】
　前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記サーバから送信され少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータによって登録されることを特徴とする、請求項１に記載のファイアウォール装置。
【請求項３】

前記サービスデータは、前記サーバのサービスが使用不可であることを示すサービス抹消データをさらに含み、
前記ディレクトリ管理機能部の前記サービス情報は、前記サービス抹消データによって該当するサービスが抹消されることを特徴とする、請求項２に記載のファイアウォール装置。
【請求項４】
前記サービスデータは、前記公開先データを変更する公開先変更データをさらに含み、
前記ディレクトリ管理機能部の前記サービス情報は、前記公開先変更データによって該当するサービスに接続可能な外部の使用者が変更されることを特徴とする、請求項２に記載のファイアウォール装置。
【請求項５】
前記サービスデータは、前記サーバを固定的に識別するサーバ識別情報をさらに含み、
前記ディレクトリ管理機能部は、前記サービス情報を前記サーバ識別情報基づいて関連付けられた前記内部アドレスを更新することを特徴とする、請求項２に記載のファイアウォール装置。
【請求項６】
前記ディレクトリ管理機能部に登録されている前記サービス情報は、前記ディレクトリ管理機能部が前記サーバから取得する、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて登録されることを特徴とする、請求項１に記載のファイアウォール装置。
【請求項７】
前記ディレクトリ管理機能部は、少なくとも前記内部アドレスと前記サービス種別とが含まれたサービスデータに基づいて前記サービス情報を登録し、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記サービスデータに係る公開先データを自動生成することを特徴とする、請求項１に記載のファイアウォール装置。
【請求項８】
前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。
【請求項９】
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。
【請求項１０】
前記ディレクトリ管理機能部は、前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが存在しない場合に適用される初期公開先データを格納する初期公開先データ格納手段を含み、
前記サーバが有する前記内部アドレスと前記サービス種別とに関連付けられる前記公開先データが前記ディレクトリ管理機能部に存在しない場合、前記ディレクトリ管理機能部は、現時点において管理している前記公開先データの中から、前記サービスデータに対して一部の条件を除いて条件が一致する前記公開先データを選出し、当該選出された公開先

データの数が所定数以上である場合には、当該選出された公開先データに基づいて、当該サービスデータに係る公開先データを新たに作成し、一方、当該選出された公開先データの数が所定数以上でない場合には、前記初期公開先データに基づいて、当該サービスデータに係る前記公開先データを新たに生成することを特徴とする、請求項７に記載のファイアウォール装置。

【請求項１１】

前記ディレクトリ管理機能部への前記サービス情報の登録は、予め設定された時間が経過することにより抹消されることを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１２】

前記通信路設定機能部は、

さらに設定した前記通信路を通るデータを監視し、

予め設定された期間に前記通信路をデータが通らないとき、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１３】

前記通信路設定機能部は、前記外部端末から送信され前記サーバとのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１４】

前記通信路設定機能部は、前記サーバから送信され前記外部端末とのサービス通信の終了を示すサービス通信終了データを受信することにより、前記通信路を解除することを特徴とする、請求項１に記載のファイアウォール装置。

【請求項１５】

外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール装置であって、

前記サーバから送信され少なくとも前記サーバが有する内部アドレスとサービス種別とが含まれたサービスデータを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理部と、

前記データ処理部で設定された前記通信路に基づいて、前記サーバと前記外部端末とを接続するスイッチ部とを備え、

前記データ処理部は、

少なくとも前記サービスデータを受信し、そのデータ内容に応じて各機能部に処理を依頼する通信部と、

前記内部アドレスと前記サービス種別と前記サーバに接続可能な前記外部端末を示す予め設定された公開先データとを関連付けてサービス情報として登録するディレクトリ管理機能部と、

前記サービス情報が登録された時に、前記公開先データに該当する前記外部端末が有する外部アドレスと前記サーバの前記内部アドレスとを用いて前記通信路を設定する通信路設定機能部とを含む、ファイアウォール装置。

【請求項１６】

前記ディレクトリ管理機能部に設定される前記公開先データは、前記サーバに対して全ての前記外部端末が接続可能であることを特徴とする、請求項１５に記載のファイアウォール装置。

【請求項１７】

外部ネットワークを介して外部端末と接続された複数のサーバを有する内部ネットワークに対する外部からの不正なアクセスを遮断するファイアウォール設定方法であって、

前記外部端末から送信され少なくとも外部端末が有する外部アドレスと前記外部端末の使用者を識別するユーザ識別データとを含んだ通信データを処理し、前記サーバおよび前記外部端末に対して通信路を設定する接続先を決定するデータ処理ステップと、

前記データ処理ステップで設定された前記通信路に基づいて、前記サーバと前記外部端

末とを接続する接続ステップとを備え、

前記データ処理ステップは、

少なくとも前記通信データを受信し、そのデータ内容に応じて各ステップに処理を依頼する通信ステップと、

前記ユーザ識別データを認証する認証ステップと、

前記サーバが有する内部アドレスとサービス種別と前記サーバに接続可能な外部の使用者を示す予め設定された公開先データとを関連付けてサービス情報として登録し、前記認証ステップで認証を受けた使用者に対して接続可能な前記サービス情報から選択させるディレクトリ管理ステップと、

前記ディレクトリ管理ステップで前記サービス情報から選択された前記サーバの前記内部アドレスと前記外部端末の前記外部アドレスとを用いて前記通信路を設定する通信路設定ステップとを含む、ファイアウォール設定方法。