(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3687782号
(P3687782)
(45)発行日　平成17年8月24日(2005.8.24)　(24)登録日　平成17年6月17日(2005.6.17)

(51)Int.Cl.[7]	F I		
H04L 12/56	H04L	11/20	102D
G06F 12/00	G06F	12/00	537Z
G06F 12/14	G06F	12/14	310Z
G06F 13/00	G06F	13/00	351Z
G06F 15/00	G06F	15/00	330A

請求項の数 9　(全 10 頁)　最終頁に続く

(21)出願番号　特願2000-299556(P2000-299556)
(22)出願日　平成12年9月29日(2000.9.29)
(65)公開番号　特開2002-111727(P2002-111727A)
(43)公開日　平成14年4月12日(2002.4.12)
審査請求日　平成15年2月10日(2003.2.10)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100084870
弁理士　田中　香樹
(74)代理人　100079289
弁理士　平木　道人
(72)発明者　竹森　敬祐
埼玉県上福岡市大原２－１－１５　株式会社ケイディディ研究所内
(72)発明者　田中　俊昭
埼玉県上福岡市大原２－１－１５　株式会社ケイディディ研究所内

最終頁に続く

(54)【発明の名称】不正侵入防止システム

(57)【特許請求の範囲】

【請求項１】

おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、

前記正規サーバと外部端末との間に確立された通信セッションが不正侵入に因るものであるか否かを判定する不正侵入監視手段と、

不正侵入と判定された通信セッションを、正規サーバからおとりサーバに引継がせる通信セッション引継手段と、

前記不正侵入と判定された通信セッションにおいて、正規サーバ宛のデータパケットをおとりサーバに転送する経路切換手段と、

前記おとりサーバから出力される応答パケットの内容を、前記正規サーバが前記データパケットを受信すれば出力するであろう応答パケットの内容に変換する応答変換手段とを具備し、

前記応答変換手段は、おとりサーバから出力される応答パケットの発信元アドレスを正規サーバのアドレスに変換する手段を含むことを特徴とする不正侵入防止システム。

【請求項２】

前記おとりサーバは正規サーバのミラーサーバであることを特徴とする請求項１に記載の不正侵入防止システム。

【請求項３】

前記通信セッション引継手段は、正規サーバ宛のデータパケットと同一のデータパケッ

トを前記おとりサーバへ順次転送する転送用バッファと、前記データパケットに応答して前記おとりサーバから返送された応答パケットを順次記憶する返送用バッファとを具備し、前記返送用バッファは、前記不正侵入と判定された通信セッションがおとりサーバに引継がれると、引継後の最初のデータパケットに対応した応答パケットから順に出力することを特徴とする請求項１または２に記載の不正侵入防止システム。

【請求項４】

前記通信セッション引継手段は、前記正規サーバ宛のデータパケットと同一のデータパケットを順次記憶する転送用バッファと、前記おとりサーバから返送された応答パケットを順次返送する返送用バッファとを具備し、前記転送用バッファは、前記不正侵入と判定された通信セッションがおとりサーバに引継がれると、引継後の最初のデータパケットから順に出力することを特徴とする請求項１または２に記載の不正侵入防止システム。

【請求項５】

サーバ機能を喪失させるコマンドを含むデータパケットに関してはおとりサーバへ転送せず、当該データパケットの応答パケットを疑似的に生成して返送する疑似応答手段を具備したことを特徴とする請求項１ないし４のいずれかに記載の不正侵入防止システム。

【請求項６】

不正侵入と判定された通信セッションの発信元アドレスを記憶し、次に当該発信元アドレスを有するデータパケットが入力されると、おとりサーバとの間に通信セッションを確立することを特徴とする請求項１ないし５のいずれかに記載の不正侵入防止システム。

【請求項７】

前記おとりサーバとの間に確立された通信セッションにおいて、その行動ログないしは追跡データを収集することを特徴とする請求項１ないし６のいずれかに記載の不正侵入防止システム。

【請求項８】

おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、前記正規サーバを宛先とするデータパケットが、不正侵入者から送出されたものであるか否かを判定する不正侵入監視手段と、不正侵入者から送出されたものと判定されたデータパケットをおとりサーバに転送する経路切換手段と、

前記おとりサーバから出力される応答パケットの内容を、前記正規サーバが前記データパケットを受信すれば出力するであろう応答パケットの内容に変換する応答変換手段とを具備し、

前記応答変換手段は、おとりサーバから出力される応答パケットの発信元アドレスを正規サーバのアドレスに変換する手段を含むことを特徴とする不正侵入防止システム。

【請求項９】

前記おとりサーバは正規サーバのミラーサーバであることを特徴とする請求項８に記載の不正侵入防止システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上のデータ端末に悪意の第三者が不正侵入し、さらにはその内容を改竄、破壊等することを防止する不正侵入防止システムに係り、特に、不正侵入者に不正侵入の失敗を悟られること無く、これを確実に防止できる不正侵入防止システムに関する。

【０００２】

【従来の技術】

近年、ホームページの改竄に代表される情報管理サーバへの不正侵入が後を立たない。このような問題点を解決するために、従来は、不正侵入者の通信セッションを情報管理サーバ内に侵入させない対策が講じられていた。例えば、情報管理サーバの不必要なポートを閉めることで攻撃されやすい経路を塞いだり、ファイアーウォールを設けて不正侵入者の

通信セッションをフィルタリングしたり、あるいは不正侵入者の通信セッションを切断することなどが行われてきた。

【０００３】

しかしながら、上記した従来の侵入防止システムでは、不正侵入者は侵入に失敗したことを認知できるため、他の侵入方法で再度侵入を試みたり、あるいは侵入を諦める代わりに大量の通信セッションを集中させ、サーバをダウンさせるなどの破壊工作や妨害工作に転じる場合があった。

【０００４】

このような技術課題を解決するために、本来の情報管理サーバの近傍に、故意に侵入し易くしたおとりサーバを配置し、当該おとりサーバでの改竄を許容することで、情報管理サーバへの不正侵入を防止すると共に、不正侵入者に不正侵入の失敗を悟られないようにした技術が提案されている（Network Associates社製のCyberCop Sting：米国）。

【０００５】

【発明が解決しようとする課題】

上記した従来技術では、サーバにおとり機能をインストールして仮想的なネットワークあるいはおとりサーバを作り出し、この仮想的なおとりサーバ等への通信設定を正規サーバよりも簡単にすることで、不正侵入者をおとりサーバ等へおびき寄せていた。

【０００６】

しかしながら、前記おとり機能が作り出すおとりサーバ等は、その挙動が本来のサーバとは微妙に異なるために見破られてしまう可能性があった。このため、改めて正規サーバを攻撃されると、従来と同様に正規サーバへ侵入されてしまうという問題があった。

【０００７】

本発明の目的は、上記した従来技術の課題を解決し、正規サーバへの不正侵入を防止し、かつ不正侵入者に不正侵入の失敗を悟られないようにした不正侵入防止システムを提供することにある。

【０００８】

【課題を解決するための手段】

上記した目的を達成するために、本発明は、おとりサーバを正規サーバに併設し、前記正規サーバへの不正侵入を前記おとりサーバへ導く不正侵入防止システムにおいて、前記正規サーバと外部端末との間に確立された通信セッションが不正侵入に因るものであるか否かを判定する不正侵入監視手段と、不正侵入と判定された通信セッションを、正規サーバからおとりサーバに引継がせる通信セッション引継手段と、前記不正侵入と判定された通信セッションにおいて、正規サーバ宛のデータパケットをおとりサーバに転送する経路切換手段とを具備したことを特徴とする。

【０００９】

上記した特徴によれば、正規サーバとの間に確立された通信セッションが不正侵入に因るものと判定されると、当該通信セッションがおとりサーバに引継がれ、それ以後は、正規サーバ宛のデータパケットがおとりサーバに転送されるので、正規サーバを不正侵入から守ることができる。さらに、正規サーバとの間に確立された通信セッションがおとりサーバに引継がれるので、不正侵入者に不正侵入の失敗を悟られない。したがって、正規サーバを、同一の不正侵入者による更なる不正侵入行為、破壊行為あるいは迷惑行為等からも守ことができる。

【００１０】

【発明の実施の形態】

以下、図面を参照して本発明を詳細に説明する。図１は、本発明の不正侵入防止システムが適用される通信ネットワークの構成を示したブロック図である。

【００１１】

通信ネットワーク１には、複数の通信端末５と共に、悪意の第三者による不正侵入から保護すべき正規サーバ３と、前記正規サーバ３に対する不正アクセスを身代わりとなって受け入れるおとりサーバ４とが、経路切換装置としてのルータ２（あるいはスイッチングハ

ブ、帯域制御装置等）を介して接続されている。前記おとりサーバ４は正規サーバ３のミラーサーバとしての機能を有する。

【００１２】

図２は、前記ルータ２、正規サーバ３およびおとりサーバ４の構成を示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００１３】

ルータ２において、ネットワークインターフェース（Ｉ／Ｆ）２０は、当該ルータ２と通信ネットワーク１との物理的な接続を制御する。アドレス変換部２１は、例えばＮＡＴ（Network Address Translator）としての機能を具備し、メモリ２１１に記憶されたアドレス対応情報に基づいて、入出力されるデータパケットのアドレス情報を書き換える。前記メモリ２１１に記憶された前記アドレス対応情報は、後述する正規サーバ３の不正侵入監視部３１からの書き換え指示により書き換えられる。経路切換部２２は、入力されたデータパケットを、その宛先アドレスに基づいて、正規サーバ３またはおとりサーバ４、あるいはその双方へ転送する。

【００１４】

正規サーバ３において、通信アプリケーション部３０は、入力されたデータパケットに登録されているコマンドを実行する。不正侵入監視部３１（例えば、Internet Security Systems 社製のReal Secure ：米国）は、パスワードが設定されているときに、その間違え回数が基準値を越えたアクセスや、ポートスキャンを実行したアクセス等を不正侵入者によるアクセスと判定し、その旨を前記通信アプリケーション部３０、ルータ２および後述する通信セッション引継部４１へ通知する。

【００１５】

おとりサーバ４において、その主要部である通信アプリケーション部４０は、入力されたデータパケットに登録されているコマンドを、前記正規サーバ３の通信アプリケーション部３０と同様に実行する。通信セッション引継部４１は、後に詳述するように、不正侵入者と正規サーバ３との通信セッションを正規サーバ３から引継いで継続させる。

【００１６】

図３、４は、本発明におけるデータパケットの転送経路を模式的に示した図であり、図３は、正規利用者あるいは不正侵入と判定されるまでの不正侵入者による通信セッションを示し、図４は、不正侵入と判定された以降の不正侵入者による通信セッションを示している。

【００１７】

図５は、本発明における通信シーケンスの第１実施形態を示した図であり、ここでは、正規サーバ３の通信アプリケーション部３０とおとりサーバ４の通信アプリケーション部４０とが同期して動作する。

【００１８】

図３に示したように、正規利用者または不正侵入者が、いずれかの通信端末５から正規サーバ３のアドレスを指定してデータパケットを送出すると、ルータ２の経路変換部２２は、受信したデータパケットを正規サーバ３［図５(a)］およびおとりサーバ４［同図(b)］の双方へ転送する。

【００１９】

正規サーバ３では、通信アプリション部３０が前記データパケットを受信し、前記通信端末５との間に通信セッションを確立させる。通信アプリション部３０は、データパケットに登録されているコマンドを実行して応答パケットを出力［同図(c)］する。この応答パケットは、ルータ２を経由して発信元の通信端末５へ返送される。不正侵入監視部３１は、入力されるデータパケットを監視［同図(d)］し、前記通信端末５の利用者が不正侵入者であるか否かを判定する。

【００２０】

これと平行して、おとりサーバ４の通信セッション引継部４１では、図３に示したように、ルータ２から転送されたデータパケットが転送用バッファ４１１に格納（バッファリン

グ）され［図５(e)］、おとりサーバ４の通信アプリケーション部４０へ転送［同図(f)］される。

【００２１】

通信アプリケーション部４０は、入力されたデータパケットに登録されているコマンドを実行し、その応答パケットを生成して通信セッション引継部４１へ返送［同図(g)］する。当該応答パケットは、通信セッション引継部４１の返送用バッファに４１２に格納［同図(h)］されるが、この時点ではルータ２に対して返送されない。

【００２２】

当該通信セッションが正規利用者によるものであり、不正侵入監視部３１により不正侵入が検知されなければ、上記した各処理が繰り返されることになる。

【００２３】

これに対して、当該通信セッションが不正侵入者によるものであり、これが前記不正侵入監視部３１により検知されると、正規サーバ３の通信アプリケーション部３０に対しては、通信アプリケーションを終了させるためのコマンドが通知［同図(i)］され、ルータ２および通信セッション引継部４１に対しては、不正侵入を検知した旨が通知［同図(j),(k)］される。正規サーバ３の通信アプリケーション部３０は、前記通知を検知すると、実行中の通信セッションを終了し、その旨を不正侵入監視部３１へ通知［同図(l)］する。

【００２４】

通信セッション引継部４１は、前記通知を、不正侵入と判定された最初のデータパケットのパケット番号と共に不正侵入監視部３１から受信すると、図４に示したように、その返送用バッファ４１２に蓄積されている、前記パケット番号に対応した応答パケットから順にルータ２へ出力［図５(m)］する。

【００２５】

このように、本実施形態では、おとりサーバ４に通信セッション引継部４１を設け、不正侵入者に対する応答パケットを、不正侵入と判定された最初のデータパケットから順に出力するようにしたので、不正侵入者と正規サーバ３との通信セッションをおとりサーバ４に正常に引継がせて継続させることができる。

【００２６】

ルータ２では、前記アドレス変換部２１が、返送用バッファ４１２から出力された応答パケットの内容を、正規サーバ３がデータパケットを受信すれば出力するであろう応答パケットの内容に変換して返送［同図(n)］する。すなわち、応答パケットの発信元アドレスを、おとりサーバ４のアドレスから正規サーバ３のアドレスに変換し、応答パケットのコマンドを、正規サーバ３へのアクセスに成功した旨のコマンドに変換する。

【００２７】

したがって、不正侵入者は発信元アドレスが正規サーバである応答パケットを受け取ることになるので、正規サーバ３への不正侵入者に失敗したことを認識できない。

【００２８】

これ以後は、当該通信セッション内で通信端末５から出力されるデータパケット［同図(o)］の宛先アドレスは、ルータ２のアドレス変換部２１において、全ておとりサーバ４のアドレスに書き換えられるのでおとりサーバ４に転送［同図(p)］される。したがって、正規サーバ３への不正侵入を防止できる。さらに、おとりサーバ４から返送［同図(q)］される応答パケットも、ルータ２のアドレス変換部２１において、その発信元アドレスを全て正規サーバ３のアドレスに書き換えられて出力［同図(r)］されるので、正規サーバ３への不正侵入者に失敗したことを不正侵入者に悟られない。

【００２９】

上記したように、本実施形態によれば、不正侵入と判定された通信セッションのデータパケットは、その宛先アドレスを正規サーバのアドレスからおとりサーバのアドレスへ書き換えられるので、正規サーバ３への侵入を防止できる。また、不正侵入者はおとりサーバ４に侵入しているにもかかわらず、正規サーバ３への侵入に成功したものと勘違いし、比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収

集が可能になる。さらに、不正侵入者には正規サーバ３への侵入に失敗したことを悟られないので、この不正侵入者による再度の侵入行為や他の妨害行為、破壊行為、迷惑行為等を防止できる。

【００３０】

図６は、本発明による通信シーケンスの第２実施形態を示した図である。上記した第１実施形態では、正規サーバ３の通信アプリケーション部３０とおとりサーバ４の通信アプリケーション部４０とが同期していたが、本実施形態では両者が非同期に動作し、おとりサーバ４は、不正侵入監視部３１により不正侵入が検知されてからデータパケットを読み込んでコマンドを実行する。

【００３１】

図３に示したように、正規利用者または不正侵入者が、いずれかの通信端末５から正規サーバ３のアドレスを指定してデータパケットを送出すると、ルータ２の経路変換部２２は、受信したデータパケットを、正規サーバ３［図６(a)］およびおとりサーバ４［同図(b)］の双方へ転送する。

【００３２】

正規サーバ３では、通信アプリション部３０が前記データパケットを受信し、前記通信端末５との間に通信セッションを確立させる。通信アプリション部３０は、データパケットに登録されているコマンドを実行して応答パケットを出力［同図(c)］する。この応答パケットは、ルータ２を経由して発信元の通信端末５へ返送される。不正侵入監視部３１は、入力されるデータパケットを監視［同図(d)］し、前記通信端末５の利用者が不正侵入者であるか否かを判定する。

【００３３】

これと平行して、おとりサーバ４の通信セッション引継部４１では、ルータ２から転送されたデータパケットが転送用バッファ４１１に格納［同図(e)］されるが、通信アプリション部４０へは転送されない。当該通信セッションが正規利用者によるものであれば、上記した各処理が繰り返されることになる。

【００３４】

これに対して、当該通信セッションが不正侵入者によるものであり、これが前記不正侵入監視部３１により検知されると、通信アプリケーション部３０に対しては、通信アプリケーションを終了するコマンドが通知［同図(i)］され、ルータ２および通信セッション引継部４１に対しては、不正侵入を検知した旨が通知［同図(j),(k)］される。

【００３５】

正規サーバ３の通信アプリケーション部３０は、前記通知を検知すると実行中の通信セッションを終了する。通信セッション引継部４１は、不正侵入が検知された旨を、当該不正侵入と判定された最初のデータパケットのパケット番号と共に受信し、その送信用バッファ４１２にバッファリングされている、当該パケット番号に対応したデータパケットから順におとりサーバ４の通信アプリケーション部４０へ転送［同図(f)］する。

【００３６】

通信アプリケーション部４０は、当該データパケットに登録されているコマンドを実行して応答パケットを生成し、これを通信セッション引継部４１へ返送［同図(g)］する。当該応答パケットは、通信セッション引継部４１を介してルータ２へ転送［同図(m)］される。ルータ２では、前記アドレス変換部２１が応答パケットの内容を、正規サーバ３がデータパケットを受信すれば出力するであろう応答パケットの内容に変換して返送［同図(n)］する。

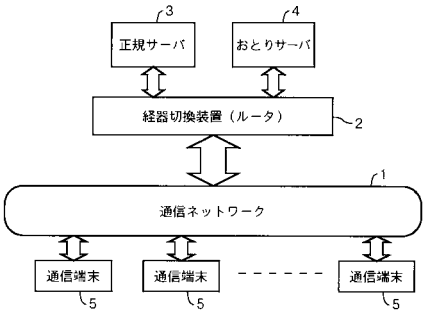
【００３７】

これ以後は、当該通信セッション内で通信端末５から出力されるデータパケット［同図(o)］の宛先アドレスは、ルータ２のアドレス変換部２１において全ておとりサーバ４のアドレスに書き換えられるので、正規サーバ３への不正侵入を防止できる。さらに、おとりサーバ４から不正侵入者に返送される応答パケット［同図(q)］の発信元アドレスも、ルータ２のアドレス変換部２１において全て正規サーバ３のアドレスに書き換えられるので

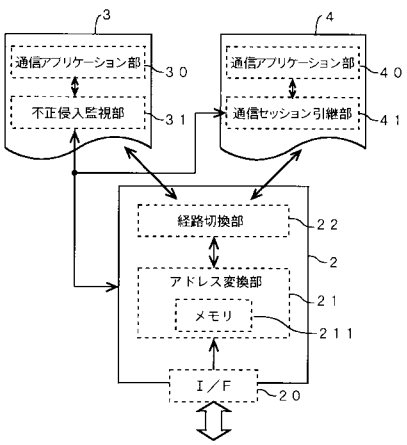
、正規サーバ３への不正侵入者に失敗したことを不正侵入者に悟られない。
【００３８】
なお、上記した各実施形態では、不正侵入監視部３１を正規サーバ３内に設け、通信セッション引継部４１をおとりサーバ４内に設けるものとして説明したが、本発明はこれのみに限定されるものではなく、正規サーバ３およびおとりサーバ４の各通信アプリケーション部３０、４０と通信ネットワーク１との間であれば、どのような形態で設けても良い。
【００３９】
さらに、上記した各実施形態では、不正侵入と判定されたセッションのデータパケットは全ておとりサーバ４へ転送するものとして説明したが、データの消去コマンドのように、おとりサーバ４の機能を喪失させるような危険なコマンドを含むデータパケットに関しては、おとりサーバ４へも侵入させないことが望ましい。
【００４０】
そこで、本実施形態では、図７に示したように、サーバ４の機能を喪失させるような危険なデータパケットはおとりサーバ４の通信アプリケーション部４０へ転送せず、通信セッション引継部４１が応答パケットを生成・返送して疑似的に応答［同図(s)］し、さらには、ルータ２のアドレス変換部２１において、その発信元アドレスを全て正規サーバ３のアドレスに書き換えて出力［同図(r)］する。このような構成によれば、おとりサーバ４を、その機能を喪失さるような危険な不正行為から守ることができる。
【００４１】
さらに、上記した各実施形態では、通信端末５からのアクセスに対して、最初は正規サーバ３との間に通信セッションを確立し、不正侵入が検知された時点で、当該通信セッションをおとりサーバ４に引継がせるものとして説明したが、不正侵入と判定されたアクセスの発信元アドレスを全て記憶しておき、次に同一の発信元アドレスを有するアクセスが検知された場合には、その通信セッションを最初からおとりサーバ４との間に確立させるようにしても良い。
【００４２】
【発明の効果】
本発明によれば、以下のような効果が達成される。
(1) 正規サーバとの間に確立された通信セッションが不正侵入に因るものと判定されると、当該通信セッションがおとりサーバに引継がれ、それ以後は、正規サーバ宛のデータパケットが全ておとりサーバに転送されるので、正規サーバを不正侵入から守ることができる。
(2) 不正侵入者はおとりサーバに侵入しているにもかかわらず、正規サーバへの侵入に成功したものと勘違いし、データを改竄あるいは破壊する。このため、不正侵入者は比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収集が可能になり、その結果、不正侵入者の特定が可能になる。
(3) 不正侵入者には、正規サーバへの侵入に失敗したことを悟られないので、この不正侵入者による再度の侵入行為、あるいは他の妨害行為や破壊行為等を防止できる。
(4) おとりサーバの機能を喪失させ得る危険なコマンドについては、おとりサーバへ転送することなく、疑似的に応答するようにしたので、おとりサーバの機能喪失を防止できるようになる。
【図面の簡単な説明】
【図１】　本発明の不正侵入防止システムが適用されるネットワークの構成を示したブロック図である。
【図２】　図１の主要部の構成を示したブロック図である。
【図３】　本発明におけるデータパケットおよび応答パケットの流れ（不正侵入検知前）を示した図である。
【図４】　本発明におけるデータパケットおよび応答パケットの流れ（不正侵入検知後）を示した図である。
【図５】　第１実施形態の通信シーケンスを示した図である。

【図６】　第２実施形態の通信シーケンスを示した図である。
【図７】　第３実施形態の通信シーケンスを示した図である。
【符号の説明】
１…通信ネットワーク，２…ルータ，３…正規サーバ，４…おとりサーバ，５…通信端末，２０…ネットワークインターフェース，２１…アドレス変換部，２２…経路切換部，３１…不正侵入監視部，４１…通信セッション引継部

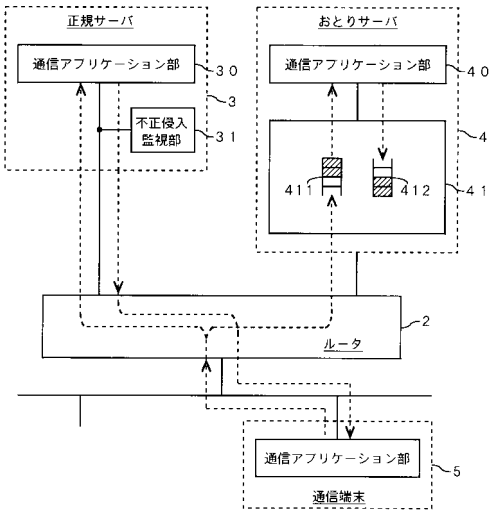
【図１】



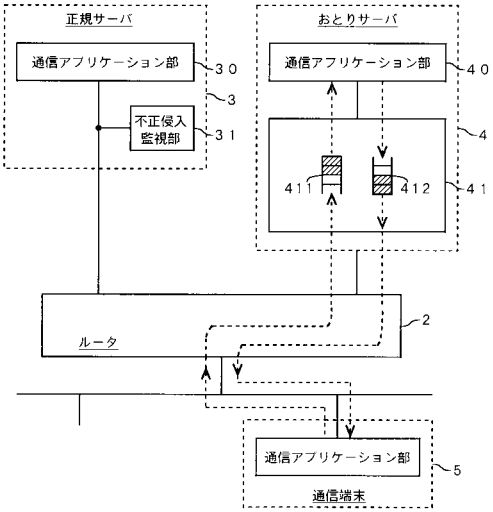
【図２】



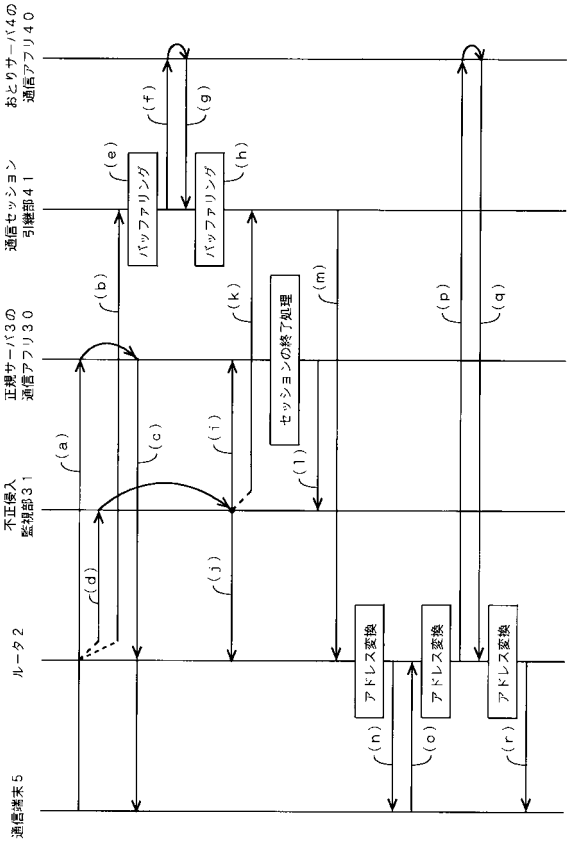
【図３】



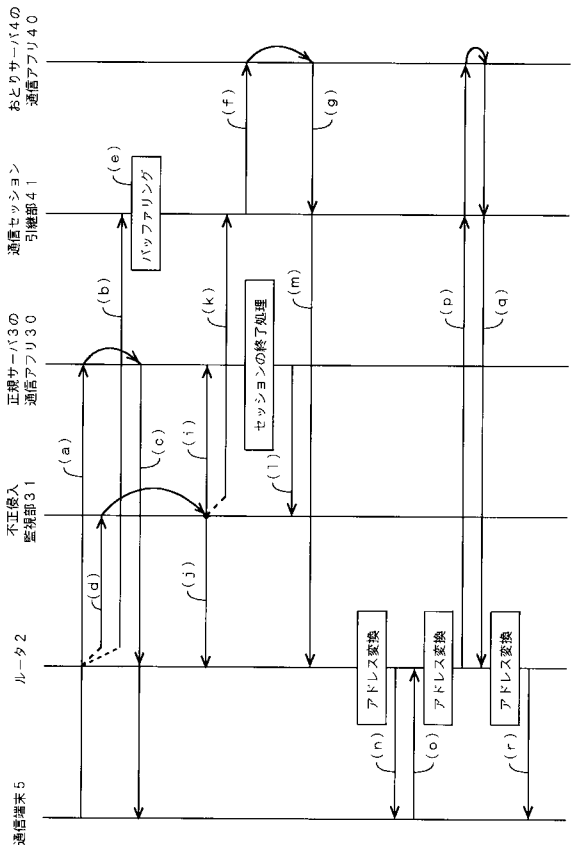
【図４】


正規サーバ
通信アプリケーション部
30
3
不正侵入
監視部
31
おとりサーバ
通信アプリケーション部
40
4
411
412
41
2
ルータ
通信アプリケーション部
5
通信端末

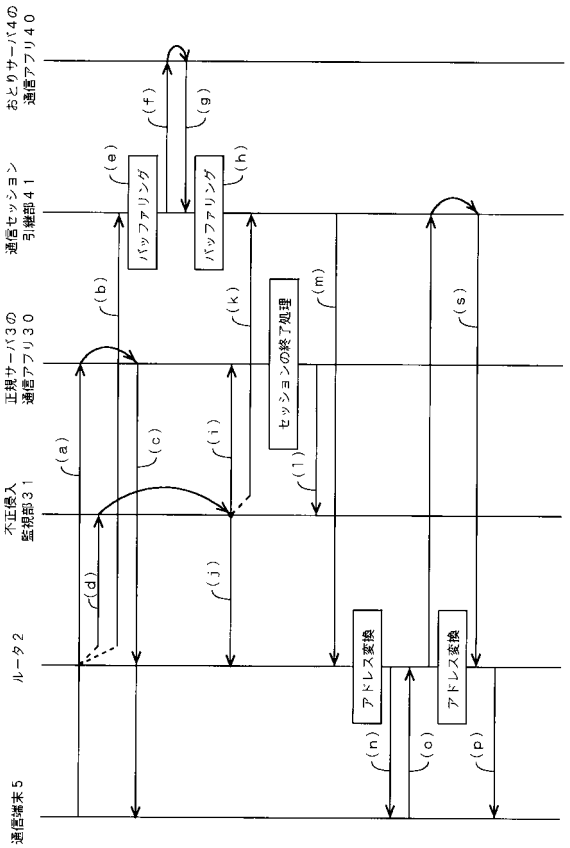
【図５】


おとりサーバ4の通信アプリ40
通信セッション引継部41
正規サーバ3の通信アプリ30
不正侵入監視部31
ルータ2
通信端末5
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)
(k)
(l)
(m)
(n)
(o)
(p)
(q)
(r)
バッファリング
セッションの終了処理
アドレス変換
アドレス変換
アドレス変換

【図６】


おとりサーバ4の通信アプリ40
通信セッション引継部41
正規サーバ3の通信アプリ30
不正侵入監視部31
ルータ2
通信端末5
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(i)
(j)
(k)
(l)
(m)
(n)
(o)
(p)
(q)
(r)
バッファリング
セッションの終了処理
アドレス変換
アドレス変換
アドレス変換

【図７】


おとりサーバ4の通信アプリ40
通信セッション引継部41
正規サーバ3の通信アプリ30
不正侵入監視部31
ルータ2
通信端末5
(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)
(k)
(l)
(m)
(n)
(o)
(p)
(s)
バッファリング
セッションの終了処理
アドレス変換
アドレス変換

フロントページの続き

(51)Int.Cl.[7] F I
H０４L 12/22 H０４L 11/26

(72)発明者 中尾 康二
埼玉県上福岡市大原２－１－１５ 株式会社ケイディディ研究所内

審査官 石井 研一

(56)参考文献 特開２０００－２６１４８３（ＪＰ，Ａ）
特開２００２－０４１４６８（ＪＰ，Ａ）
特開２００２－００７２３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 12/56
G06F 12/00 537
H04L 12/22