(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-20004
(P2007-20004A)
(43)公開日　平成19年1月25日(2007.1.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	B	5J104
H04L 9/32	(2006.01)	H04L	12/56	400Z	5K030
		H04L	9/00	675D	
		H04L	9/00	675A	

審査請求 未請求　請求項の数 13　ＯＬ　（全 17 頁）

(21)出願番号　特願2005-200783 (P2005-200783)
(22)出願日　平成17年7月8日 (2005.7.8)

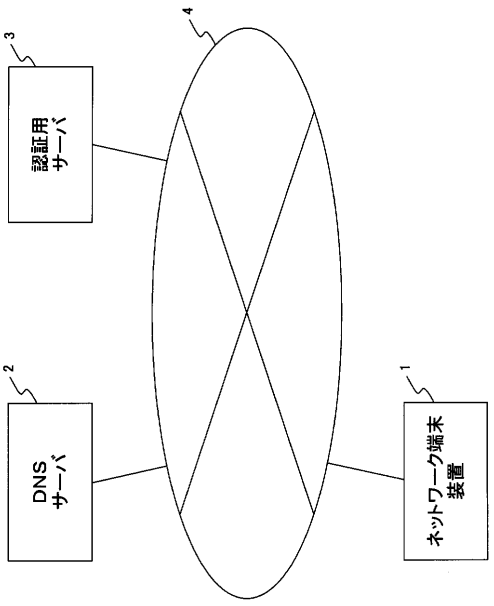
(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(71)出願人　300015528
カシオソフト株式会社
東京都中野区本町３丁目２３番３号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100093632
弁理士　阪本　紀康
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(72)発明者　小笠原　聡
東京都渋谷区本町１－６－２　カシオ計算機株式会社内

最終頁に続く

(54)【発明の名称】ファーミング詐欺防止システム、ネットワーク端末装置及びプログラム

(57)【要約】
【課題】　本発明は、ファーミング詐欺の可能性がある場合にネットワーク端末装置の使用者に警告を発することが出来るファーミング詐欺防止システムを提供することを課題とする。
【解決手段】　使用者がネットワーク端末装置１から、表示するＷｅｂページのドメイン名を入力すると、ネットワーク端末装置１はこのドメイン名の指すＩＰアドレスをＤＮＳサーバ２及び認証用サーバ３に問い合わせる。認証用サーバ３は、ＤＮＳサーバ２と同様、ドメイン名とそのドメイン名が指すＩＰアドレスとの対応関係を示す情報を記憶しており、ネットワーク端末装置１から問い合わせに対して、対応するＩＰアドレスを応答する。ネットワーク端末装置１では、ＤＮＳサーバ２から応答として得たＩＰアドレスと、認証用サーバ３から応答として得たＩＰアドレスを比較し、両者が一致すればファーミングによる不正が行われていないと判断し、一致しなければファーミングによる不正が行われている可能性があると判断して使用者に通知する。
【選択図】　図１

本実施形態のシステムの概略構成を示す図



【特許請求の範囲】
【請求項１】
ネットワーク端末装置がネットワークを介して認証用サーバと接続された構成を有するファーミング詐欺防止システムであって、
前記認証用サーバは、
ドメイン名と対応するＩＰアドレストを対応付けて記憶するＩＰアドレス記憶部と、
前記ネットワーク端末装置からの問い合わせに対して、前記ＩＰアドレス記憶部を参照し、問い合わされたドメイン名に対応するＩＰアドレスを応答として返す応答部と、
を備え、
前記ネットワーク端末装置は、
使用者が入力したドメイン名を用いて、前記ネットワーク上のＤＮＳサーバに対応するＩＰアドレスを問い合わせるＤＮＳ問い合わせ部と、
前記ドメイン名を用いて、前記認証用サーバに対応するＩＰアドレスを問い合わせるアドレス解決部と、
前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスと、前記アドレス解決部が応答として得たＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行う警告部と
を備えることを特徴とするファーミング詐欺防止システム。
【請求項２】
前記Ｐアドレス記憶部に記憶されている情報は、前記ＤＮＳサーバ内の情報とは異なった系統の出所による情報を元にしたものであることを特徴とする請求項１に記載のファーミング詐欺防止システム。
【請求項３】
前記ＩＰアドレス記憶部１つのドメイン名に１乃至複数のＩＰアドレスを対応付けて記憶し、前記応答部は、前記ドメイン名に対応する複数のＩＰアドレスが前記ＩＰアドレス記憶部に記憶されているとき、当該複数のＩＰアドレスを応答として返し、前記警告部は、前記アドレス解決部が応答として得たＩＰアドレスが複数あるとき、当該複数のアドレスと前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスとを比較することを特徴とする請求項１又は２に記載のファーミング詐欺防止システム。
【請求項４】
前記ネットワーク端末装置は、前記認証用サーバからの応答を復号化する暗号解読・認証部を更に備え、
前記応答部は、問い合わされたドメイン名に対応するＩＰアドレスを暗号化した後応答として返すことを特徴とする請求項１乃至３のいずれか１つに記載のファーミング詐欺防止システム。
【請求項５】
前記応答部は、問い合わされたドメイン名に対応するＩＰアドレス及び前記正規認証情報を暗号化した後応答として返し、前記暗号解読・認証部は、前記認証用サーバからの応答を復号化して、送信元の認証用サーバが真正であることを証明する正規認証情報を取り出し、当該正規認証情報に基づいて送信元である前記認証用サーバの認証を行うことを特徴とする請求項４のいずれか１つに記載のファーミング詐欺防止システム。
【請求項６】
ＤＮＳサーバ及び認証用サーバとネットワークを介して接続されるネットワーク端末装置であって、
使用者が入力したドメイン名を用いて、前記ＤＮＳサーバに対応するＩＰアドレスを問い合わせるＤＮＳ問い合わせ部と、
前記ドメイン名を用いて、前記認証用サーバに対応するＩＰアドレスを問い合わせるアドレス解決部と、
前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスと、前記アドレス解決部が応答として得たＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行う警告部と
を備えることを特徴とするネットワーク端末装置。

【請求項７】
前記警告部は、前記アドレス解決部が応答として得たＩＰアドレスが複数あるとき、当該複数のアドレスと前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスとを比較することを特徴とする請求項６に記載のネットワーク端末装置。
【請求項８】
暗号化して送られてきた前記認証用サーバからの応答を復号化する暗号解読・認証部を更に備えることを特徴とする請求項６又は７に記載のネットワーク端末装置。
【請求項９】
前記暗号解読・認証部は、暗号化して送られてきた前記認証用サーバからの応答を復号化して、送信元の認証用サーバが真正であることを証明する正規認証情報を取り出し、当該正規認証情報に基づいて送信元である前記認証用サーバの認証を行うことを特徴とする請求項８に記載のネットワーク端末装置。
【請求項１０】
ＤＮＳサーバとネットワークを介して接続されるネットワーク端末装置であって、
ドメイン名と対応するＩＰアドレスを対応付けたリストを記憶するリスト記憶部と、
使用者が入力したドメイン名を用いて、前記ＤＮＳサーバに対応するＩＰアドレスを問い合わせるＤＮＳ問い合わせ部と、
前記ドメイン名を用いて前記リストを参照し、対応するＩＰアドレスを得るアドレス解決部と、
前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスと、前記アドレス解決部がＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行う警告部と
を備えることを特徴とするネットワーク端末装置。
【請求項１１】
前記ネットワーク端末装置は、前記ネットワークを介して認証用サーバと接続され、前記リスト記憶部内のリストは、前記認証用サーバからの情報に基づいて更新されることを特徴とする請求項１０に記載のネットワーク端末装置。
【請求項１２】
ＤＮＳサーバ及び認証用サーバとネットワークを介して接続されるネットワーク端末装置で実行されるプログラムであって、
使用者が入力したドメイン名を用いて、前記ＤＮＳサーバに対応するＩＰアドレスを問い合わせるステップと、
前記ドメイン名を用いて、前記認証用サーバに対応するＩＰアドレスを問い合わせるステップと、
前記ＤＮＳサーバから応答として得たＩＰアドレスと、前記認証用サーバから応答として得たＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行うステップと、
を前記ネットワーク端末装置に実行させるプログラム。
【請求項１３】
ＤＮＳサーバとネットワークを介して接続されるネットワーク端末装置で実行されるプログラムであって、
使用者が入力したドメイン名を用いて、前記ＤＮＳサーバに対応するＩＰアドレスを問い合わせるステップと
前記ドメイン名を用いて、記憶部に記憶されているドメイン名と対応するＩＰアドレスを対応付けたリストを参照し、対応するＩＰアドレスを得るステップと、
前記ＤＮＳサーバから応答として得たＩＰアドレスと、前記リストを参照して得たＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行うステップと、
を前記ネットワーク端末装置に実行させるプログラム。

【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、ＤＮＳサーバに不当に働きかけるファーミングによる詐欺を防止する技術に関する。
【背景技術】
【０００２】
ＴＣＰ／ＩＰネットワーク環境において、ドメイン名から対応するＩＰアドレスを取得できるようにするアドレス解決の仕組みとして、ＤＮＳ（Domain Name System）が知られている。
【０００３】
ＤＮＳでは、ネットワーク端末装置は、使用者が入力したドメイン名から接続先のＩＰアドレスを求めるため、ネットワーク上に設けてあるＤＮＳサーバにドメイン名によってＩＰアドレスを問い合わせる。
【０００４】
ＤＮＳでは、複数のＤＮＳサーバがツリー構造を持ち、ＩＰアドレスを問い合わされた下位のＤＮＳサーバは、自己が対応する情報を保持している場合はその情報に基づいてＩＰアドレスを応答するが、保持していない場合に、上位のＤＮＳサーバに問い合わせを行い、上位サーバから受け取った情報に基づいてＩＰアドレスを応答する。またこのとき受け取った情報は、キャッシュとして自己に保持し、以降同一のドメイン名に対する問い合わせがあったときにはこのキャッシュの情報を用いる（特許文献１など）。
【特許文献１】特開２００４－２９７４９７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
インターネット等ＴＣＰ／ＩＰを用いてＷｅｂページにアクセスするとき、ＤＮＳサーバの情報を不正に書き換えて、ＤＮＳサーバに問い合わせを行ったネットワーク端末装置を目的とするページ以外の詐欺ページへ誘導し、クレジットカード番号、ＩＤ／Ｐａｓｓｗｏｒｄなどを搾取する詐欺をファーミング詐欺という。
【０００６】
ＤＮＳ情報を不正に書き換えるには２つの方法が考えられる。
１.使用者のネットワーク端末装置内に不正なソフトウエアを埋め込む。
この方法は、ウイルスなどを用い、ネットワーク端末装置内のファイル情報を書き換えることで、正規のサーバへアクセスしようとしたときに、詐欺サーバへのＩＰアドレスを提供して誘導するものである。
２.サーバ名からＩＰアドレスを見つけるアドレス解決の仕組みを悪用する。
【０００７】
この方法は、アドレス解決の仕組み、すなわちＤＮＳサーバ内の情報を不正に書き換えるものである。
この方法では、ＤＮＳの仕組みを悪用し、ＤＮＳサーバのツリー構造の途中に偽のサーバを立てて不正な情報を提供する。ツリー構造の下位にあるＤＮＳサーバは、上位サーバの偽サーバから一度不正な情報を受け取ると、その情報をキャッシュするため、しばらくの間、不正な情報があたかも正規な情報として流通してしまう。
【０００８】
上記した２つの方法のうち１番目の方法は、ネットワーク端末装置内のファイルを書き換える、若しくはウイルスを埋め込む等、使用者のネットワーク端末装置に何らかの痕跡を残す。従ってネットワーク端末装置にウイルス除去ソフトや監視ソフトなどを導入することによって防ぐことが出来る。
【０００９】
しかし２番目のＤＮＳサーバにキャッシュされている情報を不正な情報に書き換えてしまう方法の場合、使用者のネットワーク端末装置側には何ら痕跡は残らないので、不正が行われているかどうかの判断を行う手立てがなかった。

【００１０】
上記問題点を鑑み、本発明は、ファーミング詐欺の可能性がある場合にネットワーク端末装置の使用者に警告を発することによる詐欺に遭うのを未然に防ぐことが出来るファーミング詐欺防止システムを提供することを課題とする。
【課題を解決するための手段】
【００１１】
本発明によるファーミング詐欺防止システムは、ネットワーク端末装置がネットワークを介して認証用サーバと接続された構成を有することを前提とし、上記問題点を解決するため、前記認証用サーバは、ＩＰアドレス記憶部及び応答部を備え、前記ネットワーク端末装置は、ＤＮＳ問い合わせ部、アドレス解決部及び警告部を備える。
【００１２】
ＩＰアドレス記憶部は、ドメイン名と対応するＩＰアドレストを対応付けて記憶する。
応答部は、前記ネットワーク端末装置からの問い合わせに対して、前記ＩＰアドレス記憶部を参照し、問い合わされたドメイン名に対応するＩＰアドレスを応答として返す。
【００１３】
ＤＮＳ問い合わせ部は、使用者が入力したドメイン名を用いて、前記ネットワーク上のＤＮＳサーバに対応するＩＰアドレスを問い合わせる。
アドレス解決部は、前記ドメイン名を用いて、前記認証用サーバに対応するＩＰアドレスを問い合わせる。
【００１４】
警告部は、前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスと、前記アドレス解決部が応答として得たＩＰアドレスを比較し、両者が一致しないとき使用者に警告を行う。
【００１５】
この構成により、ＤＮＳサーバから得たＩＰアドレスと、認証用サーバから得たアドレスを比較することによって、ファーミングの可能性を検出し、使用者に通知することが出来る。
【００１６】
また前記Ｐアドレス記憶部に記憶されている情報は、例えば前記ＤＮＳサーバ内の情報とは異なった系統の出所による情報を元にしたものである。
これにより、ＤＮＳがファーミングされても、認証用サーバのＤＮＳとは異なる系統の情報からファーミング詐欺を検出することが出来る。
【００１７】
また前記ＩＰアドレス記憶部１つのドメイン名に１乃至複数のＩＰアドレスを対応付けて記憶し、前記応答部は、前記ドメイン名に対応する複数のＩＰアドレスが前記ＩＰアドレス記憶部に記憶されているとき、当該複数のＩＰアドレスを応答として返し、前記警告部は、前記アドレス解決部が応答として得たＩＰアドレスが複数あるとき、当該複数のアドレスと前記ＤＮＳ問い合わせ部が応答として得たＩＰアドレスとを比較する構成とすることも出来る。
【００１８】
これによって、サーバの引越し等によってＤＮＳに複数のＩＰアドレスが存在する場合においても対処することが出来る。
更に前記ネットワーク端末装置は、前記認証用サーバからの応答を復号化する暗号解読・認証部を更に備え、前記応答部は、問い合わされたドメイン名に対応するＩＰアドレスを暗号化した後応答として返す。
【００１９】
これによって、ネットワーク端末装置と認証用サーバとの間の通信は暗号化され、第３者が内容を両者のやり取りを知ることが出来ない。
また前記応答部は、問い合わされたドメイン名に対応するＩＰアドレス及び前記正規認証情報を暗号化した後応答として返し、前記暗号解読・認証部は、前記認証用サーバから

の応答を復号化して、送信元の認証用サーバが真正であることを証明する正規認証情報を取り出し、当該正規認証情報に基づいて送信元である前記認証用サーバの認証を行う。

【００２０】

これにより、ネットワーク端末装置はデータの送信元の認証用サーバに対する認証を行うことが出来る。

また本発明は、ネットワーク端末装置やネットワーク端末装置内で実行されるプログラムもその範囲に含む。

【発明の効果】

【００２１】

本発明によれば、ＤＮＳに対してファーミングが行われても、不正なＷｅｂページへのＩＰアドレスであることを検出し、使用者にファーミングの可能性があることを通知することが出来る。

【００２２】

また、サーバの引越し等によって複数のＩＰアドレスがＤＮＳに存在している場合においても、対処することが出来る。

更に、ネットワーク端末装置と認証用サーバ間の通信を暗号化したり、認証用サーバに対する認証を行っている。よって認証用サーバに対するファーミングに対しても、対処することが出来る。

【発明を実施するための最良の形態】

【００２３】

以下に図面を参照しながら、本発明の一実施形態について説明する。

図１は、本実施形態のシステムの概略構成を示す図である。

同図において、本実施形態のシステムは使用者が用いるネットワーク端末装置１、ＤＮＳサーバ２及び認証用サーバ３及びこれらを接続するインターネット等のＴＣＰ／ＩＰを用いたインターネット等のネットワーク４を有している。

【００２４】

ネットワーク端末装置１は、ネットワーク４上に多数存在するネットワーク端末で、ＤＮＳを用いてネットワーク４上のサーバに接続してＷｅｂページを表示する。ＤＮＳサーバ２は、ネットワーク端末装置１からの問い合わせに対してＩＰアドレスを返す、ＤＮＳを実現するためのサーバで、ネットワーク４上に複数存在する。認証用サーバ３は、後述するネットワーク端末装置１がＤＮＳサーバ２から得たＩＰアドレスの認証処理を行うために用いられるもので、ＤＮＳサーバ２とは別の系統から得たドメイン名とそのドメイン名に対応するＩＰアドレスの対応関係を情報として保持している。尚ＤＮＳサーバが記録しているドメイン名は、本システムを運営する組織と事前に契約を結んだ会社等のサーバのドメイン名であり、認証用サーバ３にはこれらのドメイン名と対応するＩＰアドレスの関係が、ＤＮＳとは別系統の出所による情報を元に登録されている。

【００２５】

以下に、本実施形態におけるシステムの動作概略を説明する。

ネットワーク端末装置１上から使用者がドメイン名によって、ネットワーク端末装置１に表示させたいＷｅｂページを指定すると、ネットワーク端末装置１はこのドメイン名の指すＩＰアドレスをＤＮＳサーバ２に問い合わせる。また同様にネットワーク端末装置１はドメイン名の指すＩＰアドレスを認証用サーバ３にも問い合わせる。

【００２６】

認証用サーバ３は、ＤＮＳサーバ２と同様、ドメイン名とそのドメイン名が指すＩＰアドレスとの対応関係を示す情報を記憶しており、ネットワーク端末装置１から問い合わせがあると、対応するＩＰアドレスをネットワーク端末装置１に応答する。

【００２７】

ネットワーク端末装置１では、ＤＮＳサーバ２から応答として得たＩＰアドレスと、認証用サーバ３から応答として得たＩＰアドレスを比較し、両者が一致すればファーミングによる不正が行われていないと判断し、また両者が一致しなければファーミングによる不

正が行われている可能性があると判断して使用者に通知する。

【００２８】

これによって、不正ページからパスワード等を入力する前に、使用者に詐欺のＷｅｂページへ接続されていることを通知することが出来、使用者が詐欺の被害に遭うのを未然に防ぐことが出来る。

【００２９】

図２は、ネットワーク端末装置１の構成を示す図である。

本実施形態のネットワーク端末装置１は、ＣＰＵ１１、主記憶装置１２、ハードディスク等の補助記憶装置１３、入力部１１及び出力部１１に該当するディスプレイ、キーボード等の入出力装置（Ｉ／Ｏ）１４、モデム等のネットワーク接続装置１５及びディスク、磁気テープなどの可搬記憶媒体から記憶内容を読み出す媒体読み取り装置１６を有し、これらが互いにバス１８により接続される構成を備えている。

【００３０】

図２のネットワーク端末装置１では、ネットワーク接続装置１５によってネットワーク４からプログラムやデータをダウンロードしたり、媒体読み取り装置１６により磁気テープ、フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ、ＭＯ等の可搬記憶媒体１７に記憶されているプログラム、データを読み出し、これを主記憶装置１２または補助記憶装置１３にダウンロードする。そしてこのプログラムやデータをＣＰＵ１１が実行したり用いたりすることにより、後述するフローチャート等で示す各処理をネットワーク端末装置１内でソフトウエア的に実現する。

【００３１】

次に本システムにおける第１の実施形態について説明する。

図３は、第１の実施形態におけるネットワーク端末装置１及び認証用サーバ３のソフトウエア的構成を示す図である。

【００３２】

同図において、ネットワーク端末装置１は、Ｗｅｂページ表示部２１、アドレス解決部２２、第１のＩＰアドレス記憶部２３、第２のＩＰアドレス記憶部２４、ＩＰアドレス比較部２５及び警告表示部２６を有している。

【００３３】

Ｗｅｂページ表示部２１は、いわゆるＷｅｂブラウザに対応するもので、使用者が入力したドメイン名からＤＮＳサーバ２に問い合わせを行い、応答として得られたＩＰアドレスのサーバに接続してデータを読み出し表示を行うものである。尚このときＤＮＳサーバ２から得られるＩＰアドレスは、第１のＩＰアドレス記憶部２３に記憶される。アドレス解決部２２は、使用者が入力したドメイン名から認証用サーバ３に問い合わせを行い、応答結果として得られるＩＰアドレスを第２のＩＰアドレス記憶部２４に記憶するものである。第１のＩＰアドレス記憶部２３はＤＮＳサーバから応答として得たＩＰアドレスを記憶するものである。第２のＩＰアドレス記憶部２４は認証用サーバ３から応答として得たＩＰアドレスを記憶するものである。ＩＰアドレス比較部２５は第１のＩＰアドレス記憶部２４内のＩＰアドレスと第２のＩＰアドレス記憶部２５内のＩＰアドレスを比較し、両者が一致するがどうかのチェックを行うものである。警告表示部２６は、ＩＰアドレス比較部２５による比較の結果、２つのＩＰアドレスが一致しなかったとき、画面表示等によって使用者に不正ページに接続されている可能性があることを通知するものである。

【００３４】

このＷｅｂページ表示部２１、アドレス解決部２２、ＩＰアドレス比較部２５及び警告表示部２６は、ＣＰＵ１１が主記憶装置１２や補助記憶装置１３上のプログラムを実行することによって実現され、また第１のＩＰアドレス記憶部２３及び第２のＩＰアドレス記憶部２４は、主記憶装置１２若しくは補助記憶装置１３上の記憶領域として実現される。

【００３５】

この構成要素２０ａ部分は、ブラウザの構成要素として実現しても、或いはブラウザ用のｐｌｕｇ－ｉｎとして構成してブラウザにインストールする構成としても良い。

また認証用サーバ３は、登録されているドメイン名２７とＩＰアドレス２８を対応付けて記憶部に記憶しており、情報端末１から問い合わせがあると、問い合わせがあったドメイン名と自己が記憶するドメイン名２７を参照して、一致するドメイン名２７に対応するＩＰアドレス２８を応答として返す。

【００３６】

このような構成において、以下に第１の実施形態における動作を説明する。

使用者が、Ｗｅｂページ表示部２１からドメイン名を入力して接続先を指定すると、Ｗｅｂページ表示部２１は、そのドメイン名によってネットワーク４上のＤＮＳサーバ２の１つにＩＰアドレスの問い合わせを行い、応答として得たＩＰアドレスを第１のＩＰアドレス記憶部２３に記憶する。またＷｅｂページ表示部２１は、得られたＩＰアドレスにネットワーク接続して、サーバからデータを読み込みＷｅｂページの表示処理を行う。

【００３７】

上記Ｗｅｂ表示部２１の処理と並列してアドレス解決部２２は、使用者が入力したドメイン名から認証用サーバ３に問い合わせを行い、応答結果として得られるＩＰアドレスを第２のＩＰアドレス記憶部２４に記憶する。

【００３８】

２つのＩＰアドレスが第１のアドレス記憶部２３及び第２のアドレス記憶部２４に記憶されると、ＩＰアドレス比較部２５はこれらを比較する。そして、両者が一致すればこのＩＰアドレスは正規のサーバへのものと判断し、また両者が一致しなかった場合、Ｗｅｂページ表示部２１によるＷｅｂページの表示に対して、この表次ページがファーミングされている可能性があることを画面に強調表示、例えばＷｅｂページのロゴに切り換えて所定の警告メッセージを表示して、使用者に警告する。なお警告は表示だけによらず音声と共に行ってもよく、また音声だけでも良い（以下の警告も同様）。

【００３９】

このように、第１の実施形態では、ＤＮＳサーバ内の情報を書き換えてファーミングを行っても、ネットワーク端末装置は認証用サーバによる問い合わせによって、ファーミングを検出して使用者に警告を発することが出来るので、ファーミング詐欺の被害に遭うのを未然に防ぐことが出来る。

【００４０】

次に第２の実施形態について説明する。

第２の実施形態では、認証用サーバ３において、一つのドメイン名に複数のＩＰアドレスを関連付けて記憶し、ネットワーク端末装置１からの問い合わせに対して対応する複数のＩＰアドレスを応答する。ネットワーク端末装置１側ではこれら複数のＩＰアドレスとＤＮＳサーバ２からのＩＰアドレスとを比較する。

【００４１】

これにより、サーバの移動などでＤＮＳに旧サーバのＩＰアドレスと新サーバのＩＰアドレスが存在する場合、両方のＩＰアドレスを認証用サーバ３に登録することによって、正しいサーバの判断が可能となる。

【００４２】

図４は、第２の実施形態におけるネットワーク端末装置１及び認証用サーバ３のソフトウエア的構成を示す図である。

尚図４は、図３に示す第１の実施形態の構成と同一構成要素については、同一の符号が付せられている。

【００４３】

図４の構成を図３の第１の実施形態の構成と比較すると、図４の第２の実施形態では、ネットワーク端末装置１側では認証用サーバ３から受け取った複数のＩＰアドレスを記憶出来るよう複数の第２のＩＰアドレス記憶部２４－１，２４－２，・・・を備え、また認証用サーバ３側では、１つのドメイン名２７に複数のＩＰアドレス２８－１，２８－２，・・・が対応付けられて登録されている点が第１の実施形態とは異なる。

【００４４】

尚図４の構成においても、構成要素２０ｂ部分はブラウザの一構成要素として構成しても、ｐｌｕｇ－ｉｎとして構成しても良い。

図５は、第２の実施形態におけるネットワーク端末装置１の動作処理を示すフローチャートである。同図の処理は、ＣＰＵ１１が、メモリ上のプログラムを実行することにより実現される。

【００４５】

尚図５のフローチャートにおいてステップＳ４のｎの値が１のとき、図５のフローチャートは、第１の実施形態時のネットワーク端末装置１の動作処理を表すフローチャートとなる。

【００４６】

ネットワーク端末装置１の使用者が表示させるＷｅｂページのドメイン名を入力し、図５の処理が開始されると、まずステップＳ１としてＷｅｂページ表示部２１がネットワーク４上のＤＮＳサーバ２に問い合わせを行い、入力されたドメイン名に対応するＩＰアドレスを応答として受け取る。そしてＷｅｂページ表示部２１は、ステップＳ２としてステップＳ１でＤＮＳサーバ２から応答として得たＩＰアドレスを第１のＩＰアドレス記憶部２３に記憶する。

【００４７】

次に若しくはステップＳ１、Ｓ２の処理と平行して、ステップＳ３としてアドレス解決部２２は、ネットワーク４上の認証用サーバ３に使用者が入力したドメイン名を用いて問い合わせを行う。

【００４８】

これに対して認証用サーバ３では、問い合わされたドメイン名を自己が記憶しているドメイン名２７と照らし合わせ、一致するドメイン名２７に対応する一乃至複数のＩＰアドレス２８を応答として返す。

【００４９】

このＩＰアドレスを応答として受け取ると、ネットワーク端末装置１では、ステップＳ４として受け取ったＩＰアドレスの数を変数ｎに代入する。

次に変数ｉを１に初期化し（ステップＳ５）、認証用サーバから受け取ったｉ番目のＩＰアドレスｉの値を第２のＩＰアドレス記憶部２４－ｉに格納する。

【００５０】

そしてステップＳ７として、変数ｉの値が変数ｎの値に達したかどうかを判断し、達していなければ（ステップＳ７、ＮＯ）、ステップＳ８として変数ｉの値を＋１インクリメント後、処理をステップＳ６に戻す。

【００５１】

またステップＳ７において、変数ｉの値が変数ｎの値に達して認証用サーバから受け取った全てのＩＰアドレスが第２のＩＰアドレス記憶部２４－ｉに格納されたならば（ステップＳ７、ＹＥＳ）、ステップＳ９に処理を移す。

【００５２】

ステップＳ９で、変数ｉを１に初期化後、ステップＳ１０として第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４－ｉに記憶されているＩＰアドレスとを比較する。その結果両者の値が一致すれば（ステップＳ１０、ＹＥＳ）、ステップＳ１でＤＮＳサーバから受け取ったＩＰアドレスは、正規のサーバへのアドレスと判断し、本処理を終了する。

【００５３】

またステップＳ１０における第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４－ｉに記憶されているＩＰアドレスとの比較の結果、両者が一致しなかったとき（ステップＳ１０、ＮＯ）、次にステップＳ１１として変数ｉの値が変数ｎの値に達したかどうかを判断し、達していなければ（ステップＳ１１、ＮＯ）、ステップＳ１２として変数ｉの値を＋１インクリメント後、処理をステップＳ１０に戻す。

【００５４】
またステップＳ１１において、変数ｉの値が変数ｎの値に達して、第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスが第２のＩＰアドレス記憶部２４に記憶されている全てのＩＰアドレスと比較されたならば（ステップＳ１１、ＹＥＳ）、第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスは第２のＩＰアドレス記憶部２４に記憶されている全てのＩＰアドレスの値と一致しなかったので、ステップＳ１３として使用者にＷｅｂページ表示部２１によって表示されたＷｅｂページは、ファーミングされたＷｅｂページである可能性があることを使用者に警告表示した後、本処理を終了する。
【００５５】
このように第２の実施形態では、１つのドメイン名を複数のＩＰアドレスと対応させて認証用サーバ３に登録でき、またネットワーク端末装置１ではＤＮＳサーバから得たＩＰアドレス値を認証用サーバから得た複数のＩＰアドレス値と比較することによって、サーバの引越しなどでＤＮＳ上のＩＰアドレスが旧サーバと新サーバ等複数混在している場合にも対処することが出来る。
【００５６】
次に第３の実施形態について説明する。
第３の実施形態は、認証用サーバ３からネットワーク端末装置１への応答に正規認証情報を付加し、また応答として送る情報を暗号化して送信する。そしてネットワーク端末装置１側では、暗号を復号化して、中に含まれる正規認証情報を確認することによって認証用サーバ３からの正規の情報であることを認識する。
【００５７】
この構成により、認証用サーバ３へのＩＰアドレスのファーミングによる書き換えに対しても対応することが出来る。
図６は、第３の実施形態におけるネットワーク端末装置１及び認証用サーバ３のソフトウエア的構成を示す図である。
【００５８】
尚図６は、図３、図４に示す第１及び第２の実施形態の構成と同一構成要素については、同一の符号が付せられている。
図６の第３の実施形態と図３の第１の実施形態の構成を比較すると、第３の実施形態では、第１の実施形態の構成に加え、ネットワーク端末装置１側には、暗号解読・認証部３１を、また認証用サーバ３側には、暗号部３２及び正規認証情報３３を備えている。
【００５９】
暗号解読・認証部３１は、認証用サーバ３から受信した暗号化情報を復号化し、正規認証情報３３を用いて認証用サーバ３の認証を行う。暗号部３２は、ネットワーク端末装置１に対して応答として返信するＩＰアドレス２８と正規認証情報３３を暗号化してネットワーク端末装置１に返信する。正規認証情報３３は、デジタル証明書等の、送信元の認証用サーバ３が真正であることを証明するデータである。
【００６０】
尚図６の構成においてもまた、構成要素２０ｃ部分はブラウザの一構成要素として構成しても、ｐｌｕｇ－ｉｎとして構成しても良い。
図７は、第３の実施形態におけるネットワーク端末装置１の動作処理を示すフローチャートである。同図の動作処理もＣＰＵ１１がメモリ上のプログラムを実行することによって実現される。
【００６１】
ネットワーク端末装置１の使用者が表示させるＷｅｂページのドメイン名を入力し、図７の処理が開始されると、まずステップＳ２１としてＷｅｂページ表示部２１がネットワーク４上のＤＮＳサーバ２に問い合わせを行い、入力されたドメイン名に対応するＩＰアドレスを応答として受け取る。そしてＷｅｂページ表示部２１は、ステップＳ２２としてステップＳ２１でＤＮＳサーバ２から応答として得たＩＰアドレスを第１のＩＰアドレス記憶部２３に記憶する。

【００６２】
次に若しくはステップＳ２１、Ｓ２２の処理と平行して、ステップＳ２３としてアドレス解決部２２は、ネットワーク４上の認証用サーバ３に使用者が入力したドメイン名を用いて問い合わせを行う。
【００６３】
これに対して認証用サーバ３では、問い合わされたドメイン名を自己が記憶しているドメイン名２７と照らし合わせ、一致するドメイン名に対応するＩＰアドレス２７を求め、このＩＰアドレスと自己が真正であることを証明する正規認証情報３３を暗号化部によって暗号化後、この暗号化情報を応答としてネットワーク端末装置１に返す。
【００６４】
この暗号化情報を受け取ったネットワーク端末装置１は、ステップＳ２４としてこれを暗号解読・認証部３１によって復号化する。
そしてステップＳ２５として、暗号解読・認証部３１は、復号化した情報内の正規認証情報３３が正規のものかどうかを判定し、正規のものでなければ（ステップＳ２５、ＮＯ）、ファーミングされている可能性があることを使用者に通知して（ステップＳ２８）、本処理を終了する。
【００６５】
ステップＳ２５において、正規認証情報３３が正規のものであれば（ステップＳ２５、ＹＥＳ）、受信した暗号化情報の送り先の認証用サーバ３が認証されたものとして、ステップＳ２６として、復号化したＩＰアドレスを第２のＩＰアドレス記憶部２４に記憶する。
【００６６】
そしてステップＳ２７において、ＩＰアドレス比較部２５が第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４に記憶されているＩＰアドレスとを比較し、両者が一致すれば（ステップＳ２７、ＹＥＳ）、ステップＳ２１でＤＮＳサーバから受け取ったＩＰアドレスは、正規のサーバへのアドレスと判断し、本処理を終了する。
【００６７】
またステップＳ２７における第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４に記憶されているＩＰアドレスとの比較の結果、両者が一致しなかったとき（ステップＳ２７、ＮＯ）、ステップＳ２８として警告表示部２６が、使用者にＷｅｂページ表示部２１によって表示されたＷｅｂページは、ファーミングされたＷｅｂページである可能性があることを使用者に警告表示後、本処理を終了する。
【００６８】
このように第３の実施形態では、認証用サーバ３からネットワーク端末装置１への通信内容が暗号化されて送られる。従って、悪意のある第３者は、Ｗｅｂ端末と認証用サーバとのやり取りを盗聴しても内容が不明なので、偽の認証用サーバを立てることは出来ず、認証用サーバへのＩＰアドレスを書き換えるファーミング詐欺を行うことが出来ない。
【００６９】
次に第４の実施形態について説明する。
第４の実施形態では、ネットワーク端末装置１が事前にドメイン名とＩＰアドレスの対応関係を示したリストを保持しており、ネットワーク接続を行うときは、ＤＮＳサーバから得たＩＰアドレスと、このリストを参照して得たＩＰアドレスを比較することによってファーミング詐欺に対処する。
【００７０】
これによって、第１乃至第３の実施形態のようにＤＮＳサーバ２に問い合わせる必要が無くなる。尚ネットワーク端末装置１が保持するリストは、定期的に或いは不定期に認証用サーバ３に接続して情報を得ることによって更新される。
【００７１】

図８は、第４の実施形態におけるネットワーク端末装置１及び認証用サーバ３のソフトウエア的構成を示す図である。

尚図８もまた、第１乃至第３の実施形態の構成と同一構成要素については、同一の符号が付せられている。

【００７２】

同図の構成を図３の第１の実施形態の構成を比較すると、図８の第４の実施形態では、第１の実施形態の構成に加え、ネットワーク端末装置１側ではリストを記憶するリスト記憶部４１を備え、また認証用サーバ３側では複数のドメイン名とＩＰアドレスの関係を示すリスト４２を保持している。

【００７３】

尚リスト記憶部４１に記憶されるリストは、ネットワーク端末装置１に本実施形態の機能を有するブラウザがインストールされたとき、或いは２０ｄ部分がブラウザにｐｌｕｇ－ｉｎとしてインストールされたときに生成され、リスト記憶部４１に記憶される。

【００７４】

そしてこのリスト記憶部４１内のリストは、定期的に或いは使用者の指示によって不定期に認証用サーバ３から受け取ったリスト４２に基づいて更新される。

図９は、第４の実施形態におけるＷｅｂページを表示する際に行われるネットワーク端末装置１の動作処理を示すフローチャートである。尚リスト記憶部４１内のリストの更新処理については、フローチャートによる詳細説明は省略する。

【００７５】

ネットワーク端末装置１の使用者がＷｅｂページ表示部２１によって表示させるＷｅｂページのドメイン名を入力し、図９の処理が開始されると、まずステップＳ３１としてＷｅｂページ表示部２１がネットワーク４上のＤＮＳサーバ２に問い合わせを行い、入力されたドメイン名に対応するＩＰアドレスを応答として受け取る。そしてＷｅｂページ表示部２１は、ステップＳ３２としてステップＳ３１でＤＮＳサーバ２から応答として得たＩＰアドレスを第１のＩＰアドレス記憶部２３に記憶する。

【００７６】

次に若しくはステップＳ３１、Ｓ３２の処理と平行して、ステップＳ３３としてアドレス解決部２２は、ネットワーク４上の認証用サーバ３に使用者が入力したドメイン名によってリスト記憶部４１が記録しているリストを参照し、ドメイン名に対応するＩＰアドレスを求め、ステップＳ３４としてこのＩＰアドレスを第２のＩＰアドレス記憶部２４に記憶する。

【００７７】

そしてステップＳ３５において、第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４に記憶されているＩＰアドレスとを比較し、両者が一致すれば（ステップＳ３５、ＹＥＳ）、ステップＳ３１でＤＮＳサーバから受け取ったＩＰアドレスは、正規のサーバへのアドレスと判断し、本処理を終了する。

【００７８】

またステップＳ３５において、第１のＩＰアドレス記憶部２３に記憶されているＩＰアドレスと第２のＩＰアドレス記憶部２４に記憶されているＩＰアドレスとが一致しなかったとき（ステップＳ３５、ＮＯ）、ステップＳ３６として使用者にＷｅｂページ表示部２１によって表示されたＷｅｂページは、ファーミングされたＷｅｂページである可能性があることを使用者に警告表示後、本処理を終了する。

【００７９】

このように第４の実施形態では、事前にＤＮＳとは別系統で得たドメイン名と対応するＩＰアドレスを示すリストをネットワーク端末装置１が保持しているので、ＤＮＳサーバ２に問い合わせを行う度に、認証用サーバ４に接続する必要が無い。よってその分、応答速度が速くなり、また認証用サーバ３をファーミングされたときに生じる危険度を軽減することが出来る。

【００８０】

尚第１乃至第３の実施形態では、認証用サーバ３はネットワーク端末装置１からの問い合わせに対してＩＰアドレスを返し、ネットワーク端末装置１によってＤＮＳサーバ２からのＩＰアドレスと比較を行う構成としたが、ネットワーク端末装置１がＤＮＳサーバから受け取ったＩＰアドレスも認証用サーバ３に渡して２つのＩＰアドレスの比較を認証用サーバ３で行い、結果をネットワーク端末装置１に応答する構成としてもよい。

【００８１】

また上記説明では、第３の実施形態のみネットワーク端末装置１が暗号解読・認証部３を、また認証用サーバ３には暗号部３２を備え、正規認証３３を保持しているが、これらの構成要素は、第１、第２及び第４の実施形態の構成においても備え、ネットワーク端末装置１と認証用サーバ３との間の通信を暗号化通信を行い、またネットワーク端末装置１において認証用サーバ３の認証を行うように構成しても良い。

【図面の簡単な説明】

【００８２】

【図１】本実施形態のシステムの概略構成を示す図である。

【図２】ネットワーク端末装置の構成を示す図である。

【図３】第１の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図である。

【図４】第２の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図である。

【図５】第２の実施形態におけるネットワーク端末装置の動作処理を示すフローチャートである。

【図６】第３の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図である。

【図７】第３の実施形態におけるネットワーク端末装置の動作処理を示すフローチャートである。

【図８】第４の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図である。

【図９】第４の実施形態におけるＷｅｂページを表示する際に行われるネットワーク端末装置の動作処理を示すフローチャートである。

【符号の説明】

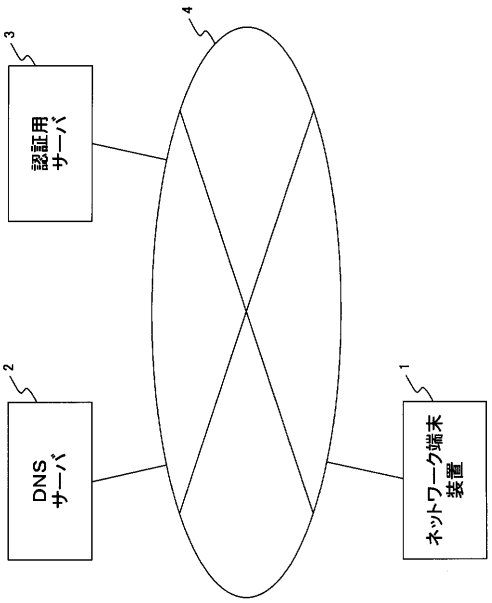
【００８３】

１	ネットワーク端末装置
２	ＤＮＳサーバ
３	認証用サーバ
４	ネットワーク
１１	ＣＰＵ
１２	主記憶装置
１３	補助記憶装置
１４	入出力装置
１５	ネットワーク接続装置
１６	媒体読み取り装置
１７	可搬記憶媒体
１８	バス
２１	Ｗｅｂページ表示部
２２	アドレス解決部
２３	第１のＩＰアドレス記憶部
２４	第２のＩＰアドレス記憶部
２５	ＩＰアドレス比較部
２６	警告表示部
２７	ドメイン名

２８　　ＩＰアドレス
３１　　暗号解読・認証部
３２　　暗号部
３３　　正規認証情報
４１　　リスト記憶部
４２　　リスト

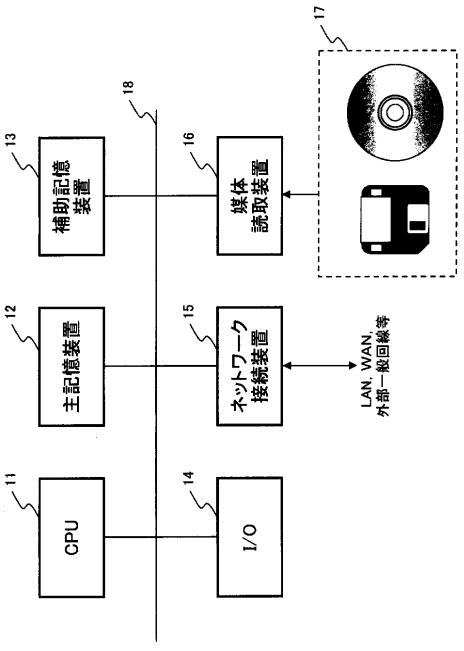
【図１】

本実施形態のシステムの概略構成を示す図



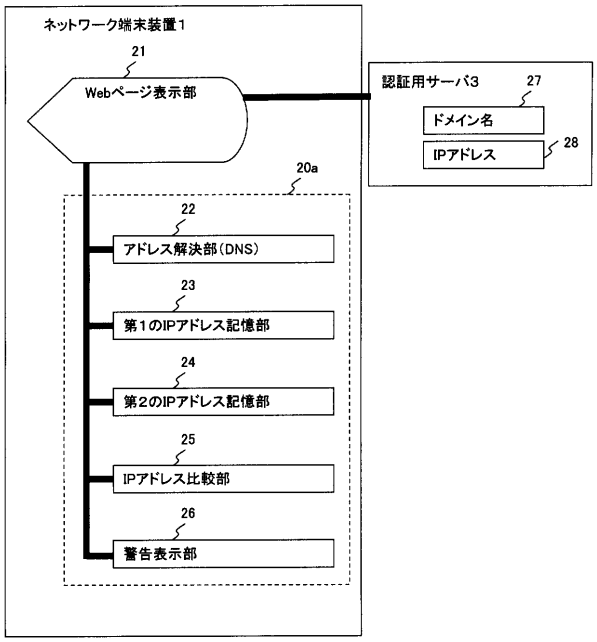
【図２】

ネットワーク端末装置の構成を示す図



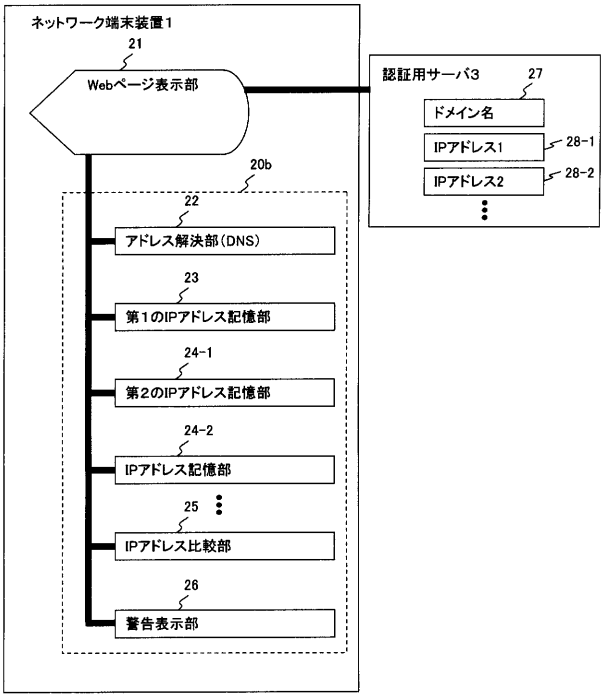
【図３】

第１の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図



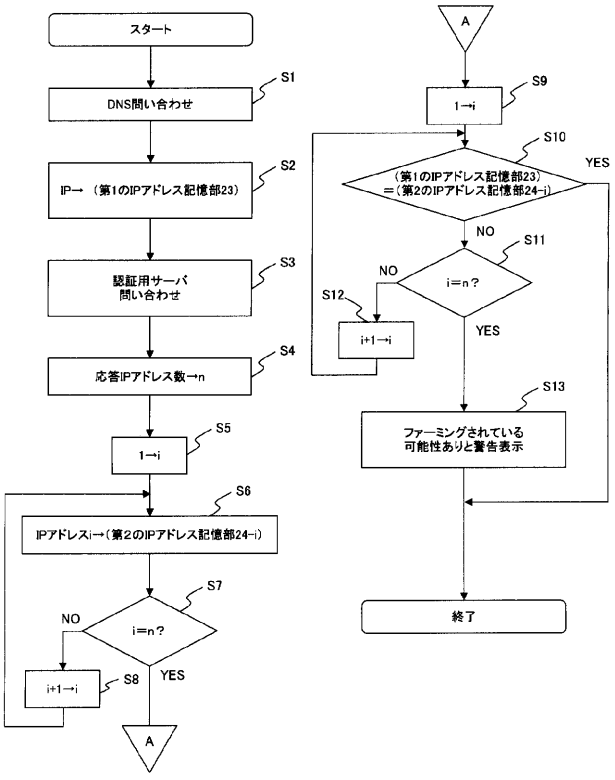
【図４】

第２の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図



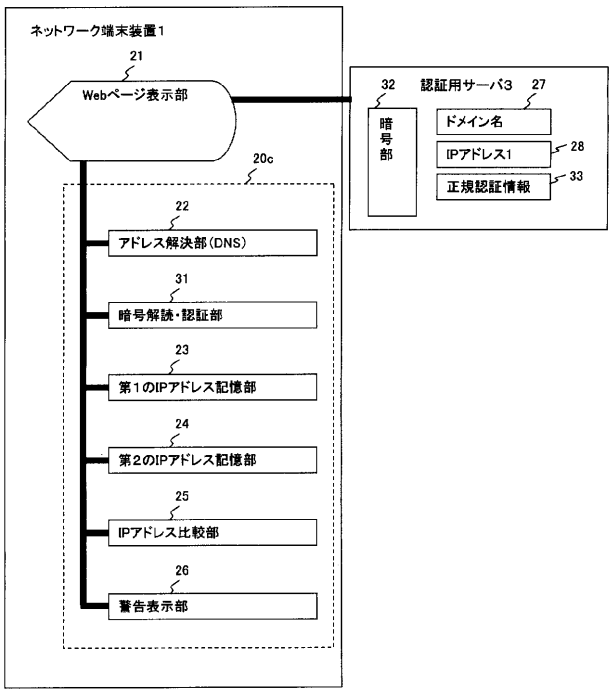
【図５】

第２の実施形態におけるネットワーク端末装置の動作処理を示すフローチャート



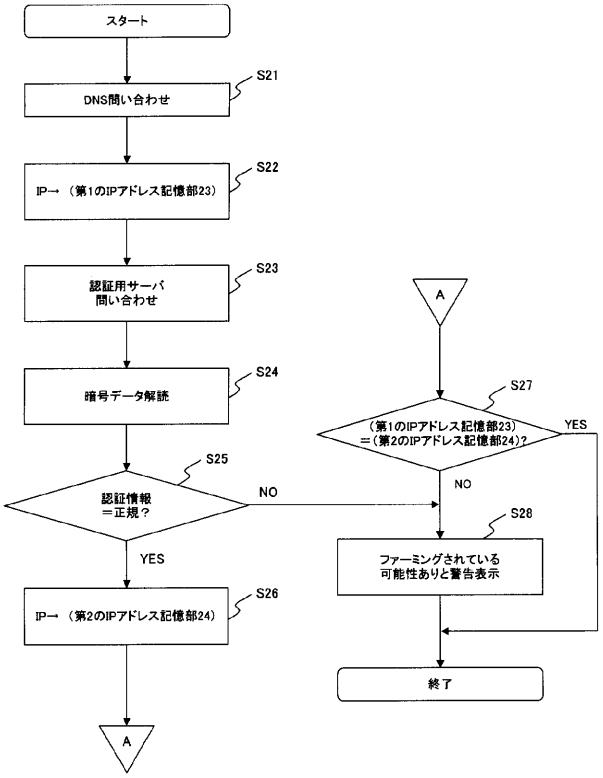
【図６】

第３の実施形態におけるネットワーク端末装置及び認証用サーバのソフトウエア的構成を示す図



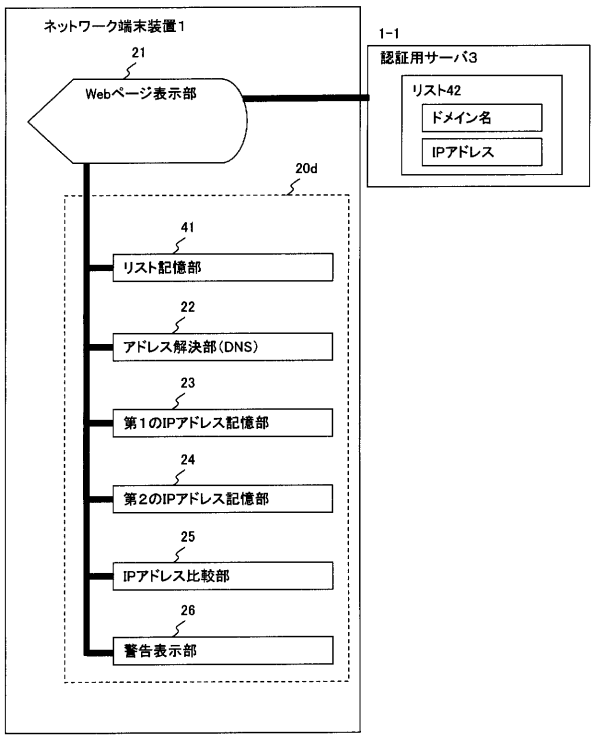
【図７】

第3の実施形態におけるネットワーク端末装置の動作処理を示すフローチャート



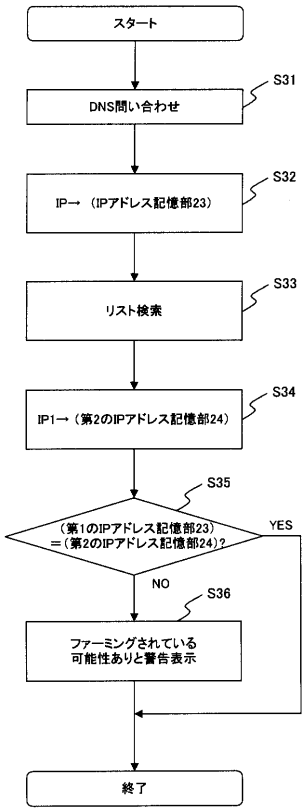
【図８】

第4の実施形態におけるネットワーク端末装置及び
認証用サーバのソフトウエア的構成を示す図



【図９】

第4の実施形態におけるWebページを表示する際に行われる
ネットワーク端末装置の動作処理を示すフローチャート



フロントページの続き

Ｆターム(参考) 5J104 AA26 KA02 PA07
5K030 GA15 HA08 HD03 HD06 JA10 JT03 KA02 MB18