(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7577456号
(P7577456)

(45)発行日　令和6年11月5日(2024.11.5)

(24)登録日　令和6年10月25日(2024.10.25)

(51)国際特許分類

		FI		
Ｈ０４Ｌ　67/02　(2022.01)		Ｈ０４Ｌ	67/02	
Ｈ０４Ｌ　61/4511(2022.01)		Ｈ０４Ｌ	61/4511	
Ｈ０４Ｌ　9/14　(2006.01)		Ｈ０４Ｌ	9/14	
Ｇ０９Ｃ　1/00　(2006.01)		Ｇ０９Ｃ	1/00	６６０Ｅ

請求項の数　8　（全20頁）

(21)出願番号　特願2020-66185(P2020-66185)
(22)出願日　令和2年4月1日(2020.4.1)
(65)公開番号　特開2021-162778(P2021-162778A)
(43)公開日　令和3年10月11日(2021.10.11)
審査請求日　令和5年3月30日(2023.3.30)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部 琢磨
(74)代理人　100223941
弁理士　高橋 佳子
(74)代理人　100159695
弁理士　中辻 七朗
(74)代理人　100172476
弁理士　冨田 一史
(74)代理人　100126974
弁理士　大朋 靖尚
(72)発明者　森谷 郁文
東京都大田区下丸子３丁目３０番２号

最終頁に続く

(54)【発明の名称】　通信装置、通信装置の制御方法及びプログラム

(57)【特許請求の範囲】

【請求項１】

通信装置であって、

前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定する設定手段と、

アプリケーションから依頼されたホスト名の名前解決を行う場合、前記設定手段で前記暗号化通信を使用する設定がなされていることに少なくとも基づいて第１のＤＮＳサーバとの間で確立した暗号化された通信路を介して、前記第１のＤＮＳサーバに当該ホスト名の名前解決を依頼し、前記設定手段で前記暗号化通信を使用しない設定がなされていることに基づき平文で第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御する通信制御手段と、

前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの指定を受け付ける受付手段と、

前記受付手段で指定を受け付けたアプリケーションの識別情報であって、前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの識別情報を記憶する記憶手段と、

前記記憶手段に記憶されている識別情報と、依頼元のアプリケーションの種類とに基づき前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきアプリケーションであるか否かを判定する判定手段と、

ホスト名で指定された宛先にスキャンデータを送信する送信アプリケーションと、

Ｗｅｂブラウザアプリケーションと、
を有し、
前記判定手段によって、前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきでないアプリケーションであると判定された場合、前記通信制御手段は、前記設定手段で前記暗号化通信を使用する設定がなされている場合であっても、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御し、
前記送信アプリケーションと、前記Ｗｅｂブラウザアプリケーションは、前記受付手段で除外するアプリケーションとして指定することが可能であることを特徴とする通信装置。
【請求項２】
通信装置であって、
前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定する設定手段と、
アプリケーションから依頼されたホスト名の名前解決を行う場合、前記設定手段で前記暗号化通信を使用する設定がなされていることに少なくとも基づいて第１のＤＮＳサーバとの間で確立した暗号化された通信路を介して、前記第１のＤＮＳサーバに当該ホスト名の名前解決を依頼し、前記設定手段で前記暗号化通信を使用しない設定がなされていることに基づき平文で第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御する通信制御手段と、
前記暗号化通信を使用した名前解決の対象から除外する通信プロトコルの識別情報を記憶する記憶手段と、
前記記憶手段に記憶されている識別情報と、当該ホスト名で特定される相手先との通信に使用する通信プロトコルの種類とに基づき依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべき通信プロトコルであるか否かを判定する判定手段と、
を有し、
前記判定手段によって、依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきでない通信プロトコルであると判定された場合、前記通信制御手段は、前記設定手段で前記暗号化通信を使用する設定がなされている場合であっても、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御することを特徴とする通信装置。
【請求項３】
前記暗号化通信を使用した名前解決の対象から除外する通信プロトコルの指定を受け付ける受付手段を更に有し、
前記記憶手段には、前記受付手段で指定を受け付けた通信プロトコルの識別情報が記憶されることを特徴とする請求項２に記載の通信装置。
【請求項４】
前記受付手段では、少なくともＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を前記除外する通信プロトコルとして指定することが可能であることを特徴とする請求項３に記載の通信装置。
【請求項５】
前記記憶手段は、前記暗号化通信を使用した名前解決の対象から除外するホスト名のリストを更に記憶しており、
前記通信制御手段は、前記名前解決を依頼されたホスト名が、前記記憶手段に記憶されている前記除外するホスト名のリストに含まれている場合、前記設定手段でなされた設定に関わらず、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御することを特徴とする請求項１乃至４のいずれか１項に記載の通信装置。
【請求項６】
通信装置の制御方法であって、
前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定する設定工程と、
アプリケーションから依頼されたホスト名の名前解決を行う場合に、前記設定工程でな

された設定に基づき、第１のＤＮＳサーバとの間で確立した暗号化された通信路を介して、前記第１のＤＮＳサーバに当該ホスト名の名前解決を依頼するか、平文で第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するかを異ならせる通信制御工程と、
前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの指定を受け付ける受付工程と、
前記受付工程で指定を受け付けたアプリケーションの識別情報であって、前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの識別情報を記憶手段に記憶する記憶工程と、
前記記憶手段に記憶されている識別情報と、依頼元のアプリケーションの種類とに基づき前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきアプリケーションであるか否かを判定する判定工程と、
を有し、
前記判定工程によって、前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきでないアプリケーションであると判定された場合、前記通信制御工程は、前記設定工程で前記暗号化通信を使用する設定がなされている場合であっても、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御し、
前記通信装置で動作可能なアプリケーションである、ホスト名で指定された宛先にスキャンデータを送信する送信アプリケーションと、Ｗｅｂブラウザアプリケーションは、前記受付工程で除外するアプリケーションとして指定することが可能であることを特徴とする制御方法。

【請求項７】
通信装置の制御方法であって、
前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定する設定工程と、
アプリケーションから依頼されたホスト名の名前解決を行う場合、前記設定工程で前記暗号化通信を使用する設定がなされていることに少なくとも基づいて第１のＤＮＳサーバとの間で確立した暗号化された通信路を介して、前記第１のＤＮＳサーバに当該ホスト名の名前解決を依頼し、前記設定工程で前記暗号化通信を使用しない設定がなされていることに基づき平文で第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御する通信制御工程と、
前記暗号化通信を使用した名前解決の対象から除外する通信プロトコルの識別情報を記憶手段に記憶する記憶工程と、
前記記憶手段に記憶されている識別情報と、当該ホスト名で特定される相手先との通信に使用する通信プロトコルの種類とに基づき依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべき通信プロトコルであるか否かを判定する判定工程と、
を有し、
前記判定工程によって、依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきでない通信プロトコルであると判定された場合、前記通信制御工程は、前記設定工程で前記暗号化通信を使用する設定がなされている場合であっても、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御することを特徴とする通信装置。

【請求項８】
少なくとも１つのコンピュータを、請求項１乃至５のいずれか１項に記載された通信装置の各手段として機能させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部にデータを送信する通信装置に関するものである。
【背景技術】
【０００２】

近年、Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ（以下、ＤＮＳ）に対してホスト名の名前解決を依頼する際に、盗聴・なりすまし・改善を防ぐための技術として、ＤＮＳ　ｏｖｅｒ　ＨＴＴＰＳ（以下、ＤｏＨ）といった仕組みが考えられている。

【０００３】

ＤｏＨでは、ＤＮＳへの名前解決依頼等の問い合わせを平文による通信ではなく、ＨＴＴＰＳにより暗号化された通信経路を介して行うことができる。主要なＷｅｂブラウザアプリーションではＷｅｂブラウザアプリケーションのＤＮＳ設定をＤＮＳからＤｏＨに切り替えることでＤｏＨを使用することができる。この仕組みによりブラウザアプリケーションがＵＲＬを名前解決する際に、第三者による依頼内容の盗聴、なりすましによる依頼結果の改ざんを防ぐことができる。

【０００４】

また、特許文献１にはセキュリティの観点で、デバイスにインストールされたアプリケーション毎に、ＤＮＳサーバへの名前解決を許容するか否かを設定するデバイスが開示されている。

【先行技術文献】

【特許文献】

【０００５】

【文献】特開２０１７－１３９６４８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

前述したように、Ｗｅｂブラウザアプリケーション等単体のアプリケーションの設定としてＤｏＨを使用する動作設定を設けることが知られている。

【０００７】

ところで、ＭＦＰ（Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）やＰＣなどの通信装置では、ファイルサーバへのアクセスなど、Ｗｅｂブラウザアプリケーション以外でもホスト名で指定された通信相手と通信を行うことがある。また、組織や会社などのセキュリティポリシによっては通信装置におけるホスト名の名前解決によりセキュアなＤｏＨを使用することが推奨される場合がある。この場合、単体のアプリケーションの設定としてＤｏＨを使用するか否かを設ける、アプリケーション側でＤｏＨを使用するか否かを切り替えることも考えられるが、設定の手間がかかったり設定漏れが発生したりといった問題がある。しかしながら、従来はシステム全体や装置全体の通信においてＤｏＨを使用する設定を行うための具体的な仕組みが考えられていなかった。

【０００８】

本発明は上述の問題点の少なくとも１つを鑑みなされたものである。本発明の１つの側面としては、前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定できるようにし、通信装置における名前解決の依頼先を適切に切り替えることができる仕組みを提供することを目的の１つとする。

【課題を解決するための手段】

【０００９】

上記の少なくとも１つの目的を達成するために本発明の通信装置は、

前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定する設定手段と、

アプリケーションから依頼されたホスト名の名前解決を行う場合、前記設定手段で前記暗号化通信を使用する設定がなされていることに少なくとも基づいて第１のＤＮＳサーバとの間で確立した暗号化された通信路を介して、前記第１のＤＮＳサーバに当該ホスト名の名前解決を依頼し、前記設定手段で前記暗号化通信を使用しない設定がなされていることに基づき平文で第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御する通信制御手段と、

前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの指定を受け付

ける受付手段と、
前記受付手段で指定を受け付けたアプリケーションの識別情報であって、前記暗号化通信を使用した名前解決の対象から除外するアプリケーションの識別情報を記憶する記憶手段と、
前記記憶手段に記憶されている識別情報と、依頼元のアプリケーションの種類とに基づき前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきアプリケーションであるか否かを判定する判定手段と、
ホスト名で指定された宛先にスキャンデータを送信する送信アプリケーションと、
Ｗｅｂブラウザアプリケーションと、
を有し、
前記判定手段によって、前記依頼元のアプリケーションが前記暗号化通信を使用した名前解決の対象とすべきでないアプリケーションであると判定された場合、前記通信制御手段は、前記設定手段で前記暗号化通信を使用する設定がなされている場合であっても、平文で前記第２のＤＮＳサーバに当該ホスト名の名前解決を依頼するよう制御し、
前記送信アプリケーションと、前記Ｗｅｂブラウザアプリケーションは、前記受付手段で除外するアプリケーションとして指定することが可能であることを特徴とする。

【発明の効果】

【００１０】

本発明の１つの側面によれば、前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定することで通信装置の名前解決先を適切に切り替えることができるようになる。

【図面の簡単な説明】

【００１１】

【図１】通信システムの一例を示す図である。
【図２】ＭＦＰ１０１のハードウェア構成の一例を示す図である。
【図３】ＭＦＰ１０１のソフトウェア構成の一例を示す図である。
【図４】ネットワークに関する設定画面の一例を示す図である。
【図５】第１の実施形態におけるネットワークに関する設定画面の一例を示す図である。
【図６】第１の実施形態におけるＭＦＰ１０１の制御の一例を示すフローチャートである。
【図７】第２の実施形態におけるネットワークに関する設定画面の一例を示す図である。
【図８】第２の実施形態におけるＭＦＰ１０１の制御の一例を示すフローチャートである。
【図９】第３の実施形態におけるセキュリティポリシに関する設定画面の一例を示す図である。
【図１０】第３の実施形態におけるＭＦＰ１０１の制御の一例を示すフローチャートである。
【図１１】設定画面の変形例の一例を示す図である。

【発明を実施するための形態】

【００１２】

以下、本発明を実施するための実施形態について図面を用いて説明する。なお、以下の実施の形態は特許請求の範囲に係る発明を限定するものではなく、また、実施の形態で説明されている特徴の組み合わせのすべてが発明の解決手段に必須のものとは限らない。

【００１３】

＜第１の実施形態＞

まず、図１を用いて、本発明に係る通信システムの構成を説明する。本実施形態に係る通信システムには、ＭＦＰ（Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）１０１、ＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）サーバ１０２、メールサーバ１０３がネットワーク１００を介して通信可能に接続されている。また、ファイルサーバ１０４、プリントサーバ１０５がネットワーク１００を介して通信可能に接続されている。サーバ１０３～１０５には、ＤＮＳサーバ１０２で管理されるホスト名が割り振られている。また、ＭＦＰ１０１は、ネットワーク１００及び、ＷＡＮ等を介してインターネット１０

６上のＤｏＨ（ＤＮＳ　Ｏｖｅｒ　ＨＴＴＰＳ）サーバ１０７やＷｅｂサーバ１０８と通信可能に接続されている。ネットワーク１００は、例えば、社内や組織内等のローカルゾーンである。また、サーバ１０３～１０５は、ローカルゾーンのクライアント向けに提供されるサーバである。従って、サーバ１０３～１０５に対応するホスト名の名前解決はローカルゾーン内のＤＮＳサーバでしか行うことができない。言い換えると、インターネット上に配置されているＤｏＨサーバ１０７はローカルゾーンのホスト名（社内や組織内向けに運用されているホスト名）の名前解決を行えない。

【００１４】

ＭＦＰ１０１は、通信端末の一例である。本実施形態では、一例として印刷機能や原稿をスキャンして得られた画像を外部に送信する送信機能を有するＭＦＰを例示しているがこれに限定されるものではない。ＩｏＴデバイス、パーソナルコンピューター、スマートフォンなどの通信装置に適用することもできる。

【００１５】

ＭＦＰ１０１は、スキャンして得られた画像に基づくデータ（スキャンデータとも呼ぶ）をファイルサーバに送信したり、メールに添付して送信したりする送信機能を有する。以降画像に基づくデータをメール送信やファイル送信を行う送信機能を単にＳＥＮＤ機能とも呼ぶ。

【００１６】

また、ＭＦＰ１０１は、プリントサーバ１０５にアクセスし、プリントサーバに蓄積された印刷データを受信して印刷するプルプリント機能を有する。また、ＭＦＰ１０１はＷｅｂブラウザアプリケーションを有しており、Ｗｅｂサーバ１０８等から取得したＷｅｂコンテンツをＭＦＰ１０１の操作部１１６に表示することができる。

【００１７】

ＳＥＮＤ機能でデータを送信する際に、ＭＦＰ１０１は、サーバのホスト名を指定した宛先を用いて送信を行う。また、ＭＦＰ１０１は、データを添付したメールを送信する場合、メールサーバ１０３のホスト名を名前解決し、当該メールサーバ１０３と通信するためのＩＰアドレスを取得する。続けて当該ＩＰアドレスを用いてメールサーバ１０３と通信を行って、メールを送信する。また、ＭＦＰ１０１においてＷｅｂコンテンツを表示する場合、Ｗｅｂサーバ（例えば、Ｗｅｂサーバ１０８）のＵＲＬを入力して、Ｗｅｂコンテンツの取得先サーバの特定を行う。この際のホスト名の名前解決の方法については、後述する。

【００１８】

＜ＭＦＰ１０１のハードウェア構成＞

続けて、図２を用いて、ＭＦＰ１０１について説明する。図２は、ＭＦＰ１０１のハードウェア構成を示すブロック図である。ＭＦＰ１０１はシート上の画像を読み取る読取機能、当該読み取った画像を外部の通信装置に送信可能なファイル送信機能などを有している。また、シートに画像を印刷する印刷機能も有する。

【００１９】

ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１１を含む制御部１１０は、ＭＦＰ１０１全体の動作を制御する。ＣＰＵ１１１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１１２又はストレージ１１４に記憶された制御プログラムを読み出して、印刷制御や読取制御などの各種制御を行う。ＲＯＭ１１２は、ＣＰＵ１１１で実行可能な制御プログラムを格納する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１１３は、ＣＰＵ１１１がアクセスする主記憶メモリであり、ワークエリア又は各種制御プログラムを展開するための一時記憶領域として用いられる。ストレージ１１４は、印刷データ、画像データ、各種プログラム、及び各種設定情報を記憶する。このように、ＣＰＵ１１１、ＲＯＭ１１２、ＲＡＭ１１３、ストレージ１１４等のハードウェアは、いわゆるコンピュータを構成している。

【００２０】

なお、本実施形態のＭＦＰ１０１では、１つのＣＰＵ１１１が１つのメモリ（ＲＡＭ１

１３）を用いて後述するフローチャートに示す各処理を実行するものとするが、他の様態であっても構わない。例えば複数のプロセッサ、メモリ、及びストレージを協働させて後述するフローチャートに示す各処理を実行することもできる。また、ハードウェア回路を用いて一部の処理を実行するようにしてもよい。

【００２１】

プリンタＩ／Ｆ（インタフェース）１１９は、プリンタ１２０（プリンタエンジン）と制御部１１０とを接続する。プリンタ１２０は、プリンタＩ／Ｆ１１９を介して入力された印刷データに基づいて、不図示の給紙カセットから給紙されたシートに画像を印刷する。印刷の方式はトナーを紙に転写して定着させる電子写真方式であってもよいし、紙にインクを吐出して印刷するインクジェット方式であってもよい。また、プリンタ１２０は造形材料を用いて３次元形状の出力物を生成する３Ｄプリンタであってもよい。この場合、印刷データは３Ｄ形状を示す印刷データとなり、トナーやインク等の色材に代えて造形材やサポート材を用いて３次元形状の出力物を生成する。

【００２２】

スキャナＩ／Ｆ１１７は、スキャナ１１８と制御部１１０とを接続する。スキャナ１１８は、図示省略の原稿台に載置された原稿を読み取り、そして画像データを生成する。スキャナ１１８が生成した画像データは、プリンタ１２０で印刷されたり、ストレージ１１４に記憶されたり、ネットワークＩ／Ｆ１２１を介して外部装置に送信されたりする。

【００２３】

操作部Ｉ／Ｆ１１５は、操作部１１６と制御部１１０とを接続する。操作部１１６には、タッチパネル機能を有する液晶表示部や各種ハードキーなどが備えられている。操作部１１６は、ユーザに情報を表示する表示部やユーザの指示を受け付ける受付部として機能する。ＣＰＵ１１１は、操作部１１６と協働して情報の表示制御やユーザ操作の受け付け制御を行う。

【００２４】

ネットワークＩ／Ｆ１２１には、ネットワークケーブルが接続され、ネットワーク１００上やインターネット上の外部装置と通信を実行することができる。本実施形態では、ネットワークＩ／Ｆ１２１がイーサネット（登録商標）に準拠する有線通信を行う通信インタフェースである場合を想定しているがこれに限定されるものではない。例えば、ＩＥＥＥ８０２．１１シリーズに準拠する無線通信インタフェースであってもよい。また、両方が無線通信インタフェースであってもよい。また、ＣＤＭＡ等の３Ｇ回線、ＬＴＥなどの４Ｇ回線、５Ｇ　ＮＲなどの移動体通信を行う通信インタフェースであってもよい。

【００２５】

＜ＭＦＰ１０１のソフトウェア構成＞

続けて、図３を用いて、ＭＦＰ１０１のソフトウェア構成について説明する。なお、図３に示す各機能ブロックは、ＣＰＵ１１１がＲＡＭ１１３に展開したプログラムを実行することにより実現するものとする。

【００２６】

ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）１０２０は、コンピュータの基本的な制御を行うプログラムである。ＯＳ１０２０は、アプリケーションやミドルウェアのプロセスを管理する管理モジュール、ネットワーク通信を行うためのＴＣＰ／ＩＰプロトコルスタックとして機能するモジュール機能、名前解決を行うためのＯＳ標準ＤＮＳクライアント１０２１を含む。また、ミドルウェア１０３０は、ＯＳ１０２０の上位レイヤに位置するモジュール群である。ミドルウェア１０３０は、ＭＦＰ１０１の動作設定を管理するモジュールや、名前解決を暗号化した通信経路で実行するためのＤｏＨ（ＤＮＳ　ｏｖｅｒ　ＨＴＴＰＳ）クライアント１０８０を含む。また、ＭＦＰ１０１は、紙面の都合上図示を省略している印刷を制御するモジュール等のミドルウェアも備えているものとする。アプリケーション１０１０は、ＯＳ１０２０上で動作するＭＦＰの機能を実現するためのアプリケーション群である。

【００２７】

まずＭＦＰ１０１が有するアプリケーション群について説明する。Ｗｅｂブラウザアプリケーション１０１０ａは、ネットワーク上のＷｅｂサーバから取得したＷｅｂコンテンツを表示するＷｅｂブラウザである。ＳＥＮＤアプリケーション１０１０ｂはファイルサーバや、メールサーバ経由でスキャナ１１８を用いて原稿をスキャンして得られた画像に基づくデータを送信するアプリケーションである。ＳＥＮＤアプリケーション１０１０ｂは、スキャナ１１８で原稿を読み取って得られた画像に基づくファイルをユーザにより指定された送信宛先に送信することができる。送信宛先は図示省略の送信設定画面を介してユーザ操作により指定することができる。ユーザは、ファイルサーバやメールサーバのホスト名をＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）の形式で入力することで宛先を指定する。送信設定画面を介して送信宛先が設定された後に、送信を開始するキーの選択を受け付けたことに従って、ＳＥＮＤアプリケーション１０１０ａは原稿の読み取りをスキャナ１１８に依頼する。続けてＳＥＮＤアプリケーション１０１０ａは、原稿を読み取って得られた画像に基づくデータをユーザにより指定された送信宛先に送信する。なお、本実施形態では送信処理の一例としてＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）やＳＦＴＰ（ＳＳＨ　ＦＴＰ）等の送信プロトコルを用いたファイル送信を想定している。また、ＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）を用いてメールサーバ１０３を経由したメール送信処理を行うことを想定している。しかしながら、これに限定されるものではなく、ＷｅｂＤＡＶ（Ｗｅｂ－ｂａｓｅｄ　Ｄｉｓｔｒｉｂｕｔｅｄ　Ａｕｔｈｏｒｉｎｇ　ａｎｄ　Ｖｅｒｓｉｏｎｉｎｇ）等の通信プロトコルを用いたファイル送信に適用することもできる。

【００２８】

プルプリントアプリケーション１０１０ｂはプリントサーバ１０５に蓄積された印刷ジョブを受信し、印刷部１２０を介して印刷するプリントアプリケーションである。アプリケーション１０１０ｂは、ネットワーク１００上のプリントサーバ１０５に対して印刷ジョブの問い合わせを行ったり、ＵＲＬ形式で指定されるジョブデータをクラウドサーバやクラウドストレージからダウンロードして印刷を行ったりする。これらの通信にもホスト名やＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｓｅ　Ｌｏｃａｔｅｒ）で指定された宛先と通信を行うことになる。なお、これらのアプリケーションが通信を行う際の名前解決やデータの送信処理は、ミドルウェア１０３０やＯＳ１０２０と協働して行われる。

【００２９】

このように、ＭＦＰ１０１などの通信装置では、ファイルサーバへのアクセスなど、Ｗｅｂブラウザアプリケーション以外でもホスト名で指定された通信相手と通信を行うことがある。また、組織や会社などのセキュリティポリシによっては通信装置におけるホスト名の名前解決によりセキュアなＤｏＨを使用することが推奨される場合がある。この場合、単体のアプリケーションの設定としてＤｏＨを使用するか否かを設ける、アプリケーション側でＤｏＨを使用するか否かを切り替えることも考えられるが、設定の手間がかかったり設定漏れが発生したりといった問題がある。

【００３０】

本実施形態では、前記通信装置の動作設定として名前解決のために暗号化通信を使用するか否かを設定できるようにし、通信装置における名前解決の依頼先を適切に切り替える仕組みを提供する。

【００３１】

図３の説明に戻り、ＯＳ１０２０はネットワーク通信を行うためのＴＣＰ／ＩＰプロトコルスタックや、名前解決を行うためのＯＳ標準ＤＮＳクライアント１０２１も含む。本実施形態では、ＤＮＳクライアント１０２１は、Ｌｉｎｕｘ（登録商標）システムにおける標準のＤＮＳクライアントである場合を想定している。これらのクライアントを用いてドメイン名の名前解決を行う場合、「／ｅｔｃ／ｒｅｓｏｌｖｅ．ｃｏｎｆ」に位置するファイルに対して、「ｎａｍｅｓｅｒｖｅｒ　“ＤＮＳサーバのＩＰアドレス“」といった記載を行ってＤＮＳサーバを指定する。冗長化のため、利用するＤＮＳサーバを複数指定することもできる。本実施形態では、ＤＮＳサーバ１０２のＩＰアドレスが設定されてい

るものとして説明する。ＤＮＳクライアント１０２１は指定されたＤＮＳサーバに対して平文で名前解決を依頼する機能を備える。

【００３２】

続けてミドルウェア群１０３０の動作について説明する。設定値ＤＢ１０５０には通信設定を含むＭＦＰ１０１の動作設定が記憶される。通信設定には、各通信インタフェースの設定や、ＤＮＳに関する設定を示す設定を含む。ＤｏＨクライアント１０８０は、ＤｏＨをサポートするＤｏＨサーバ１０７との間で暗号化された通信経を確立し、当該確立した通信路を経由したＨＴＴＰ通信でサーバ１０７に名前解決を依頼する。

【００３３】

ＤＮＳ制御部１０４０は、設定画面を操作部１１６に表示し、管理者等のユーザから各種ネットワーク設定の変更を受け付けて設定値ＤＢ１０５０に格納する機能を有する。また、制御部１０４０は、ＤＮＳ設定制御部１０４０ａを有する。ＤＮＳ設定制御部１０４０ａは、設定値ＤＢ１０５０の値を参照し、ＤｏＨクライアント１０８０およびＤＮＳクライアント１０２１の起動制御や動作設定制御を行う。また、ＤＮＳ制御部１０４０は、アプリケーションから受け取ったホスト名の名前解決をＤＮＳクライアント１０２１に依頼するか、ＤｏＨクライアント１０８０に依頼するかを判断する機能を備える。

【００３４】

なお、制御部１０４０は、図示省略のＷｅｂサーバ機能と協働して、名前解決に関する設定を確認、変更するためのＷｅｂページを提供することもできる。この場合、管理者等のユーザは、ＰＣなどのクライアントからＭＦＰ１０１が提供するＷｅｂページにアクセスし、名前解決に関する設定の変更を行うことができる。

【００３５】

ＤＮＳサーバ自動取得部１０７０は、ＤＮＳサーバやＤｏＨサーバのアドレスをＤＨＣＰサーバやＩＰｖ６ルータから取得する機能を有する。制御部１０４０は、取得部１０７０と協働して、ＤＮＳサーバのＩＰアドレスやＤｏＨサーバのホスト名／ＩＰアドレスをＤＨＣＰサーバやＩＰｖ６サーバから取得し、ＤＮＳの動作設定として保存する。ＤＮＳサーバ自動取得部１０７０はＤＮＳサーバの自動取得が有効に設定された場合、ネットワークからＤＮＳサーバの設定を取得する。自動取得部１０７０はＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）クライアントを含む。自動取得部１０７０のＤＨＣＰクライアントは、ネットワーク上のＤＨＣＰサーバに対して名前解決サーバを問い合わせるＤＨＣＰオプションを含む要求を送信して、ＤＮＳサーバやＤｏＨサーバのアドレスを取得する。なお、プロトコルスタックとしてＩＰｖ６を採用する場合、ＲＳ（Ｒｏｕｔｅｒ Ｓｏｌｉｃｉｔａｔｉｏｎ）、ＲＡ（Ｒｏｕｔｅｒ Ａｄｖｅｒｔｉｓｅｍｅｎｔ）のやり取りで、ＤＮＳサーバやＤｏＨサーバのアドレスを取得することもできる。

【００３６】

＜ＭＦＰ１０１におけるＤＮＳに関する動作設定＞

制御部１０４０ａが提供する画面を介したＤＮＳに関する動作設定の一例について図４を用いて説明する。画面４００は、ＭＦＰ１０１の操作部１１６に表示される画面の一例である。

【００３７】

キー４０１ａは、ＤｏＨを使用する動作設定を有効（ＯＮ）にする場合に使用するキーであり、キー４０１ｂは、ＤｏＨを使用する動作設定を無効（ＯＦＦ）にする場合に使用するキーである。キー４０１ａ、４０１ｂはいずれか一方が有効にセットされ、他方は無効にセットされる。ここではＤｏＨを名前解決に使用する動作設定が有効に設定されている場合を例示している。

【００３８】

キー４０２ａは、ＤＨＣＰサーバや、ＲＡなどからＤｏＨサーバアドレスの自動取得を行う動作設定を有効（ＯＮ）にする場合に使用するキーである。一方、キー４０２ｂは、ＤｏＨサーバアドレスの自動取得を行う動作設定を無効（ＯＦＦ）にする場合に使用する

キーである。キー４０２ａ、４０２ｂはいずれか一方が有効にセットされ、他方は無効にセットされる。画面４００では、自動取得を行う設定がなされている場合を例示している。

【００３９】

領域４０３は、ＤｏＨサーバの設定を表示する領域である。また領域４０３は、キー４０１ｂが有効に設定され、自動取得が無効に設定された場合に、ＤｏＨサーバのホスト名やＩＰアドレスを手動設定する領域として機能する。この場合、ユーザは操作部１１６に表示される図示省略のソフトウェアキーボードを介してＩＰアドレスやホスト名を入力することで、ＤｏＨサーバアドレスを手動設定することができる。

【００４０】

キー４０４は、ＤｏＨの例外設定を行う場合に使用するキーである。詳細は後述する。キー４０５ａ、４０５ｂは、平文で名前解決を行うＤＮＳサーバのＩＰアドレスを自動取得するかどうかを切り替えるキーである。本実施形態では、自動取得を行う動作設定がなされている場合を例示している。領域４０７は、ＤＮＳサーバの設定を表示する領域である。当該領域４０７は自動取得が無効に設定された場合に、ＤＮＳサーバのＩＰアドレスを手動設定する領域としても機能する。制御部１０４０ａは、画面４００を介して設定操作がなされた後に、決定キーが押下されたことを検知すると、当該画面を介してなされた設定をＭＦＰ１０１の動作設定として設定値ＤＢ１０５０に記憶する。

【００４１】

続けて、ＤｏＨの例外設定について図５を用いて説明する。図５（Ａ）は、ＤｏＨの例外設定に関する画面の一例であり、図５（ｂ）は設定値ＤＢ１０５０に記憶される設定値の一例である。

【００４２】

ＭＦＰ１０１のＣＰＵ１１１は、画面４００のキー４０４が選択されたことを検知すると、操作部１１６に表示される画面を設定画面５００に遷移する。画面５００は、ＤｏＨクライアント１０８０による名前解決の例外を設定するための画面である。ユーザは、領域５０１に対するタッチ操作を行うことで、ＭＦＰ１０１が備えるアプリケーションごとに、名前解決をＤｏＨで行わない例外アプリケーションを設定することができる。ユーザは、当該画面を介した操作で、ＤｏＨから使用した名前解決の対象から除外するアプリケーションを指定することができる。本実施形態では、例外アプリケーションに、ＳＥＮＤアプリケーション１０１０ｂが設定されている場合を例示している。例えば、管理者等は、ユーザの利用実績を踏まえて、専らローカルゾーン上のサーバと通信するアプリケーションについては、ＤｏＨを使用しないようにすることができる。従って、インターネット上にローカルゾーン上でローカルゾーン向けにサービスを提供しているサーバのホスト名がＤｏＨサーバ１０７に対して漏洩することを抑制できる。

【００４３】

領域５０２は、ＤｏＨサーバに対する名前解決依頼の例外とすべきホスト名を明示的に指定する際に用いられる領域である。以降、ＤｏＨサーバに対する名前解決依頼の例外とすべきホスト名を単に例外ホスト名等とも呼ぶ。例外ホスト名を追加したい管理者は、追加キーを押下し、図示省略の入力画面を介して例外ホスト名を入力する。編集キーは既に登録済みの例外ホスト名を編集する場合に使用するキーである。削除キーは、領域５０２に対するタッチ操作で選択された１以上の登録済みの例外ホスト名を削除する場合に使用するキーである。なお、Ｗｅｂ経由の画面を用いる場合、カンマ区切りで例外ホスト名を列挙したｃｓｖファイルなどをインポートし、例外ホスト名を登録できるようにすることもできる。制御部１０４０ａは、画面５００を介して設定操作がなされた後に、決定キーが押下されたことを検知すると、当該画面を介してなされた設定をＭＦＰ１０１の動作設定として設定値ＤＢ１０５０に記憶する。

【００４４】

図５を介したユーザ操作でなされた例外アプリケーションや例外ホスト名の設定は、ＭＦＰ１０１の動作設定として設定値ＤＢ１０５０に格納される。図５（ｂ）は図４、図５（Ａ）を介してなされた名前解決に関する動作設定の一例である。領域５０２を介してな

された設定は、例外ホスト名を列挙したリスト構造のデータ（以降例外ホスト名リストとも呼ぶ）として格納される。ＤｏＨの設定は、ＤｏＨを使用するか否かを示す動作設定である。ＤＮＳプロバイダの設定は、ＭＦＰ１０１が使用するＤＮＳサーバのＩＰアドレスを示す設定である。ＤｏＨプロバイダは、ＭＦＰ１０１が使用するＤｏＨサーバのホスト名又はＩＰアドレスを示す設定である。例外アプリの設定は、ＤｏＨの例外とするアプリケーションの識別する識別情報としての名称を示す設定である。なお、設定値ＤＢ１０５０に記憶される情報は、アプリケーションを特定するためのアプリケーションを識別するＩＤなどであってもよい。当該設定は後述するフローチャートにて適宜参照される。

【００４５】

具体的な制御について図６のフローチャートを用いて説明する。図６のフローチャートに示す各動作（ステップ）は、ＣＰＵ１１１がＲＯＭ１１２またはストレージ１１４に記憶された各制御モジュールを実現するためのプログラムをＲＡＭ１１３に呼び出し、実行することにより実現される。なお、データの送受信処理などは、ネットワークＩ／Ｆ１２１と協働して実現されるものとする。また、処理の主体を明確にしたいケースにおいては、ＣＰＵ１１１により実行されるソフトウェアモジュールを主語として説明する。図６のフローチャートは、各種アプリケーションからホスト名等の名前解決の依頼がなされた場合に実行されるフローチャートである。

【００４６】

Ｓ６０１において、ＤＮＳ制御部１０４０は、設定値ＤＢ１０５０を参照し、ＤｏＨを使用する設定がなされているか否かを判定する。設定項目ＤｏＨに対応する設定値がＯＮの場合、ＤｏＨを使用する設定がなされていると判断し、処理をＳ６０２に進める。設定項目ＤｏＨに対応する設定値がＯＦＦの場合、ＤｏＨを使用する設定がなされていないと判断し、処理をＳ６０６に進める。

【００４７】

Ｓ６０２において、制御部１０４０は、アプリケーションから名前解決を依頼された名前解決対象のホスト名が例外ホスト名リストに含まれているか否かを判断する。例外ホスト名リスト内に、名前解決が依頼されたホスト名に合致するホスト名が登録されている場合、処理をＳ６０６に進め、登録されていない場合、処理をＳ６０３に進める。

【００４８】

Ｓ６０３において、制御部１０４０は、名前解決を依頼した依頼元のアプリケーションの種類を特定し、当該特定したアプリケーションの種類が例外アプリケーションとして指定されているか否かを判断する。当該特定したアプリケーションの種類が例外アプリケーションとして指定されている場合、処理をＳ６０６に進め、指定されていない場合、処理をＳ６０４に進める。Ｓ６０３で依頼元のアプリケーションを特定する具体的な手法としては以下の手法を採用することができる。例えば、ミドルウェア１０３０として機能する制御部１０４０は、名前解決を依頼する際に呼び出すべきＡＰＩ関数を各アプリケーションに対して提供する。このＡＰＩ関数は、アプリケーションを特定するための識別情報を引数として設定できるように構成される。各アプリケーションは当該ＡＰＩ関数を呼び出す（即ち、名前解決を依頼する）際に、アプリケーションを識別する識別情報を引数に設定する。制御部１０４０は、当該引数を参照することで、依頼元のアプリケーションの種類を特定することができる。

【００４９】

Ｓ６０４において、制御部１０４０は、ＤｏＨクライアント１０８０に対してアプリケーションから依頼された名前解決依頼を転送する。続けて、Ｓ６０５において、名前解決の依頼を受け付けたＤｏＨクライアント１０８０は、暗号化通信を用いてＤｏＨサーバ１０７に名前解決を依頼する。この際は、ＨＴＴＰＳの通信路で名前解決のための通信が行われるものとする。

【００５０】

Ｓ６０８において、制御部１０４０は、名前解決の結果をＤｏＨクライアント１０８０から受信し、当該名前解決の結果、ＩＰアドレスが取得できたか否かを判断する。ＤｏＨ

サーバ１０７による名前解決の結果、ホスト名に対応するＩＰアドレスが取得できた場合、処理をＳ６０９に進め、ホスト名に対応するＩＰアドレスが取得できなかった場合、処理をＳ６０６に進める。例えば、制御部１０４０は、ＤｏＨサーバと通信が行えない場合やＤｏＨサーバか受信した名前解決の結果が宛先を見つけられなかったことを示している場合、ＩＰアドレスが取得できなかったと判定する。このＳ６０８の処理は、ＤｏＨで宛先が見つからなかった場合に平文による名前解決に遷移するフォールバックを実現するための処理である。

【００５１】

Ｓ６０６において、制御部１０４０は、ＤＮＳクライアント１０２１に対して名前解決を依頼する。続けてＳ６０７において、ＤＮＳクライアント１０２１は、当該名前解決の依頼をＤＮＳサーバ１０２に転送する。当該名前解決の依頼は前述したように平文で行われる。ＤＮＳサーバ１０２は、自身が管理しているドメイン名であれば、当該ドメインに対応するＩＰアドレスを応答し、そうでなければ、上位のＤＮＳサーバに問合せを転送し、名前解決を行う。

【００５２】

最後に、Ｓ６０９において、制御部１０４０は、Ｓ６０７又はＳ６０５で送信した名前解決の依頼に対する応答をＳ６０９に返す。以上説明した一連の処理により、例外アプリケーションの設定や、例外ホスト名の設定に基づいて、ＤｏＨによる名前解決を試行するか、ＤｏＨを試行することなく従来の平文による名前解決を行うかの通信制御を柔軟に切り替えることができるようになる。

【００５３】

＜第２の実施形態＞

第１の実施形態では、アプリケーション毎にＤｏＨを行うか否かを設定する場合を例示した。第２の実施形態では、プロトコル毎にＤｏＨを行うか否かを設定する場合について説明する。なお、第２の実施形態におけるハードウェア構成及びソフトウェア構成は第１の実施形態と同様であるため、説明を省略する。

【００５４】

図７は、第２の実施形態におけるＤｏＨの例外設定を説明するための図である。図７（Ａ）は、第１の実施形態の図５（Ａ）に代えて表示される画面の一例である。図７（Ｂ）は第２の実施形態において設定値ＤＢ１０５０に記憶される設定値の一例である。

【００５５】

ＭＦＰ１０１のＣＰＵ１１１は、図４で説明した画面４００のキー４０４が選択されたことを検知すると、操作部１１６に表示される画面を設定画面７００に遷移する。領域７０２に示す例外ホスト名に関する設定は、第１の実施形態と同様であるため説明を省略する。

【００５６】

領域７０１には、ＭＦＰ１０１で使用される通信プロトコルが列挙される。ユーザは、当該領域７０１に対するタッチ操作を行うことで、例外とする通信プロトコルを設定することができる。ここでは、例外とする通信プロトコルに、ＳＭＢとＦＴＰ／ＳＦＴＰが設定されている場合を例示している。例えば、管理者等は、ユーザの利用実績を踏まえて、専らローカルゾーン上のサーバと通信する際に用いられる通信プロトコルについては、ＤｏＨを使用しないようにすることができる。制御部１０４０ａは、画面５００を介して設定操作がなされた後に、決定キーが押下されたことを検知すると、当該画面を介してなされた設定をＭＦＰ１０１の動作設定として設定値ＤＢ１０５０に記憶する。図７（Ａ）を介したユーザ操作でなされた例外アプリケーションや例外ホスト名の設定は、ＭＦＰ１０１の動作設定として設定値ＤＢ１０５０に格納される。図７（Ｂ）は図４、図７（Ａ）を介してなされた名前解決に関する動作設定の一例である。

【００５７】

第２の実施形態における具体的な制御について図８のフローチャートを用いて説明する。図８のフローチャートに示す各動作（ステップ）は、ＣＰＵ１１１がＲＯＭ１１２また

はストレージ１１４に記憶された各制御モジュールを実現するためのプログラムをＲＡＭ１１３に呼び出し、実行することにより実現される。なお、第１の実施形態と同様、データの送受信処理などは、ネットワークＩ／Ｆ１２１と協働して実現され、処理の主体を明確にしたいケースでは、ソフトウェアモジュールを主語として説明する。

【００５８】

Ｓ８０１～Ｓ８０２は第１の実施形態のＳ６０１～Ｓ６０２と同様の処理のため説明を省略する。

【００５９】

Ｓ８０３において、制御部１０４０は、名前解決を依頼されているホスト名に対応する通信プロトコルを特定し、当該通信プロトコルが例外プロトコルに指定されているか否かを判定する。例外プロトコルに指定されている場合、処理をＳ８０６に進め、指定されていない場合、処理をＳ８０４に進める。通信プロトコルの特定は第１の実施形態と同様の仕組みで、依頼元アプリケーションが引数に通信プロトコルの種類を設定した名前解決のためのＡＰＩ関数を呼び出し、制御部１０４０に通信プロトコルを通知するよう構成すればよい。

【００６０】

以降のＳ８０４～Ｓ８０９のＤｏＨ又はＤＮＳを用いた名前解決処理は第１の実施形態と同様であるため説明を省略する。

【００６１】

以上説明したように、第２の実施形態では、例外プロトコルの設定や、例外ホスト名の設定に基づいて、ＤｏＨによる名前解決を試行するかＤｏＨを試行することなく従来の平文による名前解決を行うかを柔軟に切り替えることができるようになる。

【００６２】

＜第３の実施形態＞

第１の実施形態及び第２の実施形態では、ＤｏＨによる名前解決を行うか否かの設定をネットワークに関する設定画面を介して行う場合を例に説明した。ここで、ＭＦＰ等の通信装置は、多種多様な設定を有しており、ネットワークに精通するネットワーク管理者等のユーザであっても設定漏れや設定ミスを行うことが考えられる。

【００６３】

これを鑑み、ＭＦＰ１０１には、ダイレクト接続などのネットワークの設定や認証ユーザのパスワードの桁数やロックアウトの設定など、セキュリティに関連する複数の設定を一括で変更するセキュリティポリシを設定する機能が設けられている。第３の実施形態では、第１の実施形態及び第２の実施形態で説明した設定制御に加え、セキュリティポリシを設定する画面を介して名前解決に暗号化を使用するか否かの設定変更を行えるようにする。以下具体的に説明する。

【００６４】

図９は操作部１１６に表示されるセキュリティポリシを設定する画面９００の一例である。本実施形態では、通信の運用ポリシを設定する画面から名前解決に暗号化通信を使用するか否かを設定できるようにしている。チェックボックス９０１は、名前解決に暗号化通信を使用する際に選択する表示アイテムである。また、ユーザは、図９を介して、その他の運用ポリシを設定することもできる。ＴＬＳ通信時に必ずサーバ証明書を検証するといったポリシが設定された場合、自己署名証明書や有効期限の切れた証明書によるＴＬＳ通信を遮断する設定がなされる。また、プルプリントアプリケーション１０１０ｃ等の個別設定についても、プリントサーバと通信を行う際の証明書の検証が必要な設定に変更される。また、サーバ機能で平文認証を禁止するポリシが設定された場合、平文認証や平文認証を使うサーバ機能の利用を一律禁止するよう、ＭＦＰ１０１の複数の設定値が変更される。

【００６５】

第３の実施形態における具体的な制御について図１０のフローチャートを用いて説明する。図１０のフローチャートに示す各動作（ステップ）は、ＣＰＵ１１１がＲＯＭ１１２

またはストレージ１１４に記憶された各制御モジュールを実現するためのプログラムをＲＡＭ１１３に呼び出し、実行することにより実現される。なお、第１の実施形態と同様、データの送受信処理などは、ネットワークＩ／Ｆ１２１と協働して実現される。

【００６６】

Ｓ１００１において、ＣＰＵ１１１はポリシの設定変更を反映するユーザ操作を受け付けたか否かを判断する。ポリシの設定変更を反映するユーザ操作を受け付けた場合、処理をＳ１００２に進め、受け付けていない場合、設定変更を待ち受ける。ポリシの設定変更を反映するユーザ操作は、例えば画面９００の決定キーを押下するユーザ操作である。

【００６７】

Ｓ１００２において、ＣＰＵ１１１は、名前解決に暗号化通信を使用するポリシが指定されているか否かを判断する。名前解決に暗号化通信を使用するポリシが指定されている場合、処理をＳ１００３に進め、指定されていない場合、処理をＳ１００６に進める。

【００６８】

Ｓ１００３において、ＣＰＵ１１１は、設定値ＤＢ１０５０に記憶される設定値をＤｏＨを使用する動作設定に変更する。具体的には、ＣＰＵ１１１は、ＤｏＨサーバアドレスの自動取得の設定が有効に設定するとともに、ＤｏＨを使用する設定を有効に変更する。また、図示省略のポートフィルタの設定も変更し、ＨＴＴＰＳ通信に必要な４４３番ポートの通信を許容する設定に変更する。なお、本実施形態では、自動取得を有効にする場合を例示にしたがこれに限定されるものではない。既にＤｏＨサーバのアドレスが手動入力されている場合、自動取得を有効とせずに、自動取得を無効とする設定を維持するよう制御にしてもよい。

【００６９】

続けて、Ｓ１００４において、ＣＰＵ１１１は、現在の動作設定値でＤｏＨサーバと通信可能であるか判断する。具体的にはＤｏＨサーバとの間で暗号化通信路の確立を試行し、暗号化通信を確立できるかどうかを確認する。また、実際に当該ＤｏＨサーバによる名前解決が行えるか否かを試行し名前解決が行えた場合に、通信可能であると判断してもよい。

【００７０】

通信可能であると判断した場合処理をＳ１００６に進め、通信可能でないと判断した場合処理をＳ１００５に進める。Ｓ１００５において、ＣＰＵ１１１は、操作部１１６にエラー画面を表示する。エラー画面にはエラーが発生した理由を示すエラーメッセージが表示される。また、当該エラー画面に、操作部１１６に表示する画面をＤＮＳ設定画面に遷移させるための表示アイテムを表示するように構成してもよい。この表示アイテムは、ＤｏＨサーバのアドレスが自動取得できなかったケースにおいて、ユーザがＤｏＨサーバアドレスの手動設定を行う際に役立つ。

【００７１】

Ｓ１００６において、ＣＰＵ１１１は、その他のポリシを有効に指定する操作を受け付けているか否かを判断する。その他のポリシを有効に指定する操作を受け付けている場合、処理をＳ１００７に進める。一方、その他のポリシを有効に指定する操作を受け付けていない場合、一連の処理を終了する。

【００７２】

Ｓ１００７において、ＣＰＵ１１１は、有効に指定されたその他のポリシに基づき、ＭＦＰ１０１の動作設定値を変更し、一連の処理を終了する。

【００７３】

以上説明した処理により、より簡単にＭＦＰ１０１の機能全体に波及するＤｏＨ設定を有効に切り替えることができるようになる。

【００７４】

＜変形例＞

第１の実施形態の制御に加えて、第２の実施形態の制御を行うようにしてもよい。この場合、例外設定として、アプリケーション、通信プロトコル、ホスト名を管理者等が設定

できるようになる。この場合、Ｓ６０３の判断ステップの後に、更にＳ８０３の判断ステップに示す判断処理を行うように構成すればよい。

【００７５】

また、第１乃至第２の実施形態では、ＤｏＨによる名前解決の例外とする例外アプリケーションや例外プロトコルを管理者等のユーザに選択させる場合を例示した。しかしながら、ＤｏＨを用いた名前解決を使用するか、従前の平文による名前解決を使用するかの設定方法は、適宜変形することができる。例えば、ＤｏＨによる名前解決を使用すべきアプリケーション又は通信プロトコルを選択させるようにすることができる。この場合、ＤｏＨによる名前解決を使用すべきアプリケーションを列挙した対象アプリケーションリストやＤｏＨによる名前解決を使用すべき通信アプリケーションを列挙した対象プロトコルリストが設定値ＤＢ１０５０に記憶される。この場合、第１の実施形態のＳ６０３の処理に代えて、要求元のアプリケーションが当該対象アプリケーションリストに含まれているか否かを判断する処理を行う。要求元のアプリケーションが対象アプリケーションリストに含まれている場合、処理をＳ６０４に進め、含まれていない場合、処理をＳ６０６に進めるようにすればよい。第２の実施形態についても同様に、Ｓ８０３の処理に代えて、ホスト名に対応する通信プロトコルが対象プロトコルリストに含まれているか否かを判断する処理を行うようにすればよい。

【００７６】

更に、図１１に例示するように選択方法を変形するとこもできる。図１１（Ａ）及び（Ｂ）は画面５００に代えて表示される変形例を示している。画面１１００には、アプリケーション毎にＤＮＳを使用するか、ＤｏＨを使用するかを択一で選択するための設定領域１１０１が表示される。ユーザは、当該画面を介してＭＦＰ１０１が有するアプリケーションごとにＤｏＨを使用するかＤＮＳを使用するかを決定することができる。ＭＦＰ１０１の制御部１０４０は、当該画面を介してなされた設定に基づき、前述した例外アプリケーションリストを生成して、設定値ＤＢ１０５０に格納する。１１０１には、括弧書きでＤＮＳが平文であること、ＤｏＨが暗号化であることが明確に示されている。従って管理者等のユーザは直感的に平文による名前解決を希望するか、ＤｏＨによるセキュリティの高い名前解決を希望するかをアプリケーション毎に異ならせることができる。

【００７７】

更には、画面１１１０のように選択方法を変形することもできる。領域１１１１は、アプリケーション毎に主たる通信相手先を択一で選択される表示領域である。管理者は、ＭＦＰ１０１が設置されているローカルゾーンが主な通信相手のアプリケーションについては、「イントラネット」を選択すればよい。例えば、管理者は、ローカルゾーンに設置されるプリントサーバ１０５と通信するプルプリントアプリケーションについては、ローカルゾーンを指定することができる。一方、管理者は、インターネット上のサーバが主たる通信相手のアプリケーションについては、「インターネット」を選択すればよい。

【００７８】

また、画面１１１０には、主用途にイントラネットを指定した場合、ＤｏＨを使用する設定がなされていても、平文のＤＮＳサーバでの名前解決を優先することを示すメッセージが表示される。

【００７９】

当該選択方法に変形する場合、ＭＦＰ１０１の制御部１０４０は、当該画面を介してなされた設定に基づき、主たる通信相手が「イントラネット」に指定されたアプリケーションを列挙した例外アプリケーションリストを生成し、設定値ＤＢ１０５０に格納する。

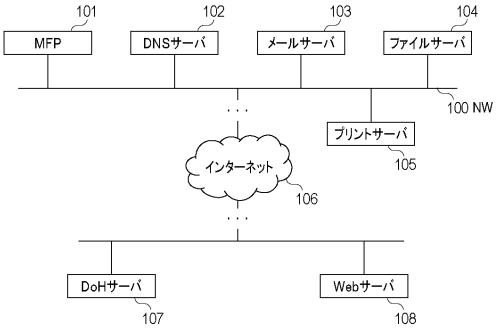
【００８０】

なお、図１１で説明した変形例は第２の実施形態に適用することもできる。この場合、ＭＦＰ１０１で使用される各通信プロトコルに対する選択方法を、図１１に例示した選択方法のように変形することができる。この場合に設定値ＤＢ１０５０に格納される例外プロトコルリストの生成方法などは例外アプリケーションリストの生成方法と同様であるため説明を省略する。

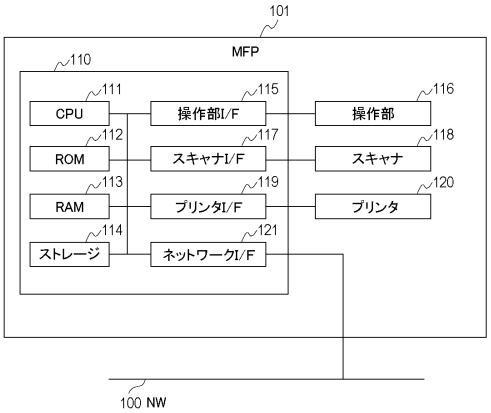
【００８１】
最後に、本実施形態では、名前解決に暗号化通信を使用する方式の一例としてＤｏＨを例示したがこれに限定されるものではない。通信路のみをＴＬＳで暗号化し、当該通信路上に平文のＤＮＳパケットを送信するＤｏＴ（ＤＮＳ　Ｏｖｅｒ　ＴＬＳ）を使用する場合にも適用することができる。
【００８２】
＜その他の実施形態＞
本発明は、上述の各実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣやＦＰＧＡ）によっても実現可能である。
【符号の説明】
【００８３】
１０１　ＭＦＰ
１１１　ＣＰＵ
１２１　ネットワークＩ／Ｆ

【図面】

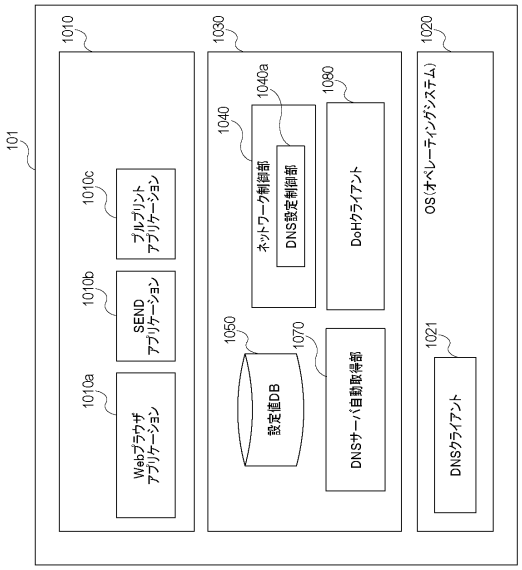
【図１】


101
MFP
102
DNSサーバ
103
メールサーバ
104
ファイルサーバ
100 NW
プリントサーバ
105
インターネット
106
DoHサーバ
107
Webサーバ
108

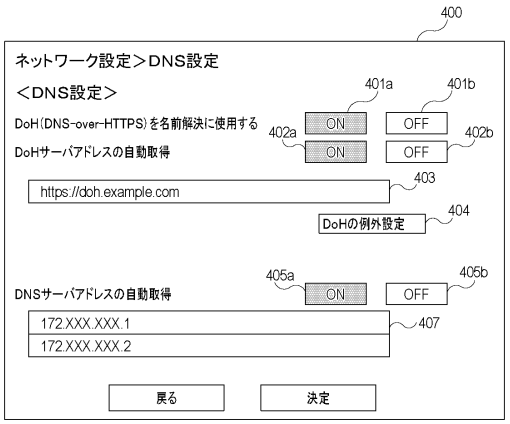
【図２】


101
MFP
110
CPU
111
ROM
112
RAM
113
ストレージ
114
操作部I/F
115
スキャナI/F
117
プリンタI/F
119
ネットワークI/F
121
操作部
116
スキャナ
118
プリンタ
120
100 NW

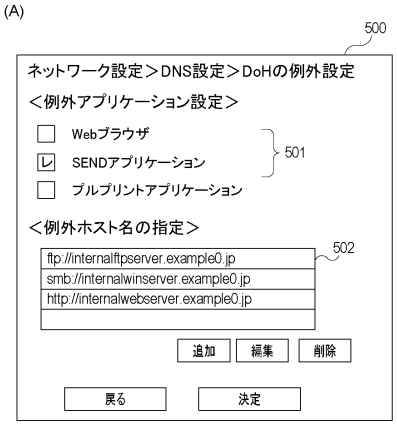
【図３】


101
1010
1010a
Webブラウザ アプリケーション
1010b
SEND アプリケーション
1010c
プルプリント アプリケーション
1030
1040
1040a
ネットワーク制御部
DNS設定制御部
1080
DoHクライアント
1050
設定値DB
1070
DNSサーバ自動取得部
1020
OS(オペレーティングシステム)
1021
DNSクライアント

【図４】


400
ネットワーク設定＞DNS設定
＜DNS設定＞
401a
401b
DoH(DNS-over-HTTPS)を名前解決に使用する
402a
ON
OFF
402b
DoHサーバアドレスの自動取得
ON
OFF
https://doh.example.com
403
DoHの例外設定
404
DNSサーバアドレスの自動取得
405a
ON
405b
OFF
172.XXX.XXX.1
172.XXX.XXX.2
407
戻る
決定

【図５】

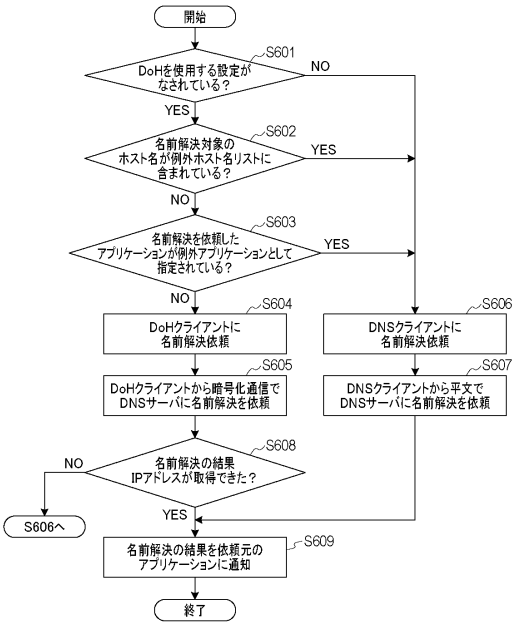


(B)

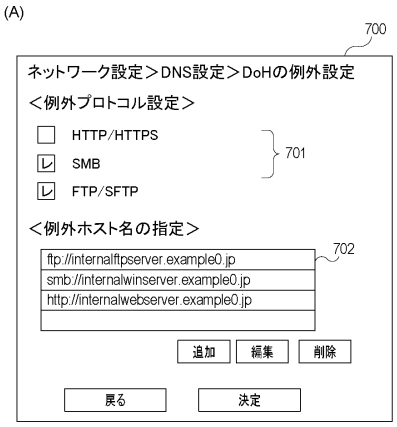
設定値DB1050に記憶される名前解決設定情報

設定項目	設定値
DoH	ON
DNSプロバイダ	172.XXX.XXX.1 172.XXX.XXX.2
DoHプロバイダ	https://doh.example.com
例外アプリ	SENDアプリケーション
例外ホスト名	ftp://internalftpserver.example0.jp, smb://internalwinserver.example0.jp, http://internalwebserver.example0.jp

【図６】



【図７】

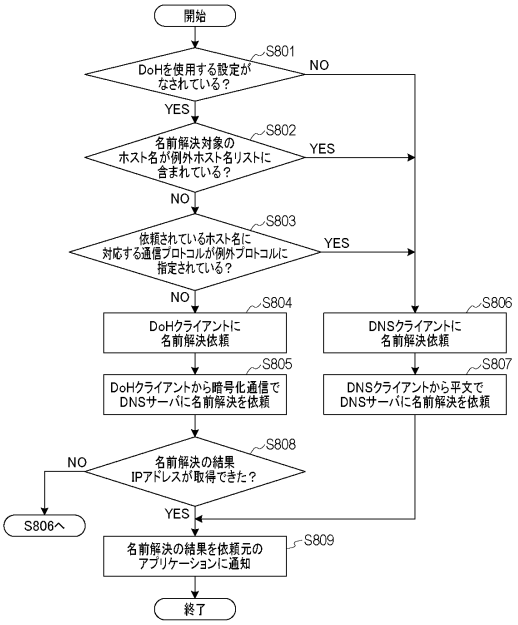


(B)

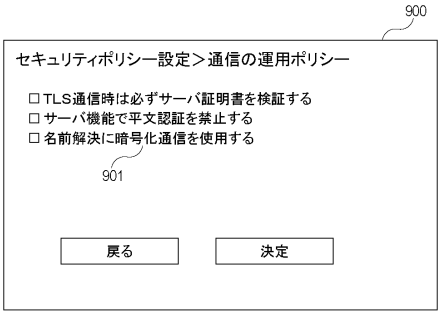
設定値DB1050に記憶される名前解決設定情報

設定項目	設定値
DoH	ON
DNSプロバイダ	172.XXX.XXX.1 172.XXX.XXX.2
DoHプロバイダ	https://doh.example.com
例外通信プロトコル	SMB, FTP, SFTP
例外ホスト名	ftp://internalftpserver.example0.jp, smb://internalwinserver.example0.jp, http://internalwebserver.example0.jp

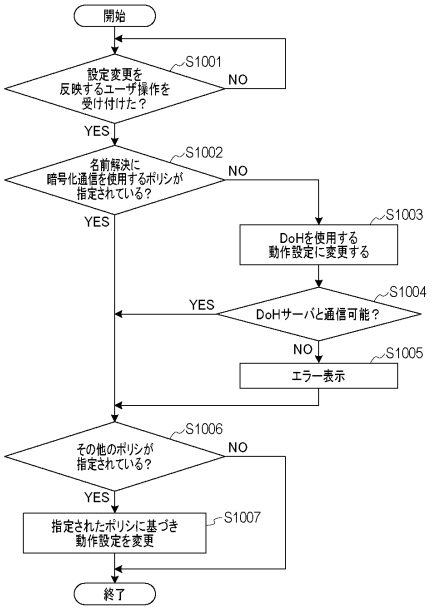
【図８】



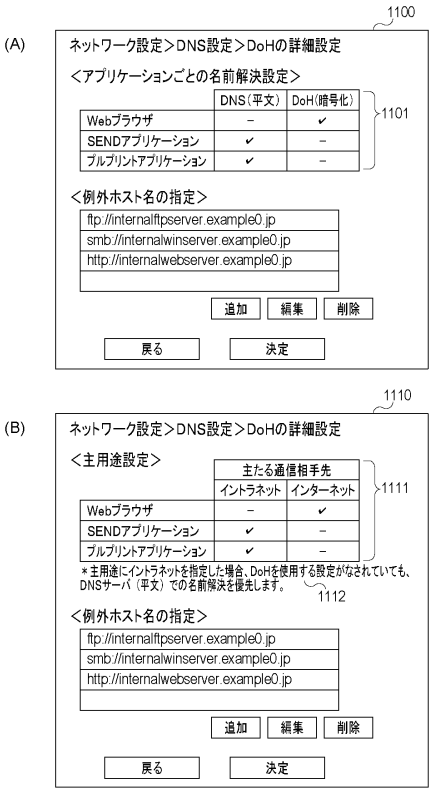
【図９】


900
セキュリティポリシー設定＞通信の運用ポリシー
□TLS通信時は必ずサーバ証明書を検証する
□サーバ機能で平文認証を禁止する
□名前解決に暗号化通信を使用する
901
戻る
決定

【図１０】


開始
S1001
設定変更を
反映するユーザ操作を
受け付けた？
NO
YES
S1002
名前解決に
暗号化通信を使用するポリシが
指定されている？
NO
YES
S1003
DoHを使用する
動作設定に変更する
S1004
DoHサーバと通信可能？
YES
NO
S1005
エラー表示
S1006
その他のポリシが
指定されている？
NO
YES
S1007
指定されたポリシに基づき
動作設定を変更
終了

【図１１】


(A)
1100
ネットワーク設定＞DNS設定＞DoHの詳細設定
＜アプリケーションごとの名前解決設定＞
DNS（平文） DoH（暗号化）
Webブラウザ － ✔
SENDアプリケーション ✔ －
プルプリントアプリケーション ✔ －
1101
＜例外ホスト名の指定＞
ftp://internalftpserver.example0.jp
smb://internalwinserver.example0.jp
http://internalwebserver.example0.jp
追加 編集 削除
戻る 決定
(B)
1110
ネットワーク設定＞DNS設定＞DoHの詳細設定
＜主用途設定＞
主たる通信相手先
イントラネット インターネット
Webブラウザ － ✔
SENDアプリケーション ✔ －
プルプリントアプリケーション ✔ －
1111
＊主用途にイントラネットを指定した場合、DoHを使用する設定がなされていても、DNSサーバ（平文）での名前解決を優先します。
1112
＜例外ホスト名の指定＞
ftp://internalftpserver.example0.jp
smb://internalwinserver.example0.jp
http://internalwebserver.example0.jp
追加 編集 削除
戻る 決定

フロントページの続き

キヤノン株式会社内

審査官　前田 健人

(56)参考文献

国際公開第２００５／０６９５３２（WO，Ａ１）
HIROKI TAGATO，IntraアプリでAndroid PのプライベートDNS機能をひと足先に試す，[オンライン]，2018年05月18日，[検索日 2024.04.24], インターネット：〈URL: https://blog.c6h12o6.org/post/android-intra〉
Mozilla，Firefox DNS-over-HTTPS，[オンライン]，2020年03月27日，２０２０年３月２７日インターネットアーカイブ受入 [検索日 2024.04.24], インターネット：〈URL: https://web.archive.org/web/20200327025822/https://support.mozilla.org/en-US/kb/firefox-dns-over-https〉
閲覧ページの盗み見や別ページへの誘導などの「ネット検閲」を防ぐためのDNS暗号アプリ「Intra」を使ってみました，[オンライン]，2018年10月04日，[検索日 2024.04.24], インターネット：〈URL: https://gigazine.net/news/20181004-jigsaw-intra〉
CNET Japan，Alphabet、DNSクエリを暗号化するアプリ「Intra」を公開--ネット検閲に対抗，[オンライン]，2018年10月04日，[検索日 2024.04.24], インターネット：〈URL: https://japan.cnet.com/article/35126541〉

(58)調査した分野　(Int.Cl.，ＤＢ名)

Ｈ０４Ｌ　６７／００－６７／７５
Ｈ０４Ｌ　６１／００－６１／５９
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／１４