(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2006-50407
(P2006-50407A)
(43)公開日　平成18年2月16日(2006.2.16)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/56	(2006.01)	H04L 12/56	Z	5J104
G09C 1/00	(2006.01)	G09C 1/00	660E	5K030
H04L 12/22	(2006.01)	H04L 12/22		5K101
H04M 11/00	(2006.01)	H04M 11/00	302	

審査請求 有　請求項の数 6　ＯＬ　（全 13 頁）

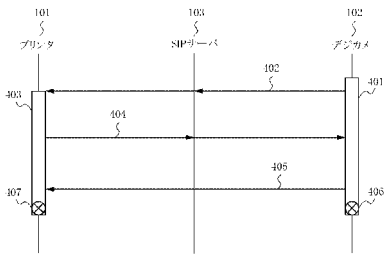
(21)出願番号　特願2004-230802 (P2004-230802)
(22)出願日　平成16年8月6日 (2004.8.6)

(71)出願人　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　100090538
弁理士　西山　恵三
(74)代理人　100096965
弁理士　内尾　裕一
(72)発明者　小川　勝久
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　鈴木　直彦
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

最終頁に続く

(54)【発明の名称】セキュリティポリシー設定方法、プログラム、及び、通信装置

(57)【要約】
【課題】　ＩＰｓｅｃ通信では、端末機器に、双方のＩＰアドレス、アプリケーションのポート番号、セキュリティタイプ、セキュリティレベル等のセキュリティポリシーを、事前設定しておかなければならない。
【解決手段】　デジカメ１０２が、ＳＩＰサーバ１０３を介してプリンタ１０１を呼び出すための接続呼出しメッセージ４０２を、デジカメ１０２のセキュリティポリシー設定情報を添付して送信する。プリンタ１０１は、受信したデジカメ１０２のセキュリティポリシー設定情報に基づいて、プリンタ１０１のセキュリティポリシーを設定し、接続応答メッセージ４０４を、プリンタ１０１のセキュリティポリシー設定情報を添付して送信する。デジカメ１０２は、受信したプリンタ１０１のセキュリティポリシー設定情報に基づいて、デジカメ１０２のセキュリティポリシーを設定する。
【選択図】　図５



【特許請求の範囲】
【請求項１】
第一の装置と第二の装置にセキュリティポリシーを設定する設定方法であって、
第一の装置が、ＳＩＰサーバを介して第二の装置を呼び出すための接続呼出しメッセージを、第一の装置のセキュリティポリシー設定情報を添付して送信し、
第二の装置は、受信した第一の装置のセキュリティポリシー設定情報に基づいて、第二の装置のセキュリティポリシーを設定し、接続応答メッセージを、第二の装置のセキュリティポリシー設定情報を添付して送信し、
第一の装置は、受信した第二の装置のセキュリティポリシー設定情報に基づいて、第一の装置のセキュリティポリシーを設定することを特徴とするセキュリティポリシーの設定方法。
【請求項２】
ＳＩＰサーバを介して通信相手を呼び出すための接続呼出しメッセージを、自身のセキュリティポリシー設定情報を添付して送信し、
通信相手のセキュリティポリシー設定情報を受信し、
受信した通信相手のセキュリティポリシー設定情報に基づいて、自身のセキュリティポリシーを設定することを特徴とするセキュリティポリシーの設定方法。
【請求項３】
通信相手のセキュリティポリシー設定情報の添付された接続呼出しメッセージを、ＳＩＰサーバを介して受信し、
受信した通信相手のセキュリティポリシー設定情報に基づいて、自身のセキュリティポリシーを設定し、
接続応答メッセージを、自身のセキュリティポリシー設定情報を添付して送信することを特徴とするセキュリティポリシーの設定方法。
【請求項４】
請求項２又は３の設定方法を実現するためのプログラム。
【請求項５】
ＳＩＰサーバを介して通信相手を呼び出すための接続呼出しメッセージを、自身のセキュリティポリシー設定情報を添付して送信する送信手段と、
通信相手のセキュリティポリシー設定情報を受信する受信手段と、
受信した通信相手のセキュリティポリシー設定情報に基づいて、自身のセキュリティポリシーを設定する設定手段を有することを特徴とする通信装置。
【請求項６】
通信相手のセキュリティポリシー設定情報の添付された接続呼出しメッセージを、ＳＩＰサーバを介して受信する受信手段と、
受信した通信相手のセキュリティポリシー設定情報に基づいて、自身のセキュリティポリシーを設定する設定手段と、
接続応答メッセージを、自身のセキュリティポリシー設定情報を添付して送信する送信手段を有することを特徴とする通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、第一の装置と第二の装置にセキュリティポリシーを設定する設定方法、セキュリティポリシーの設定プログラム、及び、通信装置に関する。
【背景技術】
【０００２】
ＩＰｓｅｃは、エンド・ツー・エンドのＩＰレイヤでのセキュリティを実現するための機能と安全性を備えた標準化技術である。ＩＰｓｅｃの中核はＩＫＥ（Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃａｎｇｅ）プロトコルによるＳＡ（Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ）の自動生成であり、ＳＡ確立は、セキュリティポリシー（ＳＰ）に基づきＰｈ

ａｓｅ　１（またはＩＳＡＫＭＰ　ＳＡ）、Ｐｈａｓｅ　２（またはＩＰｓｅｃ　ＳＡ）の二段階に分けて行わる。ＩＰｓｅｃに関する特許文献としては、特許文献１がある。

【０００３】

アグレッシブモードの場合、Ｐｈａｓｅ　１では、１往復目でＩＫＥ通信路の暗号アルゴリズムを選び、２往復目でＤＨ（Ｄｉｆｆｅｅ－Ｈｅｌｌｍａｎ）鍵交換アルゴリズムにより鍵交換（ＩＫＥ通信用の鍵）を行い３往復目で通信相手の認証を行う。Ｐｈａｓｅ　２では、１往復目でＰｈａｓｅ　１で確立した秘密の通信路を使いセキュリティ・プロトコルＥＳＰあるいはＡＨで用いる暗号アルゴリズムや秘密鍵を交換し、以降の接続了承を送信のみとして送る。こうして交換された設定情報は、両端末機器のＳＡＤ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ　Ｄａｔａｂａｓｅ）のＳＡエントリとして登録され、相互のセキュアな通信で利用される。

【特許文献１】特開２００１－２９８４４９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

ＩＰｓｅｃ通信は、このように端末機器間で、自動でＳＡ確立が行えるように標準化されているが、端末機器には、双方のＩＰアドレス、アプリケーションのポート番号、セキュリティタイプ、セキュリティレベル等のセキュリティポリシーを、事前設定しておかなければならない。

【０００５】

本発明は、ＳＩＰプロトコルを用い、相手を呼び出す際に行うことにより、多数の通信相手毎のＳＰ設定という障害を排除する。

【課題を解決するための手段】

【０００６】

本発明は、第一の装置と第二の装置にセキュリティポリシーを設定する設定方法であって、第一の装置が、ＳＩＰサーバを介して第二の装置を呼び出すための接続呼出しメッセージを、第一の装置のセキュリティポリシー設定情報を添付して送信し、第二の装置は、受信した第一の装置のセキュリティポリシー設定情報に基づいて、第二の装置のセキュリティポリシーを設定し、接続応答メッセージを、第二の装置のセキュリティポリシー設定情報を添付して送信し、第一の装置は、受信した第二の装置のセキュリティポリシー設定情報に基づいて、第一の装置のセキュリティポリシーを設定することを特徴とする。

【発明の効果】

【０００７】

本発明により、多数の通信相手と相互に、セキュア通信を行うことが可能となる。

【発明を実施するための最良の形態】

【０００８】

以下、図面を参照しながら本発明に係る実施の形態を詳細に説明する。

【０００９】

図１は本発明の一実施形態のネットワーク構成図である。図１において１００はインターネットであり、ＩＰｖ６プロトコルを利用した通信が可能である。１０１はインターネット１００に直接または間接的に接続したプリンタであり、インターネット１００を介してＩＰｖ６プロトコルを用いた通信が可能である。１０２はインターネット１００に直接または間接的に接続したデジタルスチルカメラ（以降、デジカメと呼ぶ）であり、インターネット１００を介してＩＰｖ６プロトコルを用いた通信が可能である。本形態では、デジカメ（第一の装置）１０２とプリンタ（第二の装置）１０１にセキュリティポリシーを設定する。

【００１０】

１０３はインターネット１００に接続したＳＩＰサーバであり、プリンタ１０１とデジカメ１０２とのＩＰｖ６プロトコルを利用したピアツーピアな通信のためのセッションを確立する。つまり、プリンタ１０１とデジカメ１０２がピアツーピアに通信を行う際、Ｓ

ＩＰサーバ１０３に対して両機器がアドレス登録（ＳＩＰ　Ｒｅｇｉｓｔｅｒ）を行い、デジカメ１０２から接続呼出しメッセージであるセッション要求（ＳＩＰ　Ｉｎｖｉｔｅ）をプリンタ１０１にＳＩＰサーバ１０３を経由して送信することで、両機器はピアツーピア通信を行うためのセッション確立を行う。このセッション確立後に、両機器は所用のアプリケーションによるピアツーピア通信を行うことが可能となる。なお、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）は、ＲＦＣ２５４３で規定されている。

【００１１】

ＳＩＰサーバ１０３は、ロケーションデータベースを有する。ロケーションデータベースには、ＳＩＰ　ＵＲＩとＩＰｖ６アドレスが格納される。本形態では、このロケーションテーブルには、プリンタ１０１のＳＩＰ　ＵＲＩ（例えば、ＢＪ００１@ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ）とＩＰｖ６アドレス（例えば、２００１：３４０：：１）、デジカメ１０２のＳＩＰ　ＵＲＩ（例えば、ＤＣ@ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ）とＩＰｖ６アドレス（例えば、２００２：２００：１）が格納される。

【００１２】

以下、ＳＩＰサーバ１０３のロケーションデータベースにこれらの情報が登録される流れを簡単に説明する。ＳＩＰサーバ１０３は、「ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ」というドメインのＳＩＰサーバとしてレジストリサービス、ロケーションサービス、プロキシサービスを提供している。プリンタ１０１はインターネット１００に接続した際に自動的に設定されるＩＰｖ６アドレス（２００１：３４０：：１）を、自己のＩＤ（ＢＪ００１）と共にＳＩＰサーバ１０３に登録（ＳＩＰ　Ｒｅｇｉｓｔｅｒ）する。

【００１３】

登録要求を受けたＳＩＰサーバ１０３は、ＳＩＰで定義された認証を行い、プリンタ１０１の登録を受け付ける。この際、機器のＩＤ（ＢＪ００１）に、ＳＩＰサーバ１０３が管理しているドメイン（ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ）を「@」で繋げることで、その機器のＳＩＰ　ＵＲＩを作成する。また、ＩＰｖ６アドレス（２００１：３４０：：１）をプリンタ１０１からの登録要求メッセージ（ＳＩＰ　Ｒｅｇｉｓｔｅｒメッセージ）より抽出し、先に作成したＳＩＰ　ＵＲＩ（ＢＪ００１@ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ）と共にロケーションデータベースに格納する。

【００１４】

図２は、本実施形態でのプリンタ１０１及びデジカメ１０２の機能を実現するソフトウェアプログラムを動作させるためのハードウェア構成の一例を示したものである。なお、ＳＩＰサーバ１０３も、同様に構成可能である。

【００１５】

コンピュータ９００は、ＣＰＵ９０１と、ＲＯＭ９０２と、ＲＡＭ９０３と、ハードディスク（ＨＤ）９０７及びフロッピー（登録商標）ディスク（ＦＤ）９０８のディスクコントローラ（ＤＣ）９０５と、ネットワークインタフェースカード（ＮＩＣ）９０６とが、システムバス９０４を介して互いに通信可能に接続された構成としている。そして、システムバス９０４が、上記図１に示したインターネット１００とネットワークインタフェースカード９０６を介して接続される。

【００１６】

ＣＰＵ９０１は、ＲＯＭ９０２あるいはＨＤ９０７に記憶されたソフトウェア、あるいはＦＤ９０８より供給されるソフトウェアを実行することで、ステムバス９０４に接続された各構成部を統括的に制御する。すなわち、ＣＰＵ９０１は、以下に説明する処理シーケンスに従った処理プログラムを、ＲＯＭ９０２、あるいはＨＤ９０７、あるいはＦＤ９０８から読み出して実行することで、本実施形態での動作を実現するための制御を行う。ＲＡＭ９０３は、ＣＰＵ９０１の主メモリあるいはワークエリア等として機能する。ＤＣ９０５は、ブートプログラム、種々のアプリケーション、編集ファイル、ユーザファイル、ネットワーク管理プログラム、および本実施形態における上記処理プログラム等を記憶するＨＤ９０７、およびＦＤ９０８とのアクセスを制御する。ＮＩＣ９０６は、インター

ネット１００を通じてＩＰ通信プロトコルを用いた相互通信をする。ＮＩＣ９０６は、通信相手と（ＳＩＰを介して、又は、介さずに）データの送信／受信を行う手段である。ＣＰＵ９０１は、ＮＩＣ９０６により送信するデータを生成し、また、ＮＩＣ９０６により受信したデータを解釈する手段である。また、ＣＰＵ９０１は、自身のセキュリティポリシーの設定を行う。

【００１７】

図３は、デバイス機器に搭載したソフトウェア・モジュール構成図である。特に、デジカメ１０２のモジュール構成を示すが、プリンタ１０１も同様の構成でよい。

【００１８】

３０１はＳＩＰ通信モジュールであり、ＳＩＰサーバ１０３とＳＩＰメッセージのやり取りが行われる。３０２はメッセージ解析モジュールであり、ＳＩＰ通信モジュール３０１でやり取りされたＳＩＰメッセージの解析処理が行われる。３０３はＳＩＰ　ＵＡインタフェースであり、デジカメ１０２を利用しているユーザがプリンタ１０１とピアツーピア通信を行う際に、このＳＩＰ　ＵＡインタフェースを利用して、セッションの確立とアプリケーションの通信を開始する。３０４はＳＤＰネゴシエーションモジュールであり、ＳＩＰ　Ｉｎｖｉｔｅ処理においてピアツーピア通信を行うアプリケーション情報を記述した二つのＳＤＰ情報（自己ＳＤＰ情報と通信相手ＳＤＰ情報）のネゴシエーションを行う。３０５はＳＰ情報データベースであり、ＩＰｓｅｃで利用するセキュリティポリシーの設定項目を格納するデータベースである。なお、ＳＰ情報データベースに関する詳細は図４にて説明する。

【００１９】

３０６はＳＰ作成モジュールであり、前記ＳＰ情報データベース３０５に格納されたセキュリティポリシーの設定項目から、実際にセキュリティポリシーを設定するモジュールである。３０７は自己ＳＤＰ情報であり、このデバイス（デジカメ１０２）にてピアツーピア通信にて利用するアプリケーションの情報を格納する。ＳＰ情報ＤＢ３０５、自己ＳＤＰ情報３０７は、ＲＡＭ９０３上、又は、ＨＤ９０７上に設けられる。

【００２０】

３０８は（一つ、又は、複数の）上位アプリケーションであり、前記自己ＳＤＰ情報３０７にて記述された、デバイス間ピアツーピア通信にて利用されるアプリケーションである。

【００２１】

ＳＤＰネゴシエーションモジュール３０４は、ＳＩＰ　Ｉｎｖｉｔｅ処理においてＳＤＰ情報のネゴシエーションを行うが、ＳＩＰ　Ｉｎｖｉｔｅ関連メッセージに添付されるＳＤＰ情報３０７に関する詳細例は以下の通りである。なお、この例は、デジカメ１０２がＳＩＰ　Ｉｎｖｉｔｅメッセージに添付するデジカメ側のＳＤＰ情報３０７である。

【００２２】

ｖ＝０
ｏ＝ＤＣ１０１　１８６８５８７６１５　１１２１４４３８７０　ＩＮ　ＩＰ６　２００２：２００：：１
ｓ＝－
ｃ＝ＩＮ　ＩＰ６　２００２：２００：：１
ｔ＝０　０
ｍ＝ａｐｐｌｉｃａｔｉｏｎ　４６１２７　ＨＴＴＰ／ＴＣＰ
ｋ＝ＳＥＣ＿Ｌｅｖｅｌ　ｒｅｑｕｉｒｅ
ｋ＝ＳＥＣ＿Ｔｙｐｅ　ａｈ＆ｅｓｐ

【００２３】

重要な情報に関して説明する。二行目「ｏ＝」の「ＤＣ１０１」が機器ＩＤ、「２００２：２００：：１」がデジカメ１０２のＩＰアドレスである。同様に、「ｃ＝」にもＩＰアドレスが記述される。「ｍ＝」の「４６１２７」がアプリケーションのポート番号であり、「ＨＴＴＰ／ＴＣＰ」のプロトコルを利用する記載がある。そして、最後の２行の「

ｋ＝」にて、ＳＥＣ＿Ｌｅｖｅｌ（セキュリティレベル）、ＳＥＣ＿Ｔｙｐｅ（セキュリティタイプ）がそれぞれ記述される。セキュリティタイプには、ＩＰｓｅｃで利用するプロトコルタイプを登録する。指定できるタイプとしては、暗号化を行う「ｅｓｐ」、認証を行う「ａｈ」、暗号化と認証を両方利用する「ａｈ＆ｅｓｐ」がある。セキュリティレベルには、ＩＰｓｅｃの利用を必須とする「ｒｅｑｕｉｒｅ」、ＩＰｓｅｃの有効な設定があった場合には利用するが、ない場合にはＩＰｓｅｃを利用せずに通信を行う「ｕｓｅ」がある。このＳＤＰ情報３０７は、上位アプリケーション３０８が複数ある場合上位アプリケーション毎に、設けられる。

【００２４】

図４は前記ＳＰ情報データベース３０５の一例を示す。特に、前記デジカメ１０２から前記プリンタ１０１に対してピアツーピア通信を行う際のデジカメ１０２において作成されるＳＰ情報を示す。６０１はローカルアドレスであり、デジカメ１０２に割り当てられたＩＰアドレスを登録する。６０２はローカルポート番号であり、デジカメ１０２がピアツーピア通信の際に利用するアプリケーションのポート番号を登録する。６０３はリモートアドレスであり、通信相手であるプリンタ１０１のＩＰアドレスを登録する。６０４はリモートポート番号であり、通信相手であるプリンタ１０１がピアツーピア通信の際に利用するアプリケーションのポート番号を登録する。

【００２５】

６０５はセキュリティタイプであり、ＳＤＰ情報に付加されたセキュリティポリシーの項目の一つであり、ＩＰｓｅｃで利用するプロトコルタイプを登録する。指定できるタイプは、先に説明したように、暗号化を行う「ｅｓｐ」、認証を行う「ａｈ」、暗号化と認証を両方利用する「ａｈ＆ｅｓｐ」である。

【００２６】

６０６はセキュリティレベルであり、ＳＤＰ情報に付加されたセキュリティポリシーの項目の一つであり、ＩＰｓｅｃの利用レベルを登録する。指定できるレベルは、先に説明したように、ＩＰｓｅｃの利用を必須とする「ｒｅｑｕｉｒｅ」、ＩＰｓｅｃの有効な設定があった場合には利用するが、ない場合にはＩＰｓｅｃを利用せずに通信を行う「ｕｓｅ」である。

【００２７】

そして、デジカメ１０２にて実際に登録されたＳＰ情報のエントリが６１１である。このエントリから、デジカメ１０２のアドレスは「２００２：２００：：１」、デジカメ１０２で起動されるアプリケーションのポート番号は「４６１２７」、プリンタ１０１のアドレスは「２００１：３４０：：１」、プリンタ１０１で起動されるアプリケーションのポート番号は「８０」、両デバイスのセキュリティタイプは「ａｈ＆ｅｓｐ」、両デバイスのセキュリティレベルは「ｒｅｑｕｉｒｅ」であることがわかる。

【００２８】

図５は本実施形態のシーケンス図である。特に、前記デジカメ１０２から前記プリンタ１０１に対してピアツーピア通信を行う際の手順を示す。ここでは、デジカメ（第一の装置）１０２とプリンタ（第二の装置）１０１にセキュリティポリシーを設定する設定方法を示す。

【００２９】

４０１はデジカメ１０２にてプリンタ１０１とのピアツーピア通信を要求した際に動作する、ＳＩＰ　Ｉｎｖｉｔｅ処理とセキュリティポリシー設定処理を示す。デジカメ１０２のユーザは、ピアツーピア通信を行う相手となるプリンタ１０１と、そのピアツーピア通信にて利用するアプリケーションを、前記ＳＩＰ　ＵＡインタフェース３０３で指定することで、本処理が開始される。デジカメ１０２は、ユーザによるプリンタ１０１とのピアツーピア通信の要求により、４０２にてＳＤＰ情報（セキュリティポリシー設定情報）３０７を添付したＳＩＰ　Ｉｎｖｉｔｅメッセージ（接続呼出しメッセージ）を、ＳＩＰサーバ１０３を経由してプリンタ１０１に送信する。すなわち、デジカメ（第一の装置）１０２が、ＳＩＰサーバ１０３を介してプリンタ（第二の装置）１０１を呼び出すための

接続呼出しメッセージを、デジカメ（第一の装置）１０２のセキュリティポリシー設定情報を添付して送信する。

【００３０】

４０２のＳＩＰ Ｉｎｖｉｔｅメッセージを受信したプリンタ１０１は、４０３にてデジカメ１０２とのピアツーピア通信のコネクション確立のためのＳＩＰ Ｉｎｖｉｔｅ処理と、セキュリティポリシー設定処理を開始する。４０２のＳＩＰ Ｉｎｖｉｔｅメッセージを受信したプリンタ１０１は、添付されたデジカメ１０２のＳＤＰ情報３０７のチェックを行い、その結果より４０４にてプリンタ１０１のＳＤＰ情報（セキュリティポリシー設定情報）を添付した２００ＯＫメッセージを返信する。すなわち、プリンタ（第二の装置）１０１は、接続応答メッセージを、プリンタ（第二の装置）１０１のセキュリティポリシー設定情報を添付して送信する。２００ＯＫに添付するＳＤＰ情報については、あとで、詳細に説明する。４０４の２００ＯＫメッセージは、ＳＩＰサーバ１０３を経由してデジカメ１０２に到達する。

【００３１】

４０４の２００ＯＫメッセージを受信したデジカメ１０２は、メッセージの内容と、添付されたプリンタ１０１のＳＤＰ情報を確認し、４０５のＡｃｋメッセージを送信する。４０５のＡｃｋメッセージ送信後、自己ＳＤＰ情報と通信相手であるプリンタ１０１のＳＤＰ情報（セキュリティポリシー設定情報）から作成されたセキュリティポリシーの設定を４０６にて行う。すなわち、デジカメ（第一の装置）１０２は、受信したプリンタ（第二の装置）１０１のセキュリティポリシー設定情報に基づいて、デジカメ（第一の装置）１０２のセキュリティポリシーを設定する。

【００３２】

一方、４０５のＡｃｋメッセージを受信したプリンタ１０１でも、自己ＳＤＰ情報と通信相手であるデジカメ１０２のＳＤＰ情報から作成されたセキュリティポリシーの設定を４０７にて行う。すなわち、プリンタ（第二の装置）１０１は、受信したデジカメ（第一装置）１０２のセキュリティポリシー設定情報に基づいて、プリンタ（第二の装置）１０１のセキュリティポリシーを設定する。

【００３３】

図６は、実際に設定するセキュリティポリシーを生成する際に利用されるテンプレートである。なお、前記ＳＰ作成モジュール３０６は、前記ＳＰ情報データベース３０５に格納されたセキュリティポリシーの設定項目（ＳＰ情報）から、このテンプレートを利用して、実際に設定するセキュリティポリシーを生成する。＜ｌｏｃａｌ＿ａｄｄｒ＞はローカルアドレスであり、前記６０１の値が設定される。＜ｌｏｃａｌ＿ｐｏｒｔ＞はローカルアドレスであり、前記６０２の値が設定される。＜ｒｅｍｏｔｅ＿ａｄｄｒ＞はリモートアドレスであり、前記６０３の値が設定される。＜ｒｅｍｏｔｅ＿ｐｏｒｔ＞はリモートポートであり、前記６０４の値が設定される。＜ｓｅｃ＿ｔｙｐｅ＞はセキュリティタイプであり、前記６０５の値が設定され、＜ｓｅｃ＿ｌｅｖｅｌ＞はセキュリティレベルであり、前記６０６の値が設定される。なお、ｓｅｃ＿ｔｙｐｅに「ａｈ＆ｅｓｐ」を指定されている場合（つまり、認証と暗号化を両方利用する場合）、「＜ｓｅｃ＿ｔｙｐｅ＞／ｔｒａｎｓｐｏｒｔ／／＜ｓｅｃ＿ｌｅｖｅｌ＞」を繰り返し設定する。つまり、「～ａｈ／ｔｒａｎｓｐｏｒｔ／／ｒｅｑｕｉｒｅ ｅｓｐ／ｔｒａｎｓｐｏｒｔ／／ｒｅｑｕｉｒｅ ～」のように記述される。

【００３４】

図７、図８では本実施形態の処理フローを示す。特に、ＳＩＰ Ｉｎｖｉｔｅ処理とセキュリティポリシーの設定処理（デジカメ（第一の装置）１０２とプリンタ（第二の装置）１０１にセキュリティポリシーを設定する設定処理）に関して示す。

【００３５】

図７の５０１にてユーザからのピアツーピア通信の要求が入力されたか判定する。つまり、デジカメ１０２においてユーザが、ピアツーピア通信を行う相手となるプリンタ１０１と、そのピアツーピア通信にて利用するアプリケーションを、前記ＳＩＰ ＵＡインタ

フェース３０２で指定した場合、５０３へ処理が進み、ユーザからの要求がない場合には５０２に処理が進む。５０２では、ＳＩＰ Ｉｎｖｉｔｅメッセージを受信したかを判定する。つまり、プリンタ１０１において前記４０２のＳＩＰ Ｉｎｖｉｔｅメッセージを受信した場合には５１２へ処理が進み、受信しなかった場合には処理が終了となり、もう一度５０１からの処理が始まる。この５０１、５０２の判定処理は、デバイス間ピアツーピア通信におけるアクセス側の端末における処理と、被アクセス側の端末における処理を判定している。

【００３６】

アクセス側の端末処理は５０３より行われる。５０１、及び、５０３から５１１は、アクセス側であるデジカメ１０２のＣＰＵ９０１が実行するプログラムを示す。５０３では、前記５０１にて受理したユーザからの要求内容から、前記自己ＳＤＰ情報３０７より該当するアプリケーション情報が含まれている自己ＳＤＰ情報を取得し、自己のアドレスとポート番号を前記ＳＰ情報データベース３０５に登録する。５０４では、前記５０３で取得した自己ＳＤＰ情報（セキュリティポリシー設定情報）を、ＳＩＰ Ｉｎｖｉｔｅメッセージに添付する。そして、５０５にてＳＩＰ Ｉｎｖｉｔｅメッセージ（接続呼出しメッセージ）を前記ＳＩＰサーバ１０３に対して送信する。すなわち、デジカメ（第一の装置）１０２が、ＳＩＰサーバ１０３を介してプリンタ（第二の装置）１０１を呼び出すための接続呼出しメッセージを、デジカメ（第一の装置）１０２のセキュリティポリシー設定情報を添付して送信する。このとき、ＳＩＰ Ｉｎｖｉｔｅメッセージの宛先としては、ピアツーピア通信を行う相手のＳＩＰ ＵＲＩを指定する。つまり、デジカメ１０２からプリンタ１０１へのピアツーピア通信の要求の場合、プリンタ１０１のＳＩＰ ＵＲＩ「ＢＪ００１@ｄｅｖｉｃｅ．ｏａｎｏｎ．ｃｏｍ」に対して送信される。

【００３７】

５０６では、前記５０５のＳＩＰ Ｉｎｖｉｔｅメッセージに対する返信メッセージである２００ＯＫメッセージを受信する。この２００ＯＫメッセージにはピアツーピア通信の相手となるデバイス機器のＳＤＰ情報（セキュリティポリシー設定情報）が添付されており、５０７にてその添付されている通信相手ＳＤＰ情報（セキュリティポリシー設定情報）を取得する。すなわち、通信相手のセキュリティポリシー設定情報を受信する。取得した通信相手ＳＤＰ情報から５０８にて、セキュリティポリシーの設定に関する項目（ＳＥＣ＊項目）が有効な値であるかどうかを判定する。有効な値とは、ＳＩＰ Ｉｎｖｉｔｅメッセージに添付した自己ＳＤＰ情報のセキュリティポリシーの項目と、２００ＯＫメッセージに添付された通信相手ＳＤＰ情報のセキュリティポリシーの項目が、同一の値であることである。ここで有効な値の場合は５０９に処理が進み、有効でない場合には５１１に処理が進む。

【００３８】

５０９では、通信相手ＳＤＰ情報（セキュリティポリシー設定情報）より、前記５０８にてチャックしたセキュリティポリシーの項目と、通信相手のアドレスとポート番号の各情報を、前記５０３にて登録したＳＰ情報データベース３０５に追加登録する。この５０３、５０９の各ＳＰ情報の登録処理により、ＳＰ情報のエントリが完成するので、５１０にて完成したＳＰ情報から実際にデバイスに設定するセキュリティポリシーを作成し、カーネルに設定する。すなわち、デジカメ（第一の装置）１０２は、受信したプリンタ（第二の装置）１０１のセキュリティポリシー設定情報に基づいて、デジカメ（第一の装置）１０２のセキュリティポリシーを設定する。５１１ではＳＩＰ Ｉｎｖｉｔｅ処理の最後に送信するＡｃｋメッセージを、通信相手のデバイスに送信し、処理を終了する。

【００３９】

一方、被アクセス側の端末処理は５１２より行われる。５０２、及び、５１２から５２４は、アクセス側であるデジカメ１０２のＣＰＵ９０１が実行するプログラムを示す。５１２にてピアツーピア通信を要求するデバイスからのＳＩＰ Ｉｎｖｉｔｅメッセージ（接続呼出しメッセージ）を受信すると、５１３にて前記５１２のＳＩＰ Ｉｎｖｉｔｅメッセージに添付された通信相手ＳＤＰ情報（セキュリティポリシー設定情報）３０７を取

得する。すなわち、通信相手のセキュリティポリシー設定情報の添付された接続呼出しメッセージを、ＳＩＰサーバを介して受信する。

【００４０】

取得した通信相手ＳＤＰ情報３０７よりセキュリティポリシーの項目（セキュリティタイプ、レベル）を図８の５１４にてチェックし、値が設定されている場合には５１５に処理が進み、値がない場合には５１９に処理が進む。セキュリティポリシーの項目がある場合、５１５にて自己ＳＤＰ情報のセキュリティポリシーの項目と比較を行い、５１６にてそれらの値がすべて同一かどうかを判定する。すべてのセキュリティポリシーの項目が同一の場合には５１７に処理が進み、そうでない場合には５１９に処理が進む。

【００４１】

通信相手ＳＤＰ情報のセキュリティポリシーの項目（セキュリティタイプ、レベル）と、自己ＳＤＰ情報のセキュリティポリシーの項目とが一致した場合、５１７にて自己ＳＤＰ情報をそのまま取得する。そして、５１８にて通信相手ＳＤＰ情報と自己ＳＤＰ情報より、ＳＰ情報データベース３０５にＳＰ情報を登録する。具体的には、両ＳＤＰ情報から共通のセキュリティポリシーの項目と、通信相手ＳＤＰ情報（セキュリティポリシー設定情報）よりアドレスとポート番号、自己ＳＤＰ情報よりアドレスとポート番号をそれぞれ取得し、ＳＰ情報データベース３０５に登録する。すなわち、プリンタ（第二の装置）１０１は、受信したデジカメ（第一の装置）１０２のセキュリティポリシー設定情報に基づいて、プリンタ（第二の装置）１０１のセキュリティポリシーを、ＳＰ情報データベース３０５に登録する。そして、５２０へ処理が進む。

【００４２】

一方、通信相手ＳＤＰ情報のセキュリティポリシーの項目（セキュリティタイプ、レベル）と、自己ＳＤＰ情報のセキュリティポリシーの項目が一致しなかった場合、５１９にて自己ＳＤＰ情報のセキュリティポリシーの項目を空欄に変更する。

【００４３】

５２０では、前記５１７または５１９にて取得・修正した自己ＳＤＰ情報（セキュリティポリシー設定情報）を、２００ＯＫメッセージ（接続応答メッセージ）に添付し、５２１にて２００ＯＫメッセージを送信する。すなわち、プリンタ（第二の装置）１０１は、受信したデジカメ（第一の装置）１０２のセキュリティポリシー設定情報に基づいて、接続応答メッセージを、プリンタ（第二の装置）１０１のセキュリティポリシー設定情報を添付して送信する。

【００４４】

５２２にてＡｃｋメッセージを受信すると、５２３にて５１８でＳＰ情報が作成されたかどうかを判定する。ＳＰ情報が作成されている場合には５２４に処理が進み、ＳＰ情報が作成されていない場合には処理を終了する。５２４では作成されたＳＰ情報から実際にデバイスに設定するセキュリティポリシーを作成し、カーネルに設定し、処理を終了する。すなわち、プリンタ（第二の装置）１０１は、受信したデジカメ（第一の装置）１０２のセキュリティポリシー設定情報に基づいて、プリンタ（第二の装置）１０１のセキュリティポリシーを設定する。

【図面の簡単な説明】

【００４５】

【図１】本発明の一実施形態のネットワーク構成図である。

【図２】本実施形態のハードウェア構成図である。

【図３】本実施形態のモジュール構成図である。

【図４】ＳＰ情報データベースの構成図である。

【図５】本実施形態のシーケンス図である。

【図６】セキュリティポリシーを生成する際に利用されるテンプレートの図である。

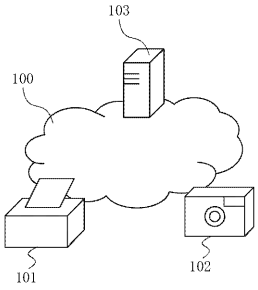
【図７】本実施形態の処理フロー図である。

【図８】本実施形態の処理フロー図である。

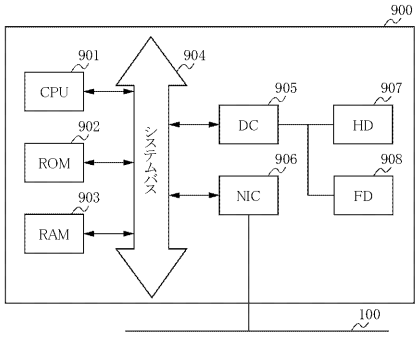
【符号の説明】

【００４６】
１０１　プリンタ
１０２　デジタルカメラ（デジカメ）
１０３　ＳＩＰサーバ

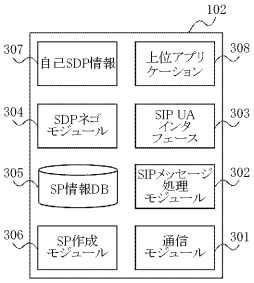
【図１】



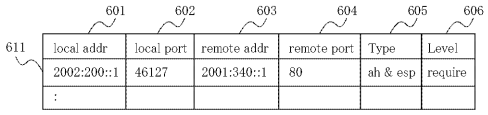
【図２】



【図３】

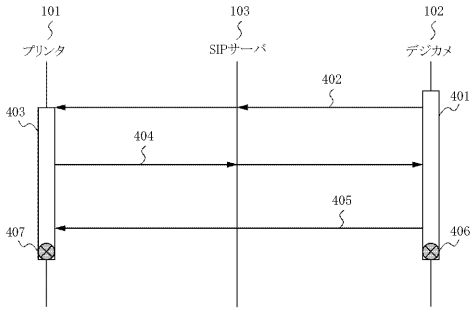


【図４】



611	601 local addr	602 local port	603 remote addr	604 remote port	605 Type	606 Level
	2002:200::1	46127	2001:340::1	80	ah & esp	require
	:					

【図５】

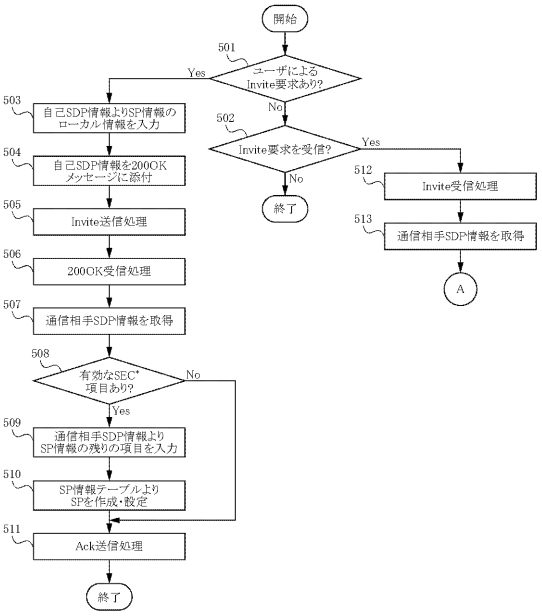


【図６】

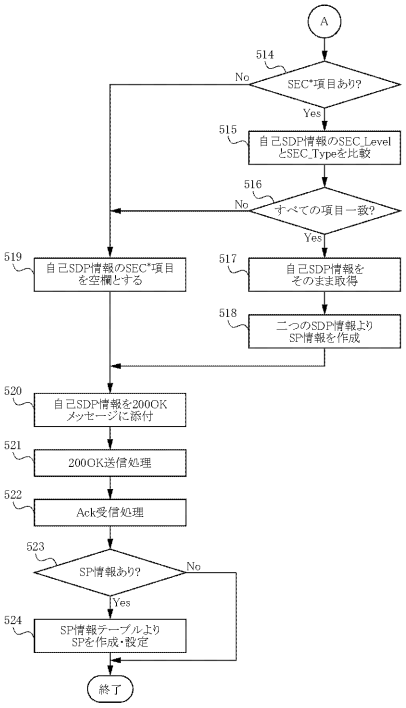
```
spdadd<local_addr>[<local_port>]<remote_addr>[<remote_port>]any-P out ipsec
<sec_type>/transport//<sec_level>...;

spdadd<remote_addr>[<remote_port>]<local_addr>[local_port>]any-P in ipsec
<sec_type>/transport//<sec_level>...;
```

【図７】


開始
501
ユーザによる
Invite要求あり?
Yes
No
503
自己SDP情報よりSP情報の
ローカル情報を入力
504
自己SDP情報を200OK
メッセージに添付
505
Invite送信処理
506
200OK受信処理
507
通信相手SDP情報を取得
508
有効なSEC*
項目あり?
No
Yes
509
通信相手SDP情報より
SP情報の残りの項目を入力
510
SP情報テーブルより
SPを作成・設定
511
Ack送信処理
終了
502
Invite要求を受信?
Yes
No
終了
512
Invite受信処理
513
通信相手SDP情報を取得
A

【図８】


A
514
SEC*項目あり?
No
Yes
515
自己SDP情報のSEC_Level
とSEC_Typeを比較
516
すべての項目一致?
No
Yes
519
自己SDP情報のSEC*項目
を空欄とする
517
自己SDP情報を
そのまま取得
518
二つのSDP情報より
SP情報を作成
520
自己SDP情報を200OK
メッセージに添付
521
200OK送信処理
522
Ack受信処理
523
SP情報あり?
No
Yes
524
SP情報テーブルより
SPを作成・設定
終了

フロントページの続き

(72)発明者　中澤　宏昭
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

Ｆターム(参考) 5J104 AA01 AA07 AA16 EA04 EA15 EA16 JA03 KA02 KA04 NA02
NA37 NA38 PA07
5K030 GA15 HA08 LA08 LB02
5K101 KK20 LL02 NN14 RR11