(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3944182号
(P3944182)
(45)発行日　平成19年7月11日(2007.7.11)　(24)登録日　平成19年4月13日(2007.4.13)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28 200Z

請求項の数 5　(全 23 頁)

(21)出願番号　特願2004-104635(P2004-104635)
(22)出願日　平成16年3月31日(2004.3.31)
(65)公開番号　特開2005-295038(P2005-295038A)
(43)公開日　平成17年10月20日(2005.10.20)
審査請求日　平成17年2月16日(2005.2.16)

(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　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】セキュリティ通信方法

(57)【特許請求の範囲】
【請求項１】
提供装置が、セキュリティ通信を行うためのパラメータの候補を第１の装置及び第２の装置から受信し、前記第１の装置及び第２の装置から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成し、
前記第１の装置及び第２の装置が、前記生成されたセキュリティ通信を行うために必要な情報を元に、前記第１の通信装置と前記第２の通信装置との間の通信にセキュリティを確保するセキュリティ通信方法であって、
前記第１の装置が、セッションの確立を要求するセッション確立要求メッセージを前記提供装置経由で前記第２の装置に送信し、
前記第２の装置が、前記セッション確立要求メッセージの返信メッセージを前記提供装置経由で前記第１の装置に送信し、
前記第１の装置が、前記返信メッセージを受理した旨を通知する通知メッセージを前記第２の装置に送信し、セキュリティ通信を要求するための第１のセキュリティ通信要求メッセージを前記提供装置に送信し、
前記第２の装置が、前記通知メッセージを受信すると、セキュリティ通信を要求するための第２のセキュリティ通信要求メッセージを前記提供装置に送信し、
前記提供装置が、前記第１のセキュリティ通信要求メッセージ及び前記第２のセキュリティ通信要求メッセージを受信すると、前記セキュリティ通信を行うために必要な情報を前記第１の装置及び第２の装置に提供することを特徴とするセキュリティ通信方法。

【請求項２】
提供装置が、第１の装置と第２の装置との間のセッションを識別する識別情報、及び、セキュリティを確保するためのパラメータの候補を前記第１の装置及び第２の装置から受信し、前記第１の装置及び第２の装置から受信したパラメータの候補に基づいて、通信のセキュリティを確保するために必要な情報を生成し、
前記第１の装置及び第２の装置が、前記生成された、通信のセキュリティを確保するために必要な情報を元に、前記第１の通信装置と第２の通信装置との間の通信にセキュリティを確保するセキュリティ通信方法であって、
前記第１の装置が、セッションの確立を要求するセッション確立要求メッセージを前記提供装置経由で前記第２の装置に送信し、
前記第２の装置が、前記セッション確立要求メッセージの返信メッセージを前記提供装置経由で前記第１の装置に送信し、
前記第１の装置が、前記返信メッセージを受理した旨を通知する通知メッセージを前記第２の装置に送信し、セキュリティ通信を要求するための第１のセキュリティ通信要求メッセージを前記提供装置に送信し、
前記第２の装置が、前記通知メッセージを受信すると、セキュリティ通信を要求するための第２のセキュリティ通信要求メッセージを前記提供装置に送信し、
前記提供装置が、前記第１のセキュリティ通信要求メッセージ及び前記第２のセキュリティ通信要求メッセージを受信すると、前記通信のセキュリティを確保するために必要な情報を前記第１の装置及び第２の装置に提供することを特徴とするセキュリティ通信方法。
【請求項３】
前記パラメータの候補は、認証アルゴリズム又は暗号化アルゴリズムの候補であることを特徴とする請求項２のセキュリティ通信方法。
【請求項４】
前記必要な情報は、認証アルゴリズム又は暗号化アルゴリズムであることを特徴とする請求項１又は２のセキュリティ通信方法。
【請求項５】
前記必要な情報は、セキュリティを確保するための鍵であることを特徴とする請求項１又は２のセキュリティ通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティ通信方法に関する。
【背景技術】
【０００２】
ＩＰｓｅｃは、一般的なＩＰレイヤでのセキュリティを実現するための十分な機能と安全性を備えた、標準化された技術である。ＩＰｓｅｃの中核は、ＲＦＣ２４０９“Ｔｈｅ Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ（ＩＫＥ）”で規定されたＩＫＥプロトコルによるＳＡ（Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ）の自動生成であり、ＳＡ確立は、Ｐｈａｓｅ１（またはＩＳＡＫＭＰ ＳＡ）、Ｐｈａｓｅ２（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、Ｐｈａｓｅ１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。Ｐｈａｓｅ２では、１往復目でＰｈａｓｅ１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（Ｓｅｃｕｒｉｔ

ｙ 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。

【０００４】

ＩＰｓｅｃ通信は、このように端末機器間で自動設定できるように標準化されているが、このためにはいくつかの事前設定が必須である。

【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】

【０００５】

Ｐｈａｓｅ１の３往復目で実施される認証は、Ｐｒｅ－Ｓｈａｒｅｄ Ｋｅｙ方式による認証が一般的に支持されている。Ｐｒｅ－Ｓｈａｒｅｄ Ｋｅｙ方式はセキュリティ通信を行う２者の端末機器間のみで有効な、つまり、他者に知られないように秘匿しなければならない共通鍵を、技術を持った管理者が対象機器に対し直接設定する事を前提としている。このため、特定少数機器間では運用可能であるが、不特定多数の機器間でＰｒｅ－Ｓｈａｒｅｄ Ｋｅｙを設定する際の運用上の困難さが指摘されている。

【０００６】

また、ＩＰｓｅｃで利用する、ＤＨ鍵交換アルゴリズム、公開鍵暗号アルゴリズム等は処理が重く、ＣＰＵパワーの比較的低い移動体端末等でＩＰｓｅｃを処理した場合に、数秒以上の時間がかかるため、実用的には専用演算チップを必要とするなど、実装面での問題が指摘されている。

【０００７】

本発明は、セキュリティを確保するための処理を軽減することを目的とする。

【課題を解決するための手段】

【０００８】

本発明のセキュリティ通信方法は、提供装置が、セキュリティ通信を行うためのパラメータの候補を第１の装置及び第２の装置から受信し、前記第１の装置及び第２の装置から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成し、前記第１の装置及び第２の装置が、前記生成されたセキュリティ通信を行うために必要な情報を元に、前記第１の通信装置と前記第２の通信装置との間の通信にセキュリティを確保するセキュリティ通信方法であって、前記第１の装置が、セッションの確立を要求するセッション確立要求メッセージを前記提供装置経由で前記第２の装置に送信し、前記第２の装置が、前記セッション確立要求メッセージの返信メッセージを前記提供装置経由で前記第１の装置に送信し、前記第１の装置が、前記返信メッセージを受理した旨を通知する通知メッセージを前記第２の装置に送信し、セキュリティ通信を要求するための第１のセキュリティ通信要求メッセージを前記提供装置に送信し、前記第２の装置が、前記通知メッセージを受信すると、セキュリティ通信を要求するための第２のセキュリティ通信要求メッセージを前記提供装置に送信し、前記提供装置が、前記第１のセキュリティ通信要求メッセージ及び前記第２のセキュリティ通信要求メッセージを受信すると、前記セキュリティ通信を行うために必要な情報を前記第１の装置及び第２の装置に提供することを特徴とする。

【０００９】

また、本発明のセキュリティ通信方法は、提供装置が、第１の装置と第２の装置との間のセッションを識別する識別情報、及び、セキュリティを確保するためのパラメータの候補を前記第１の装置及び第２の装置から受信し、前記第１の装置及び第２の装置から受信したパラメータの候補に基づいて、通信のセキュリティを確保するために必要な情報を生成し、前記第１の装置及び第２の装置が、前記生成された、通信のセキュリティを確保するために必要な情報を元に、前記第１の通信装置と第２の通信装置との間の通信にセキュリティを確保するセキュリティ通信方法であって、前記第１の装置が、セッションの確立を要求するセッション確立要求メッセージを前記提供装置経由で前記第２の装置に送信し、前記第２の装置が、前記セッション確立要求メッセージの返信メッセージを前記提供装

置経由で前記第１の装置に送信し、前記第１の装置が、前記返信メッセージを受理した旨を通知する通知メッセージを前記第２の装置に送信し、セキュリティ通信を要求するための第１のセキュリティ通信要求メッセージを前記提供装置に送信し、前記第２の装置が、前記通知メッセージを受信すると、セキュリティ通信を要求するための第２のセキュリティ通信要求メッセージを前記提供装置に送信し、前記提供装置が、前記第１のセキュリティ通信要求メッセージ及び前記第２のセキュリティ通信要求メッセージを受信すると、前記通信のセキュリティを確保するために必要な情報を前記第１の装置及び第２の装置に提供する。

【発明の効果】

【００１０】

従って、本発明によれば、セッションを確立して、通信を開始する時から、複雑な処理を行うことなく、セキュリティを確保することができる。

【発明を実施するための最良の形態】

【００１１】

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。

【００１２】

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。

【００１３】

１０３はインターネット１００に接続したセキュリティ管理サーバであり、プリンタ１０１やデジカメ１０２の、インターネット１００を介したピアツーピア通信におけるセキュリティを管理するサーバである。セキュリティ管理サーバ１０３は、両機器の詳細情報を保持しており、両機器とのインターネット１００を介した通信は既にセキュリティを確保されている。つまり、セキュリティ管理サーバ１０３とプリンタ１０１には、共通な認証鍵・暗号鍵が、外部に情報が漏洩しないように仕込まれており、この認証鍵・暗号鍵の情報を元に、セキュリティ管理サーバ１０３とプリンタ１０１がお互いに通信に関する認証と通信内容の暗号化が行える。

【００１４】

プリンタ１０１とデジカメ１０２は、ＩＰｖ６プロトコルを利用したピアツーピアな通信が可能である。両機器によるセキュリティ管理サーバ１０３に対するアドレス登録（ＳＩＰ　Ｒｅｇｉｓｔｅｒ）は行われている。この状態で、デジカメ１０２からセッション要求（ＳＩＰ　Ｉｎｖｉｔｅ）をプリンタ１０１に送信することで、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。すなわち、本形態では、セキュリティ管理サーバ１０３は、ＳＩＰサーバを兼ねる。なお、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）は、ＲＦＣ２５４３で規定されている。

【００１５】

図１のネットワーク構成における、各機器、サーバのネットワーク情報は、以下のとおりである。

【００１６】

すなわち、例えば、プリンタ１０１、デジカメ１０２の機器ＩＤは、ＢＪ００１、ＤＣ１０１であり、この機器ＩＤは、セキュリティ管理サーバ１０３内で機器の識別子として利用される。なお、この機器ＩＤは、機器同士のピアツーピア通信を行う際にやり取りされるＳＩＰ通信にも、ＳＩＰ　ＵＲＩとして利用される。また、プリンタ１０１、デジカメ１０２、セキュリティ管理サーバ１０３のＩＰｖ６アドレスは、３ｆｆｅ：５１４：：

１、２００２：２００：：１、２００１：３４０：：１である。プリンタ１０１、デジカメ１０２の機器ＩＤ、ＩＰｖ６アドレスは、セキュリティ管理サーバ１０３に登録されている。

【００１７】

セキュリティ管理サーバ１０３は、デジカメ１０２とプリンタ１０１がセッション（通信）を確立するための仲介を行う装置であり、デジカメ１０２からのセッション要求に含まれるプリンタ１０１の機器ＩＤ（識別子）をプリンタ１０１のＩＰアドレスに変換する。デジカメ１０２とプリンタ１０１の間のセッションは、このＩＰアドレスを元に確立される。

【００１８】

セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であって、セキュリティ通信を行うためのパラメータの候補を、デジカメ１０２及びプリンタ１０１から受信し、デジカメ１０２及びプリンタ１０１から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成し、前記生成されたセキュリティ通信を行うために必要な情報を、デジカメ１０２及びプリンタ１０１に送信する。

【００１９】

セキュリティ管理サーバ１０３は、デジカメ１０２とプリンタ１０１間の通信を識別する識別情報を、デジカメ１０２及びプリンタ１０１から受信し、生成されたセキュリティ通信を行うために必要な情報を、識別情報により識別される通信のセキュリティを確保するために、デジカメ１０２及びプリンタ１０１に送信する。

【００２０】

プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ１０３（提供装置）から受け取る通信装置であって、セキュリティを確保するためのパラメータの候補を、セキュリティ管理サーバ１０３に送信し、セキュリティを確保するために必要な情報を、セキュリティ管理サーバ１０３から受信し、セキュリティ管理サーバ１０３から受信した情報を元に、通信相手との通信にセキュリティを確保する。

【００２１】

プリンタ１０１、デジカメ１０２は、通信相手との間で確立された通信を識別する識別情報を、セキュリティ管理サーバ１０３に送信し、セキュリティ管理サーバ１０３から受信した情報を元に、通信相手との間で確立された通信にセキュリティを確保する。

【００２２】

セキュリティ通信を行うためのパラメータの候補は、例えば、セキュリティを確保するための認証アルゴリズムと暗号化アルゴリズムの少なくとも一方もしくは両方の候補である。

【００２３】

また、セキュリティを確保するために必要な情報は、セキュリティを確保するための認証アルゴリズム及び暗号化アルゴリズムの少なくとも一方もしくは両方、あるいは、セキュリティを確保するための鍵である。

【００２４】

図２は、本実施形態で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。ここでは、セキュリティ管理サーバ１０３をコンピュータ１５００により構成した場合の例を示すが、プリント部、撮像部を追加することにより、プリンタ１０１、デジカメ１０２も、同様に、構成できる。

【００２５】

コンピュータ１５００は、ＣＰＵ１５０１と、ＲＯＭ１５０２と、ＲＡＭ１５０３と、ハードディスク（ＨＤ）１５０７及びフロッピー（登録商標）ディスク（ＦＤ）１５０８のディスクコントローラ（ＤＣ）１５０５と、ネットワークインタフェースカード（ＮＩＣ）１５０６とが、システムバス１５０４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１５０４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１５０６を介して接続される。

【００２６】

ＣＰＵ１５０１は、ＲＯＭ１５０２あるいはＨＤ１５０７に記憶されたソフトウェア、あるいはＦＤ１５０８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１５０４に接続された各構成部を統括的に制御する。すなわち、ＣＰＵ１５０１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、ＲＯＭ１５０２、あるいはＨＤ１５０７、あるいはＦＤ１５０８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。ＲＡＭ１５０３は、ＣＰＵ１５０１の主メモリあるいはワークエリア等として機能する。ＤＣ１５０５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ＨＤ１５０７、およびＦＤ１５０８とのアクセスを制御する。ＮＩＣ１５０６は、インターネット１００を通じてＩＰｖ６通信プロトコルを用いた相互通信をする。

【００２７】

セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であるセキュリティ管理サーバ１０３は、セキュリティ通信を行うためのパラメータの候補を、デジカメ１０２及びプリンタ１０１から受信するＮＩＣ１５０６と、デジカメ１０２及びプリンタ１０１から受信したパラメータの候補に基づいて、セキュリティ通信を行うために必要な情報を生成するＣＰＵ１５０１とを有する。また、ＮＩＣ１５０６は、生成されたセキュリティ通信を行うために必要な情報を、デジカメ１０２及びプリンタ１０１に送信する送信手段である。ＮＩＣ１５０６は、デジカメ１０２がプリンタ１０１とのセッションの確立を要求するセッション要求メッセージ（Ｉｎｖｉｔｅ要求メッセージ）を受信し、ＣＰＵ１５０１は、セッション要求メッセージに含まれるプリンタ１０１の機器ＩＤ（識別子）をプリンタ１０１のＩＰアドレスに変換し、デジカメ１０２とプリンタ１０２の間のセッション（通信）が確立されるのを仲介する。

【００２８】

更に、セキュリティ管理サーバ１０３のＮＩＣ１５０６は、デジカメ１０２とプリンタ１０１間の通信を識別する識別情報を、デジカメ１０２及びプリンタ１０１から受信し、生成されたセキュリティ通信を行うために必要な情報を、識別情報により識別される通信のセキュリティを確保するために、デジカメ１０２及びプリンタ１０１に送信する。

【００２９】

プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ（提供装置）１０３から受け取る通信装置であって、セキュリティを確保するためのパラメータの候補を、セキュリティ管理サーバ１０３に送信し、セキュリティを確保するために必要な情報を、提供装置から受信するＮＩＣ１５０６と、ＮＩＣ１５０６によりセキュリティ管理サーバ１０３から受信した情報を元に、通信相手との通信にセキュリティを確保するＣＰＵ１５０１とを有する。

【００３０】

プリンタ１０１、デジカメ１０２のＮＩＣ１５０６は、通信相手との間で確立された通信を識別する識別情報を、セキュリティ管理サーバ１０３に送信し、ＣＰＵ１５０１は、セキュリティ管理サーバ１０３から受信した情報を元に、通信相手との間で確立された通信にセキュリティを確保する。デジカメ１０２のＮＩＣ１５０６は、プリンタ１０１との間のセッション（通信）の確立を要求する要求メッセージ（Ｉｎｖｉｔｅ要求メッセージ）を、セキュリティ管理サーバ１０３に送信する。

【００３１】

セキュリティ通信を行うためのパラメータの候補は、例えば、セキュリティを確保するための認証アルゴリズムと暗号化アルゴリズムの少なくとも一方もしくは両方の候補である。

【００３２】
また、セキュリティを確保するために必要な情報は、セキュリティを確保するための認証アルゴリズム及び暗号化アルゴリズムの少なくとも一方もしくは両方、あるいは、セキュリティを確保するための鍵である。
【００３３】
図３は、プリンタ１０１とセキュリティ管理サーバ１０３のモジュール構成図である。３０１～３０５はセキュリティ管理サーバ１０３内に搭載されたモジュールであり、３１１～３１６はプリンタ１０１内に搭載されたモジュールである。なお、デジカメ１０２も、プリンタ１０１と同様のモジュール構成を有する。
【００３４】
３０１は通信モジュールであり、ネットワークインタフェースカード１５０６を介したプリンタ１０１とＩＰｓｅｃ要求メッセージの受信やＩＰｓｅｃ設定内容の送信に利用される。３０２はプリンタ１０１からのＩＰｓｅｃ要求メッセージを受け付ける、要求受付モジュールである。３０３はＩＰｓｅｃ作成テーブルであり、要求受付モジュール３０２でＩＰｓｅｃ要求メッセージからから得られた各機器間のセッション情報と、機器のＩＰｓｅｃ関連情報を管理・格納される。なお、ＩＰｓｅｃ作成テーブルに関しては、図５にて詳細を説明する。３０４は暗号通信モジュールであり、プリンタ１０１と事前に確保されたセキュアな通信路を利用したメッセージのやり取りが行われる。３０５はＩＰｓｅｃ設定モジュールであり、ＩＰｓｅｃ作成テーブル３０３の情報から、プリンタ１０１にて利用するＩＰｓｅｃ設定内容の作成処理が行われる。
【００３５】
３１１は通信モジュールであり、ネットワークインタフェースカード１５０６を介したセキュリティ管理サーバ１０３とＩＰｓｅｃ要求メッセージの受信やＩＰｓｅｃ設定内容の送信に利用される。このモジュールは通信モジュール３０１と同等のモジュールである。３１２はＩＰｓｅｃ要求メッセージを作成する要求発行モジュールである。このモジュールによりＩＰｓｅｃ要求が発行され、セキュリティ管理サーバ１０３よりＩＰｓｅｃ設定内容を取得する。
【００３６】
３１３は暗号通信モジュールであり、セキュリティ管理サーバ１０３と事前に確保されたセキュアな通信路を利用したメッセージのやり取りが行われる。このモジュールは暗号通信モジュール３０４と同等のモジュールである。セキュリティ管理サーバ１０３の暗号通信モジュール３０４とデジカメ１０２の暗号通信モジュール３１３は、それぞれ所有する第一の秘密対称鍵を使って形成された暗号通信路を使って通信する。また、セキュリティ管理サーバ１０３の暗号通信モジュール３０４とプリンタ１０１の暗号通信モジュール３１３は、それぞれ所有する第二の秘密対称鍵を使って形成された暗号通信路を使って通信する。
【００３７】
３１４はＩＰｓｅｃ設定モジュールであり、ＩＰｓｅｃ設定モジュール３０５にて作成されたＩＰｓｅｃ設定内容をプリンタ１０１に設定するモジュールである。
【００３８】
３１５はＳＩＰモジュールであり、プリンタ１０１とデジカメ１０２がピアツーピアな通信を行う際に、ＳＩＰを利用してピアツーピア通信用のセッションを確立する際に利用される。つまり、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（３ｆｆｅ：５１４：：１）を自己の機器ＩＤ（ＢＪ１０１）と共にセキュリティ管理サーバ１０３に登録する。これにより、プリンタ１０１のＳＩＰ ＵＲＩ（例えば、ＢＪ１０１@ｄｅｖｉｃｅ．ｃｃｃ．ｃｏｍ）と、そのＩＰｖ６アドレスがセキュリティ管理サーバ１０３にて管理される。同様に、デジカメ１０２もセキュリティ管理サーバ１０３へＳＩＰ ＵＲＩとそのＩＰｖ６アドレスを登録する。登録されたプリンタ１０１のＳＩＰ ＵＲＩを用いて、デジカメ１０２がセッション要求メッセージ（ＳＩＰ Ｉｎｖｉｔｅ）をセキュリティ管理サーバ１０３経由でプリンタ１０１に送信

することで、セッション確立のためのネゴシエーションや相互の機器情報を交換し、セッション確立となる。以上のＳＩＰ処理を、ＳＩＰモジュール３１５にて行う。なお、セッション確立処理に関しては、図４で詳細に説明する。

【００３９】

３１６はアプリケーションであり、プリンタ１０１が他の機器（例えば、デジカメ１０２）とピアツーピアな通信を行う際に利用するアプリケーションである。

【００４０】

図４は本実施形態のシーケンス図である。このシーケンス図では、ＳＩＰ通信を行うための登録処理（ＳＩＰ　Ｒｅｇｉｓｔｅｒ）は既に完了している状態であり、デジカメ１０２からプリンタ１０１に対してピアツーピアな通信を行う際の手順を示す。

【００４１】

４０１はセッション確立を要求するＩｎｖｉｔｅ要求メッセージであり、セキュリティ管理サーバ１０３を経由してプリンタ１０１に送信される。このセッション確立を要求するＩｎｖｉｔｅ要求メッセージ４０１は、確立を要求するセッション（通信）のセッションＩＤ（通信を識別する識別情報）を含む。この４０１のＩｎｖｉｔｅ要求メッセージ内には、デジカメ１０２とプリンタ１０１でピアツーピア通信を行う際のデジカメ１０２のアドレス情報やアプリケーション情報（ポート番号）、ピアツーピア通信をセキュアに行うためのセキュリティ情報が、ＳＤＰ（Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）内に記述され、添付されている。ＳＤＰは、例えば、ＨＤ１５０７から読み出す。

【００４２】

プリンタ１０１では、受信したＩｎｖｉｔｅ要求メッセージ４０１の返信として、４０２のレスポンスメッセージをセキュリティ管理サーバ１０３経由でデジカメ１０２に対して送信する。この４０２のレスポンスメッセージとしては、例えば、セッション受入を許可する「２００ＯＫ」が返信され（これ以降、２００ＯＫメッセージと呼ぶ）、デジカメ１０２とのピアツーピア通信に必要な各種情報を記述したＳＤＰも含まれる。このＳＤＰは、例えば、ＨＤ１５０７から読み出す。なお、レスポンスメッセージ４０２には他にエラーメッセージも存在し、セッション受入が行えない場合（例えば、他の機器とセッションを確立中であり、デジカメ１０２との新たなセッションを確立できない場合や、デジカメ１０２から送信されたＳＤＰ情報の中で、プリンタ１０１側ではサポートされていない機能の要求があった場合）には４０２にてエラーメッセージが送信される。

【００４３】

４０３ではＩｎｖｉｔｅ要求に対する２００ＯＫメッセージ４０２を受信したデジカメ１０２から、２００ＯＫメッセージ４０２を受理した旨を通知するＡｃｋメッセージをプリンタ１０１に対して送信する。この４０３のＡｃｋメッセージのやり取りにより、デジカメ１０２とプリンタ１０１は、ピアツーピア通信を行うためのセッションを確立したことになる。なお、４０２にて送信されたＳＩＰメッセージが、セッション受入を拒否するエラーメッセージの場合も、４０３にてＡｃｋメッセージが送信される。

【００４４】

デジカメ１０２とプリンタ１０１の間のセッション（通信）は、セキュリティ管理サーバ１０３による仲介により、確立される。すなわち、デジカメ１０２からのＩｎｖｉｔｅ要求メッセージ（セッション要求）４０１に含まれるプリンタ１０１の機器ＩＤ（識別子）をプリンタ１０１のＩＰアドレスに変換する。デジカメ１０２とプリンタ１０１の間のセッションは、このＩＰアドレスを元に確立される。

【００４５】

４０４では、デジカメ１０２は、Ａｃｋメッセージ４０３の送信をきっかけとして、プリンタ１０１とのピアツーピア通信のためのＩＰｓｅｃ要求処理を開始する。具体的には、前述のＳＩＰモジュール３１５より要求発行モジュール３１２に対してＩＰｓｅｃ要求依頼が行われる。同様に、４０５においても、プリンタ１０１は、Ａｃｋメッセージ４０３の受信をきっかけとして、デジカメ１０２とのピアツーピア通信のためのＩＰｓｅｃ要

求処理を開始する。

【００４６】

デジカメ１０２側のＩＰｓｅｃ要求処理（４０４）では、デジカメ１０２とプリンタ１０１とのピアツーピア通信において、ＩＰｓｅｃを利用したセキュリティ通信を行うかどうかを判定し、ＩＰｓｅｃを利用する場合には、セキュリティ管理サーバ１０３に対して、４０６のＩＰｓｅｃ要求メッセージを送信する。同様に、プリンタ１０１側のＩＰｓｅｃ要求処理（４０５）においても、デジカメ１０２とプリンタ１０１とのピアツーピア通信において、ＩＰｓｅｃを利用したセキュリティ通信を行うかどうかを判定し、ＩＰｓｅｃを利用する場合には、セキュリティ管理サーバ１０３に対して、４０７のＩＰｓｅｃ要求メッセージを送信する。なお、上記のＩＰｓｅｃ要求処理（４０４、４０５）の詳細に関しては、図６、図７にて説明する。後述するように、プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ１０３（提供装置）から受け取る通信装置であって、セキュリティを確保するためのパラメータの候補（を含むＩＰｓｅｃ要求メッセージ４０６、４０７）を、セキュリティ管理サーバ１０３に送信する。

【００４７】

ＩＰｓｅｃ要求メッセージ（４０６、４０７）を受信したセキュリティ管理サーバ１０３は、ピアツーピア通信を行おうとする二つの機器からのＩＰｓｅｃ要求メッセージ内容がそろってから、４０８にてＩＰｓｅｃ要求メッセージの解析、ＩＰｓｅｃ設定内容の作成、そして、各機器に対するＩＰｓｅｃ設定内容の返信を行う。なお、上記の処理の詳細に関しては図８、図９にて説明する。後述するように、セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報を第１の装置と第２の装置に提供する提供装置であって、セキュリティ通信を行うためのパラメータの候補（を含むＩＰｓｅｃ要求メッセージ４０６、４０７）を、デジカメ（第１の装置）１０２及びプリンタ（第２の装置）１０１から受信し、デジカメ１０２及びプリンタ１０１から受信したパラメータの候補に基づいて、ＩＰｓｅｃ設定内容（セキュリティ通信を行うために必要な情報）を生成し、ＩＰｓｅｃ設定内容を、デジカメ１０２及びプリンタ１０１に送信する。

【００４８】

４０８で作成された各機器のＩＰｓｅｃ設定内容は、４０９、４１０にてデジカメ１０２とプリンタ１０１にＩＰｓｅｃ要求メッセージの返信としてそれぞれ送信される。４０９のＩＰｓｅｃ設定内容を受信したデジカメ１０２では、ＩＰｓｅｃを設定する。同様に、４１０のＩＰｓｅｃ設定内容を受信したプリンタ１０１でも、ＩＰｓｅｃを設定する。両機器とも、ＩＰｓｅｃ設定が完了すると、４１１にてデジカメ１０２とプリンタ１０１におけるセキュアなピアツーピア通信を開始する。プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ１０３（提供装置）から受け取る通信装置であって、ＩＰｓｅｃ設定内容（セキュリティを確保するために必要な情報）を、セキュリティ管理サーバ１０３から受信し、セキュリティ管理サーバ１０３から受信したＩＰｓｅｃ設定内容を元に、通信相手との通信にセキュリティを確保する。

【００４９】

すなわち、図４は、デジカメ（第一の端末）１０２とプリンタ（第二の端末）１０１の間でＩＰＳＥＣによるセキュリティ通信を実現する為に必要なセッション鍵とセキュリティ設定情報を設定する手順を示している。

【００５０】

セキュリティ管理サーバ（ＳＩＰサーバ）１０３は、デジカメ（第一の端末）１０２からのプリンタ（第二の端末）１０１に対するＩｎｖｉｔｅ要求メッセージ（接続呼出しメッセージ）４０１、及び、プリンタ１０１からのデジカメ１０２に対するレスポンスメッセージ（接続応答メッセージ）４０２を中継する。

【００５１】

セキュリティ管理サーバ１０３は、デジカメ１０２からのＩＰｓｅｃ要求メッセージ（

暗号通信設定要求メッセージ）４０６に含まれるデジカメ１０２のセキュリティ設定候補情報を獲得し、プリンタ１０１からのＩＰｓｅｃ要求メッセージ（暗号通信設定要求メッセージ）４０７に含まれるプリンタ１０１のセキュリティ設定候補情報を獲得する。

【００５２】

セキュリティ管理サーバ１０３は、デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６とプリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７を受信した段階で、デジカメ１０２及びプリンタ１０１のそれぞれに対するＩＰｓｅｃ設定内容（暗号通信で使う暗号鍵（セッション鍵）とセキュリティ設定情報）を生成する。

【００５３】

セキュリティ管理サーバ１０３とデジカメ１０２が、それぞれ所有する第一の秘密対称鍵を使って形成された暗号通信路を使って、デジカメ１０２に対するＩＰｓｅｃ設定内容４０９を、セキュリティ管理サーバ１０３からデジカメ１０２に送信し、セキュリティ管理サーバ１０３とプリンタ１０１が、それぞれ所有する第二の秘密対称鍵を使って形成された暗号通信路を使って、プリンタ１０１に対するＩＰｓｅｃ設定内容４１０を、セキュリティ管理サーバ１０３からプリンタ１０１に送信する。

【００５４】

デジカメ１０２及びプリンタ１０１は、受信したＩＰｓｅｃ設定内容からデジカメ１０２とプリンタ１０１間のＩＰｓｅｃによる暗号通信路を開始する。

【００５５】

図５では、前記ＩＰｓｅｃ作成テーブル３０３の一例を示す。このＩＰｓｅｃ作成テーブル３０３は、ＲＡＭ１５０３上に設けられる。５０１はセッションＩＤであり、二つの機器がＳＩＰを利用して確立したセッションＩＤを示す。５０２、５０３は、先のセッション確立によって、ＩＰｓｅｃを利用したピアツーピア通信を行う二つの機器の情報を格納する。先に受け取ったＩＰｓｅｃ要求メッセージ（４０６）の送信元（デジカメ１０２）の機器情報がｈｏｓｔＡに格納され、もう一方の機器情報がｈｏｓｔＢに格納される。５０４は、最後に受信したＩＰｓｅｃ要求メッセージの受信時間を格納する。これは、ＩＰｓｅｃを利用する二つの機器からのＩＰｓｅｃ要求メッセージがそろわなかった場合（つまり、デジカメ１０２からはＩＰｓｅｃ要求メッセージが受信されたが、その通信相手となるプリンタ１０１からＩＰｓｅｃ要求メッセージが受信されなかった場合）のタイムアウト処理に利用される。５０５は、ＩＰｓｅｃ作成テーブルのステータスを示す。このステータスには、ｗａｉｔｉｎｇ（もう一方の機器からのＩＰｓｅｃ要求（４０７）待ち）、ｇｅｎｅｒａｔｉｎｇ（ＩＰｓｅｃ設定内容を作成中）、ｓｅｎｔ（ＩＰｓｅｃ設定内容の返信（４０９、４１０）が完了）の値が存在する。

【００５６】

以下、５０２、５０３に格納される機器の情報の詳細を説明する。５０６には機器ＩＤが格納され、５０７にはその機器が利用しているＩＰｖ６アドレスを格納する。５０８では、ピアツーピア通信にて利用されるアプリケーションのポート番号を格納し、５０９では、ピアツーピア通信にて利用されるＩＰｓｅｃのレベルを格納する。このＩＰｓｅｃのレベルには、ｕｓｅ（ＩＰｓｅｃ利用は必須ではない）、ｒｅｑｕｉｒｅ（ＩＰｓｅｃ利用は必須）、ｕｎｉｑｕｅ（ＩＰｓｅｃで利用するＳＡを一意に指定）の値が存在する。５１０にはＩＰｓｅｃの設定で利用されるＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）の値を格納する。５１１には、その機器が保有するａｈ（認証）のアルゴリズム名を格納し、５１２には、その機器が保有するｅｓｐ（暗号化）のアルゴリズム名を格納する。なお、５１１、５１２には、複数のアルゴリズム名が格納されることがあり、その場合、利用優先度が高いものから順に格納される。

【００５７】

５２１に、具体的なＩＰｓｅｃ作成テーブルのエントリを示し、５２２、５２３にそれぞれ、エントリ５２１の５０２、５０３に格納されるｈｏｓｔＡの機器情報、ｈｏｓｔＢの機器情報を示す。

【００５８】

図６、図７では、本実施形態における機器側の処理フローを示す。図６、図７は、コンピュータであるＣＰＵ１５０１が読出すことができるように、ＲＯＭ１５０２、ＨＤ１５０７、あるいはＦＤ１５０８に格納されたプログラムの一部を示す。

【００５９】

図６では前記ＳＩＰモジュール３１５において、ＳＩＰ　Ｉｎｖｉｔｅ処理から、前記要求発行モジュール３１２へのＩＰｓｅｃ要求依頼を行う処理に関して説明する。

【００６０】

６０１では、ＳＩＰ　Ｉｎｖｉｔｅ処理におけるメッセージ種別の判定を行う。ＳＩＰ　Ｉｎｖｉｔｅ処理において、Ａｃｋメッセージ４０３（図４）を送信した場合、または、Ａｃｋメッセージ４０３を受信した場合には６０２の処理へ進み、それ以外では６０５へ進み通常のＳＩＰモジュールの処理を行う。ここで、Ａｃｋメッセージ４０３を送信する場合とは、Ｉｎｖｉｔｅ要求メッセージ４０１を送信したデジカメ１０２が該当し、Ａｃｋメッセージ４０３を受信する場合とは、２００ＯＫメッセージ４０２を送信したプリンタ１０１が該当する。

【００６１】

６０２では、ＳＩＰ　Ｉｎｖｉｔｅ処理にて確立されたセッションの情報から、Ｃａｌｌ－ＩＤ、Ｆｒｏｍ、Ｔｏの各情報と自己のＳＤＰ情報を取得する。上記の各情報には、先のＳＩＰ　Ｉｎｖｉｔｅ処理にて確立したセッションＩＤとそのセッションを利用する二つの機器ＩＤ、そして、自己の各種情報が含まれている。６０３では、上記の情報と共に、前記要求発行モジュール３１２に対して、ＩＰｓｅｃ要求依頼を行う。６０４では、６０３でのＩＰｓｅｃ要求依頼の結果を受け、上位アプリケーションに対して、通信相手のＩＰｖ６アドレスとポート番号を通知し、二つの機器にてピアツーピア通信を行う。ＩＰｓｅｃ要求依頼の結果がエラーの場合（つまり、ＩＰｓｅｃの設定が正常に完了しなかった場合、または、ＩＰｓｅｃの利用が指示されていない場合など）には、上位アプリケーションに対し、そのエラーを通知し、ユーザにＩＰｓｅｃを利用しない状態でもピアツーピア通信を行うかの確認を行うようにしてもよい。

【００６２】

図７は６０３にてＩＰｓｅｃ要求依頼を受けた前記要求発行モジュール３１２の処理を中心に説明する。

【００６３】

７０１では、６０３にてＩＰｓｅｃ要求依頼と共に受け取った自己のＳＤＰ情報より、ｓｅｃ＿ｌｅｖｅｌの値を取得する。なお、ＳＤＰ情報に関しては、詳細を後述する。７０１で取得したｓｅｃ＿ｌｅｖｅｌの値を７０２にて判定を行い、ＳＤＰ情報にｓｅｃ＿ｌｅｖｅｌ情報が存在しない場合や、ｓｅｃ＿ｌｅｖｅｌの値が「ｎｏｎｅ」の場合（つまり、ＩＰｓｅｃをピアツーピア通信にて利用しない場合）には、エラーとし、ｓｅｃ＿ｌｅｖｅｌ情報が適当な値（ｕｓｅ、ｒｅｑｕｉｒｅ、ｕｎｉｑｕｅのいずれか）の場合には７０３に処理が進む。７０３では、６０３にてＩＰｓｅｃ要求依頼と共に受け取ったＣａｌｌ－ＩＤ、Ｆｒｏｍ、Ｔｏの各情報を取得し、７０４では、自己ＳＤＰ情報よりＩＰｖ６アドレス、ポート番号を取得する。７０５では、機器に搭載されているＩＰｓｅｃアルゴリズムと、現在利用可能なＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）を取得する。このＩＰｓｅｃアルゴリズムは、認証アルゴリズムと暗号化アルゴリズムの少なくとも一方、もしくは、両方であり、機器に搭載されているＩＰｓｅｃアルゴリズム（の識別子）は、例えば、ＨＤ１５０７から取得する。７０６では、上記７０１、７０３、７０４、７０５で取得した各種情報から、セキュリティ管理サーバ１０３に対して送信するＩＰｓｅｃ要求メッセージを作成する。なお、ＩＰｓｅｃ要求メッセージに関しては詳細を後述する。

【００６４】

７０７にて、７０６にて作成されたＩＰｓｅｃ要求メッセージを、前記暗号通信モジュール３１３によるメッセージ内容の暗号化、前記通信モジュール３１１によるセキュリティ管理サーバ１０３への送信、という手順でセキュリティ管理サーバ１０３に送る。すな

わち、プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ１０３（提供装置）から受け取る通信装置であって、この７０７において、セキュリティを確保するためのＩＰｓｅｃアルゴリズム（パラメータ）の候補（を含むＩＰｓｅｃ要求メッセージ）を、セキュリティ管理サーバ１０３に送信する。この７０７では、プリンタ１０１、デジカメ１０２は、通信相手との間で確立された通信を識別する識別情報であるＣａｌｌ－ＩＤを、セキュリティ管理サーバ１０３に送信する。

【００６５】

７０８では、７０７にて送信したＩＰｓｅｃ要求メッセージ（４０６、４０７）に対するレスポンスメッセージ（４０９、４１０）を受信し、レスポンスメッセージ内から、ＩＰｓｅｃ設定内容を取得する。なお、受信したレスポンスメッセージに関しては、図１１にて詳細を説明する。７０９では、取得したＩＰｓｅｃ設定内容の有効性をチェックし、有効ではない場合（つまり、セキュリティ管理サーバ１０３がエラーを返信してきた場合など）はエラーとし、有効な場合は７１０に処理が進む。７１０では、有効性が確認されたＩＰｓｅｃ設定内容を前記ＩＰｓｅｃ設定モジュール３１４に渡し、機器のカーネルに「ｓｅｔｋｅｙ」コマンドを用いて設定する。

【００６６】

プリンタ１０１、デジカメ１０２は、通信相手との間で行う通信のセキュリティを確保するために必要な情報をセキュリティ管理サーバ１０３（提供装置）から受け取る通信装置であって、この７０８において、セキュリティを確保するために必要な情報であるＩＰｓｅｃ設定内容を、セキュリティ管理サーバ１０３から受信し、７１０において、セキュリティ管理サーバ１０３から受信した情報を元に、通信相手との通信にセキュリティを確保する。

【００６７】

プリンタ１０１、デジカメ１０２は、セキュリティ管理サーバ１０３から受信した情報であるＩＰｓｅｃを元に、通信相手との間で確立された通信（Ｉｎｖｉｔｅ要求メッセージ４０１、レスポンスメッセージ４０２、Ａｃｋメッセージ４０３の送受信により確立された通信）にセキュリティを確保する。

【００６８】

なお、上述のＳＤＰの一例は、以下のとおりである。

ｖ＝０

ｏ＝ＢＪ００１　２４５１８５１　１１２１４４８７０　ＩＮ　ＩＰ６　３ｆｆ：５１４：：１

ｓ＝－

ｃ＝ＩＮ　ＩＰ６　３ｆｆｅ：５１４：：１

ｔ＝０　０

ｍ＝ａｐｐｌｉｃａｔｉｏｎ　８０　ＨＴＴＰ

ｋ＝ｉｐｓｅｃ＿ｌｅｖｅｌ：ｒｅｑｕｉｒｅ

この例は、プリンタ１０１のＳＤＰ内容である。重要な情報に関して説明する。二行目「ｏ＝」の「３ｆｆｅ：５１４：：１」がプリンタ１０１のＩＰｖ６アドレスである。同様に、四行目「ｃ＝」にもＩＰｖ６アドレスが記述される。六行目「ｍ＝」の「８０」がアプリケーションのポート番号であり、「ＨＴＴＰ」のプロトコルを利用することを示す。そして、七行目の「ｋ＝」にて、ｓｅｃ＿ｌｅｖｅｌが記述され、この例では「ｒｅｑｕｉｒｅ」の値が指定されている。このｓｅｃ＿ｌｅｖｅｌを、要求発行モジュール３１２は、図７の７０１で取得する。二行目あるいは四行目のＩＰｖ６アドレス及び六行目のポート番号を、要求発行モジュール３１２は、７０４で取得する。このＳＤＰは、ハードディスク１５０７などに、記憶されている。

【００６９】

図７の７０６にて作成されるＩＰｓｅｃ要求メッセージの一例は、以下のとおりである。

```
＜ｉｐｓｅｃ－ｒｅｑｕｅｓｔ＞
  ＜ｓｅｓｓｉｏｎ－ｉｄ＞２４５１８５１＜／ｓｅｓｓｉｏｎ－ｉｄ＞
  ＜ｌｏｃａｌ－ｈｏｓｔ＞ＤＣ１０１＜／ｌｏｃａｌ－ｈｏｓｔ＞
  ＜ｒｅｍｏｔｅ－ｈｏｓｔ＞ＢＪ１０１＜／ｒｅｍｏｔｅ－ｈｏｓｔ＞
  ＜ｉｐｖ６－ａｄｄｒｅｓｓ＞２００２：２００：：１＜／ｉｐｖ６－ａｄｄｒｅｓ
ｓ＞
  ＜ｐｏｒｔ＞４６１２７＜／ｐｏｒｔ＞
  ＜ｌｅｖｅｌ＞ｒｅｑｕｉｒｅ＜／ｌｅｖｅｌ＞
  ＜ｓｐｉ＞０ｘ８３４＜／ｓｐｉ＞
  ＜ａｈ－ａｌｇｏ＞ｈｍａｃ－ｓｈａ１＜／ａｈ－ａｌｇｏ＞
  ＜ａｈ－ａｌｇｏ＞ｈｍａｃ－ｍｄ５＜／ａｈ－ａｌｇｏ＞
  ＜ｅｓｐ－ａｌｇｏ＞ｂｌｏｗｆｉｓｈ－ｃｂｃ＜／ｅｓｐ－ａｌｇｏ＞
  ＜ｅｓｐ－ａｌｇｏ＞３ｄｅｓ－ｃｂｃ＜／ｅｓｐ－ａｌｇｏ＞
＜／ｉｐｓｅｃ－ｒｅｑｕｅｓｔ＞
```

この例はデジカメ１０２より送信されるＩＰｓｅｃ要求メッセージを示す。データはＸＭＬ形式で記述され、＜ｉｐｓｅｃ－ｒｅｑｕｅｓｔ＞タグに囲まれている。なお、本形態において、このデータ形式をＸＭＬ形式にすることに重要性はなく、その他の形式によるデータ伝達方法でも問題はない。以下、各項目に関して説明する。＜ｓｅｓｓｉｏｎ－ｉｄ＞はデジカメ１０２とプリンタ１０１の間に確立されたセッションＩＤを示し、＜ｌｏｃａｌ－ｈｏｓｔ＞はデジカメ１０２の機器ＩＤを示す。＜ｒｅｍｏｔｅ－ｈｏｓｔ＞はピアツーピア通信の相手であるプリンタ１０１の機器ＩＤを示し、＜ｉｐｖ６－ａｄｄｒｅｓｓ＞はデジカメ１０２のＩＰｖ６アドレスを示す。＜ｐｏｒｔ＞はデジカメ１０２のアプリケーションが利用するポート番号を示し、＜ｌｅｖｅｌ＞はデジカメ１０２でのＩＰｓｅｃレベル（ｓｅｃ＿ｌｅｖｅｌ）を示す。なお、ＩＰｓｅｃレベルをネゴシエーションする形態ではピアツーピア通信の相手であるプリンタ１０１と同一の値となっている。ｓｅｃ＿ｌｅｖｅｌは、ｕｓｅ、ｒｅｑｕｉｒｅ、ｕｎｉｑｕｅのいずれかの値である。＜ｓｐｉ＞はデジカメ１０２のＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）値を示す。＜ａｈ－ａｌｇｏ＞はデジカメ１０２が保有するａｈ（認証）アルゴリズムを示し、＜ｅｓｐ－ａｌｇｏ＞はデジカメ１０２が保有するｅｓｐ（暗号化）アルゴリズムを示す。認証アルゴリズムや暗号化アルゴリズムは、複数保有している可能性があり、その場合は利用優先度の高いアルゴリズムから順に＜ａｈ－ａｌｇｏ＞タグ、＜ｅｓｐ－ａｌｇｏ＞タグを複数記述する。＜ａｈ－ａｌｇｏ＞内のａｈ（認証）アルゴリズム、及び、＜ｅｓｐ－ａｌｇｏ＞内のｅｓｐ（暗号化）アルゴリズムの少なくとも一方、もしくは、両方は、セキュリティ設定候補情報、もしくは、セキュリティ通信を行うためのパラメータの候補である。

【００７０】

以上のように、デジカメ１０２は、セキュリティ設定候補情報を含むＩＰｓｅｃ要求メッセージ（暗号通信設定要求メッセージ）４０６をセキュリティ管理サーバ１０３に送信する。また、プリンタ１０１は、セキュリティ設定候補情報を含むＩＰｓｅｃ要求メッセージ（暗号通信設定要求メッセージ）４０７をセキュリティ管理サーバ１０３に送信する。

【００７１】

デジカメ１０２及びプリンタ１０１は、以上のように、受信したＩＰｓｅｃ設定内容からデジカメ１０２とプリンタ１０１間のＩＰｓｅｃによる暗号通信路を開始する。

【００７２】

図８、図９では、本実施形態におけるセキュリティ管理サーバ側の処理フローを示す。図８、図９は、コンピュータであるＣＰＵ１５０１が読出すことができるように、ＲＯＭ１５０２、ＨＤ１５０７、あるいはＦＤ１５０８に格納されたプログラムの一部を示す。

【００７３】

図８は、前記要求受付モジュール３０２において、ＩＰｓｅｃ要求メッセージを受信し

、ＩＰｓｅｃ設定内容を返信するまでの処理を中心に説明する。特に、デジカメ１０２とプリンタ１０１間にピアツーピア通信用のセッションを確立し、デジカメ１０２から最初のＩＰｓｅｃ要求メッセージを受信し、その直後にプリンタ１０１からのＩＰｓｅｃ要求メッセージを受信する処理に関して説明する。

【００７４】

１００１はＩＰｓｅｃ要求処理のタイムアウトを判定する処理である。本ＩＰｓｅｃ要求処理は、ＳＩＰにより二つの機器間にセッションを確立することをきっかけとして、両機器からのＩＰｓｅｃ要求メッセージ４０６、４０７を受け付けることで、ＩＰｓｅｃ設定内容を作成できる。その為、何らかの原因で一方の機器からＩＰｓｅｃ要求メッセージを受信できなかった場合（例えば、デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６は受信したが、プリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７は受信できなかった場合）には、ＩＰｓｅｃ設定内容の作成が行えない状態となり、ＩＰｓｅｃ要求メッセージを正常に送信した機器１０２側では、ＩＰｓｅｃ設定内容を待ちつづけてしまう。その状態を回避するために、セキュリティ管理サーバ１０３では、１００１にて５０４のｒｅｑｕｅｓｔ　ｔｉｍｅの値と５０５のｓｔａｔｕｓの値をチェックし、ｓｔａｔｕｓがｗａｉｔｉｎｇで、かつ、ｒｅｑｕｅｓｔ　ｔｉｍｅが現在時刻よりも５秒以上過去のエントリに関しては、タイムアウトのエントリと判断する。タイムアウトと判断された場合は、１０１４にてデジカメ１０２に対してエラーを返信しエラー終了し、タイムアウトのエントリがない場合には、１００２へ処理が進む。

【００７５】

１００２では、ＩＰｓｅｃ要求メッセージを受信し、受信したＩＰｓｅｃ要求メッセージより＜ｌｅｖｅｌ＞タグのデータを取得し、その値を判定する。この値が、ｕｓｅ、ｒｅｑｕｉｒｅ、ｕｎｉｑｕｅのどれにも一致しない場合（つまり、受信したＩＰｓｅｃ要求メッセージが有効なＩＰｓｅｃ要求ではない場合）は、１０１６にてＩＰｓｅｃ要求メッセージの送信元にエラーを送信してエラー終了となり、上記のどれかに一致した場合には１００３に処理が進む。

【００７６】

セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であって、この１００２において、セキュリティ通信を行うためのパラメータの候補を含むＩＰｓｅｃ要求メッセージを、デジカメ１０２及びプリンタ１０１から受信する。なお、セキュリティ管理サーバ１０３は、この１００２で、デジカメ１０２とプリンタ１０１間の通信を識別する識別情報であるｓｅｓｓｉｏｎ　ＩＤ（セッションＩＤ）を、デジカメ１０２及びプリンタ１０１から受信する。

【００７７】

１００３では前記ＩＰｓｅｃ作成テーブル３０３に既に存在するＩＰｓｅｃ作成テーブルを参照する。このとき、ＩＰｓｅｃ作成テーブルのセッションＩＤ（５０１）と、受信したＩＰｓｅｃ要求メッセージの＜ｓｅｓｓｉｏｎ－ｉｄ＞タグ情報を比較し、同一のＩＰｓｅｃ作成テーブルを１００４にて判定、抽出する。受信したＩＰｓｅｃ要求メッセージのセッションＩＤと同一のＩＰｓｅｃ作成テーブルがない場合、つまり、デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６（図４）を受信した場合には、１００５に処理が進み、セッションＩＤが同一のＩＰｓｅｃ作成テーブルが存在する場合（つまり、プリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７を受信した場合）には１００８に処理が進む。

【００７８】

最初のＩＰｓｅｃ要求メッセージ（デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６）を受信した場合には、１００５にて新規にＩＰｓｅｃ作成テーブルを作成する。１００６では、受信したＩＰｓｅｃ要求メッセージよりセッションＩＤ情報を取得し、ＩＰｓｅｃ要求メッセージを受信した時刻も取得する。更にＩＰｓｅｃ作成テーブルに、上記の情報をそれぞれ５０１、５０４に格納し、５０５にｗａｉｔｉｎｇのステータス値を設

定する。またＩＰｓｅｃ作成テーブルに、ＩＰｓｅｃ要求メッセージを送信した機器（デジカメ１０２）情報を追加する。具体的には、ｈｏｓｔＡ（５０２）に前記の５０６から５１２（図５）の情報（デジカメ１０２の機器ＩＤ、アドレス、ポート、ＩＰｓｅｃレベル、ＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）、認証アルゴリズム、暗号化アルゴリズム）を、受信したＩＰｓｅｃ要求メッセージ４０６より格納する。１００７では、１００５で作成したＩＰｓｅｃ作成テーブルに、ＩＰｓｅｃ要求メッセージを送信した機器の通信相手となる機器（プリンタ１０１）の情報を追加する。具体的には、ｈｏｓｔＢ（５０３）に、通信相手の機器ＩＤ（プリンタ１０１の機器ＩＤ）のみを格納する。ここまでの処理にてデジカメ１０２からのＩＰｓｅｃ要求メッセージの処理が終了する。

【００７９】

続けてプリンタ１０１からのＩＰｓｅｃ要求メッセージの受信待ちとなる。プリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７を受信すると、１００１、１００２、１００３、１００４と処理が進み、受信したＩＰｓｅｃ要求メッセージの＜ｓｅｓｓｉｏｎ－ｉｄ＞タグ情報と同一のセッションＩＤを有するＩＰｓｅｃ作成テーブルを前記ＩＰｓｅｃ作成テーブル３０３より取得して１００８に処理が進む。１００８では、取得したＩＰｓｅｃ作成テーブルのｈｏｓｔＢの機器ＩＤの値と、受信したＩＰｓｅｃ要求メッセージの＜ｌｏｃａｌ－ｈｏｓｔ＞の値を比較している。この処理において、最初のＩＰｓｅｃ要求メッセージ（デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６）と、今回受信したＩＰｓｅｃ要求メッセージ（プリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７）とが、相互に相手の機器ＩＤを指定しているかを判定している。つまり、デジカメ１０２からのＩＰｓｅｃ要求メッセージには、＜ｒｅｍｏｔｅ－ｈｏｓｔ＞としてプリンタ１０１の機器ＩＤが指定され、プリンタ１０１からのＩＰｓｅｃ要求メッセージには、＜ｒｅｍｏｔｅ－ｈｏｓｔ＞としてデジカメ１０２の機器ＩＤが指定されていることをチェックしている。この判定で一致している場合には１００９に処理が進み、そうでない場合には１０１５にてデジカメ１０２、プリンタ１０１共に、エラーを返信してエラー終了する。

【００８０】

１００９では、受信したＩＰｓｅｃ要求メッセージの送信元の機器（プリンタ１０１）情報をＩＰｓｅｃ作成テーブルに追加する。具体的には、ｈｏｓｔＢ（５０３）に前記の５０７から５１２の情報（プリンタ１０１のアドレス、ポート、ＩＰｓｅｃレベル、ＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）、認証アルゴリズム、暗号化アルゴリズム）を、受信したＩＰｓｅｃ要求メッセージより格納し、５０４のｒｅｑｕｅｓｔ　ｔｉｍｅをプリンタ１０１からのＩＰｓｅｃ要求メッセージを受信した時間に変更し、５０５のｓｔａｔｕｓをｇｅｎｅｒａｔｉｎｇに変更する。

【００８１】

１０１０では、完成したＩＰｓｅｃ作成テーブルの情報と共に前記ＩＰｓｅｃ作成モジュール３０５にＩＰｓｅｃの作成を依頼する。なお、このＩＰｓｅｃ作成処理の詳細に関しては、図９にて説明する。セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であって、この１０１０において、デジカメ１０２及びプリンタ１０１から受信した認証アルゴリズム、暗号化アルゴリズム（パラメータ）の候補に基づいて、セキュリティ通信を行うために必要な情報を生成する。

【００８２】

１０１１では、１０１０のＩＰｓｅｃ作成処理が正常に完了したかを判定し、エラー終了している場合には１０１５へ処理が進み、正常終了している場合には、両機器へ返信するＩＰｓｅｃ設定内容を取得し、１０１２へ処理が進む。１０１２では、両機器（デジカメ１０２とプリンタ１０１）に対して作成されたＩＰｓｅｃ設定内容を、前記暗号通信モジュール３０４によるメッセージ内容の暗号化、前記通信モジュール３０１による各機器への送信、という手順となる。この１０１２では、セキュリティ管理サーバ１０３とデジカメ１０２が、それぞれ所有する第一の秘密対称鍵を使って形成された暗号通信路を使っ

て、デジカメ１０２に対するＩＰｓｅｃ設定内容４０９を、セキュリティ管理サーバ１０３からデジカメ１０２に送信し、セキュリティ管理サーバ１０３とプリンタ１０１が、それぞれ所有する第二の秘密対称鍵を使って形成された暗号通信路を使って、プリンタ１０１に対するＩＰｓｅｃ設定内容４１０を、セキュリティ管理サーバ１０３からプリンタ１０１に送信する。

【００８３】

セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であって、生成されたＩＰｓｅｃ設定内容（セキュリティ通信を行うために必要な情報）を、この１０１２において、デジカメ１０２及びプリンタ１０１に送信する。この１０１２で、セキュリティ管理サーバ１０３は、ＩＰｓｅｃ設定内容を、識別情報であるセッションＩＤにより識別される通信のセキュリティを確保するために、デジカメ１０２及びプリンタ１０１に送信する。

【００８４】

また、この送信処理が正常に完了すると、ＩＰｓｅｃ作成テーブルのｓｔａｔｕｓの値をｓｅｎｔへ変更する。最後に、１０１３にて該当するＩＰｓｅｃ作成テーブルを削除する。この際、該当するＩＰｓｅｃ作成テーブルのｓｔａｔｕｓ項目がｓｅｎｔであることを確認してから削除される。

【００８５】

図９は前記ＩＰｓｅｃ設定モジュール３０５での処理を示す。特に、先の１０１０のＩＰｓｅｃ作成依頼を受け、デジカメ１０２とプリンタ１０１それぞれに対するピアツーピア通信用のＩＰｓｅｃ設定内容を作成する処理に関して説明する。

【００８６】

ＩＰｓｅｃ設定依頼を受けた前記ＩＰｓｅｃ設定モジュール３０５は、１１０１にてＩＰｓｅｃ作成テーブルより指定されたエントリの内容を取得する。取得したＩＰｓｅｃ作成テーブルの情報より、二つの機器情報（デジカメ１０２の情報と、プリンタ１０１の情報）の、ｓｅｃ＿ｌｅｖｅｌ項目を１１０２にて比較する。仮に不一致の場合にはエラー終了となる。なお、これらの情報は、ＳＩＰ　Ｉｎｖｉｔｅ処理にて両機器よりＳＤＰを利用して自己情報を通知し、共通のセキュリティポリシーでの通信を行うために、ネゴシエーションを行う形態では、１１０２の比較において、一致する。両機器で設定されたｓｅｃ＿ｌｅｖｅｌが一致している場合、１１０２から１１０３に進む。

【００８７】

１１０３では、両機器の情報から、ａｈ＿ａｌｇｏ項目のデータを比較し、共通の認証アルゴリズムが存在するかを判定する。二つの機器（デジカメ１０２とプリンタ１０１）で共通の認証アルゴリズムが存在した場合には１１０４へ進み、共通の認証アルゴリズムが存在しない場合には、１１０５へ処理が進む。１１０４では、二つの機器で共通な認証アルゴリズム（の識別子）を取得する。ＩＰｓｅｃ作成テーブル３０３が図５に示される内容を有する場合、１１０４では、「ｈｍａｃ－ｓｈａ１」が取得される。

【００８８】

１１０５では、両機器の情報から、ｅｓｐ＿ａｌｇｏ項目のデータを比較し、共通の暗号化アルゴリズムが存在するかを判定する。二つの機器（デジカメ１０２とプリンタ１０１）で共通の暗号化アルゴリズムが存在した場合には１１０６へ進み、共通の暗号化アルゴリズムが存在しない場合には、１１０７へ処理が進む。１１０６では、二つの機器で共通な暗号化アルゴリズム（の識別子）を取得する。１１０７では、１１０４または１１０６にて共通のアルゴリズムが取得されたか判定する。ＩＰｓｅｃ作成テーブル３０３が図５に示される内容を有する場合、１１０７では、「３ｄｅｓ－ｃｂｃ」が取得される。ここで、認証アルゴリズムも暗号化アルゴリズムも共通なものが取得できなかった場合にはエラー終了となる。

【００８９】

１１０８では、１１０４、１１０６で取得された認証アルゴリズム、暗号化アルゴリズ

ムのそれぞれの情報から、それらのアルゴリズムに適した鍵を生成する。鍵生成は、乱数を用いて生成し、そのアルゴリズムに適した鍵の長さに調整する。アルゴリズムと鍵長の関係の詳細は、後述する。セキュリティ管理サーバ１０３は、セキュリティ通信を行うために必要な情報をデジカメ（第１の装置）１０２とプリンタ（第２の装置）１０１に提供する提供装置であって、デジカメ１０２及びプリンタ１０１から受信した認証アルゴリズム及び暗号化アルゴリズム（パラメータ）の候補に基づいて、セキュリティ通信を行うために必要な情報（デジカメ１０２とプリンタ１０１間のセキュリティ通信に用いる認証アルゴリズム、暗号化アルゴリズム、及び、鍵）を生成する。

【００９０】

１１０９では、ＩＰｓｅｃ設定内容のテンプレートデータに、１１０１で取得したＩＰｓｅｃ作成テーブルの各情報と、１１０４、１１０６、１１０８で取得・生成したＩＰｓｅｃ関連の各アルゴリズムとその鍵情報から、適したデータを入力し、ＩＰｓｅｃ設定内容を作成する。なお、ＩＰｓｅｃ設定内容テンプレートの詳細に関しては、図１０にて説明する。作成されたＩＰｓｅｃ設定内容は１１１０にてｈｏｓｔＡ側機器（デジカメ１０２）のＩＰｓｅｃ設定内容として完成する。

【００９１】

そして、１１１１では、１１０９で作成したＩＰｓｅｃ設定内容の一部を修正する。具体的な修正内容は、ＳＰ（Ｓｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙ）の設定内容において、通信の方向を規定している「ｉｎ」と「ｏｕｔ」の記述を入れ換える。１１１１で修正したＩＰｓｅｃ設定内容は１１１２にてｈｏｓｔＢ側機器（プリンタ１０１）のＩＰｓｅｃ設定内容として完成する。

【００９２】

前述した１１０８の処理における認証アルゴリズム、暗号化アルゴリズムに対応する鍵の長さに関しては、以下のとおりである。例えば、認証アルゴリズムとして「ｈｍａｃ－ｓｈａ１」が選択されていた場合、この認証アルゴリズムに対応する鍵として、長さが１６０ビットの鍵が生成される。また、暗号化アルゴリズムとして「３ｄｅｓ－ｃｂｃ」が選択されていた場合、この暗号化アルゴリズムに対応する鍵として、長さが６４ビットの鍵が生成される。また、認証アルゴリズムが「ｈｍａｃ－ｍｄ５」であれば、１２８ビットの鍵が生成される。アルゴリズムの中には、「ｂｌｏｗｆｉｓｈ－ｃｂｃ」のように鍵の長さが４０ビットから４４８ビットまでの任意のビット長で生成可能なものや、「ｒｉｊｎｄａｅｌ－ｃｂｃ」のように、１２８ビット、１９２ビット、２５６ビットのいずれかのビット長を利用するものが存在する。

【００９３】

図１０は、前述した１１０９の処理におけるＩＰｓｅｃ設定テンプレートの一例を示す。ＩＰｓｅｃ設定テンプレートは、ＩＰｓｅｃを設定する「ｓｅｔｋｅｙ」コマンドのフォーマットに合わせて記述されているが、このフォーマットに限定するものではない。一行目、二行目がＳＰ（Ｓｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙ）情報を示し、三行目から六行目がＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）情報を示す。図中の＜　＞項目にＩＰｓｅｃ作成テーブルや、先に生成された鍵情報を代入することで、ＩＰｓｅｃ設定内容が完成する。各項目の意味を以下で説明する。

【００９４】

＜Ａ＿ａｄｄｒ＞にはｈｏｓｔＡ側機器のＩＰｖ６アドレスを代入し、＜Ｂ＿ａｄｄｒ＞にはｈｏｓｔＢ側機器のＩＰｖ６アドレスを代入する。＜Ａ＿ｐｏｒｔ＞にはｈｏｓｔＡ側機器のポート番号を代入し、＜Ｂ＿ｐｏｒｔ＞にはｈｏｓｔＢ側機器のポート番号を代入する。

【００９５】

＜ｓｅｃ＿ｔｙｐｅ＞には前記１１０４、１１０６にて取得された共通なアルゴリズムの種類を代入する。つまり、二つの機器で共通な認証アルゴリズムと暗号化アルゴリズムをそれぞれ取得できた場合には「ａｈ」と「ｅｓｐ」を代入し、認証アルゴリズムのみ取得できた場合には「ａｈ」を代入し、暗号化アルゴリズムのみ取得できた場合には「ｅｓ

ｐ」を代入する。＜ｓｅｃ＿ｌｅｖｅｌ＞には両機器で共通なｓｅｃ＿ｌｅｖｅｌを代入する。この認証アルゴリズムと暗号化アルゴリズムは、デジカメ１０２及びプリンタ１０１から受信された認証アルゴリズムと暗号化アルゴリズム（セキュリティ通信を行うためのパラメータ）の候補から選択される。

【００９６】

なお、ｓｅｃ＿ｔｙｐｅに「ａｈ」と「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。この例は、認証と暗号化が、必須であることが記述されている例である。

【００９７】

＜Ａ＿ｓｐｉ＞にはｈｏｓｔＡ側機器のＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）を代入し、＜Ｂ＿ｓｐｉ＞にはｈｏｓｔＢ側機器のＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）を代入する。

【００９８】

なお、ｓｅｃ＿ｔｙｐｅでａｈのみ利用の場合は、四行目と六行目のｅｓｐに関するＳＡ登録は削除し、ｓｅｃ＿ｔｙｐｅでｅｓｐのみ利用の場合は、三行目と五行目のａｈに関するＳＡ登録を削除する。

【００９９】

また、ｓｅｃ＿ｔｙｐｅにてａｈとｅｓｐを両方利用する場合には、テンプレートからの特定行の削除は行わず、複数の＜Ａ＿ｓｐｉ＞や＜Ｂ＿ｓｐｉ＞にはプラス１を加えて異なった値を代入する。つまり、ｈｏｓｔＡ側機器のＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）が０ｘ８３４の場合、五行目の＜Ａ＿ｓｐｉ＞には「０ｘ８３４」を代入し、六行目の＜Ａ＿ｓｐｉ＞には「０ｘ８３５」を代入する。そして、＜ａｈ＿ａｌｇｏ＞、＜ｅｓｐ＿ａｌｇｏ＞にはそれぞれ、１１０４、１１０６で取得した両機器で共通の認証アルゴリズム、暗号化アルゴリズムを代入し、＜ａｈ＿ｋｅｙ＞、＜ｅｓｐ＿ｋｅｙ＞には認証、暗号用に１１０８で生成した鍵をそれぞれ代入する。認証用、暗号用の鍵は、デジカメ１０２及びプリンタ１０１から受信された認証アルゴリズムと暗号化アルゴリズム（セキュリティ通信を行うためのパラメータ）の候補に基づいて生成される。

【０１００】

図１１は、ＩＰｓｅｃ設定内容の一例を示す。特に、図のデータはデジカメ１０２に対して送信されるＩＰｓｅｃ設定内容を示す。データはＸＭＬ形式で記述され、＜ｉｐｓｅｃ－ｒｅｓｐｏｎｓｅ＞タグ内の＜ｉｐｓｅｃ－ｄａｔａ＞タグに囲まれている。なお、本形態において、このデータ形式をＸＭＬ形式にすることに重要性はなく、その他の形式によるデータ伝達方法でも問題はない。

【０１０１】

以上のように、セキュリティ管理サーバ１０３は、デジカメ１０２からのＩＰｓｅｃ要求メッセージ（暗号通信設定要求メッセージ）４０６に含まれるデジカメ１０２が有する認証アルゴリズム、暗号化アルゴリズム（セキュリティ設定候補情報）を獲得し、プリンタ１０１からのＩＰｓｅｃ要求メッセージ（暗号通信設定要求メッセージ）４０７に含まれるプリンタ１０１が有する（認証アルゴリズム、暗号化アルゴリズム）セキュリティ設定候補情報を獲得する。

【０１０２】

セキュリティ管理サーバ１０３は、デジカメ１０２からのＩＰｓｅｃ要求メッセージ４０６とプリンタ１０１からのＩＰｓｅｃ要求メッセージ４０７を受信した段階で、デジカメ１０２及びプリンタ１０１のそれぞれに対するＩＰｓｅｃ設定内容（暗号通信で使う暗号鍵（セッション鍵）とセキュリティ設定情報）を生成する（１１０８～１１１２）。

【０１０３】

セキュリティ管理サーバ１０３は、デジカメ１０２に対するＩＰｓｅｃ設定内容４０９

をデジカメ１０２に送信し、プリンタ１０１に対するＩＰｓｅｃ設定内容４１０をプリンタ１０１に送信する。

【図面の簡単な説明】

【０１０４】

【図１】本発明の実施形態のネットワーク構成図である。

【図２】本実施形態で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図である。

【図３】プリンタ１０１とセキュリティ管理サーバ１０３のモジュール構成図である。

【図４】本実施形態のシーケンス図である。

【図５】ＩＰｓｅｃ作成テーブル３０３の一例の図である。

【図６】ＳＩＰモジュール３１５において、ＳＩＰ　Ｉｎｖｉｔｅ処理から要求発行モジュール３１２へのＩＰｓｅｃ要求依頼を行う処理フロー図である。

【図７】ＩＰｓｅｃ要求依頼を受けた前記要求発行モジュール３１２の処理を中心とした処理フロー図である。

【図８】要求受付モジュール３０２において、ＩＰｓｅｃ要求メッセージを受信しＩＰｓｅｃ設定内容を返信するまでの処理を中心とする処理フロー図である。

【図９】ＩＰｓｅｃ設定モジュール３０５での処理フロー図である。

【図１０】ＩＰｓｅｃ設定テンプレートの一例を示す図である。

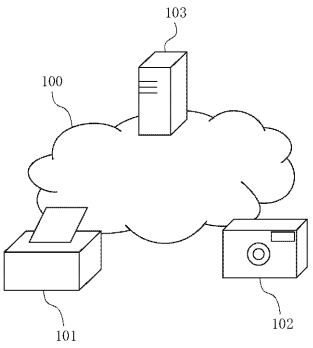
【図１１】ＩＰｓｅｃ設定内容の一例を示す図である。

【符号の説明】

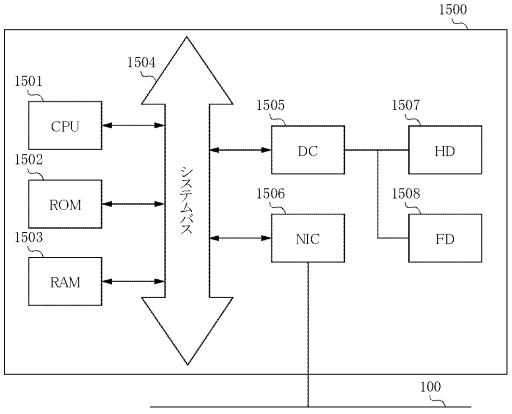
【０１０５】

１００　インターネット
１０１　プリンタ
１０２　デジタルスチルカメラ（デジカメ）
１０３　セキュリティ管理サーバ

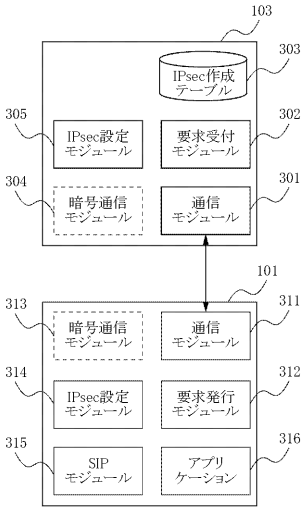
【図１】



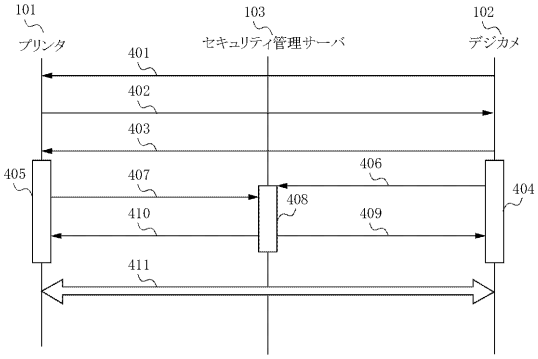
【図２】



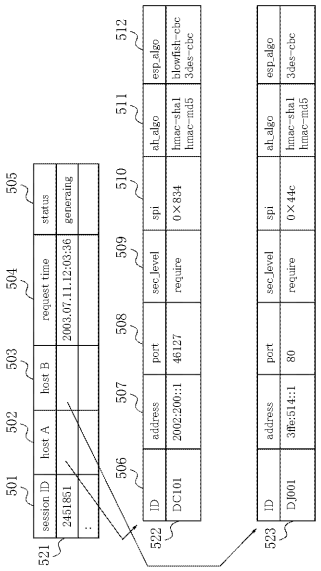
【図３】


103
303
IPsec作成
テーブル
305
IPsec設定
モジュール
302
要求受付
モジュール
304
暗号通信
モジュール
301
通信
モジュール
101
313
暗号通信
モジュール
311
通信
モジュール
314
IPsec設定
モジュール
312
要求発行
モジュール
315
SIP
モジュール
316
アプリ
ケーション

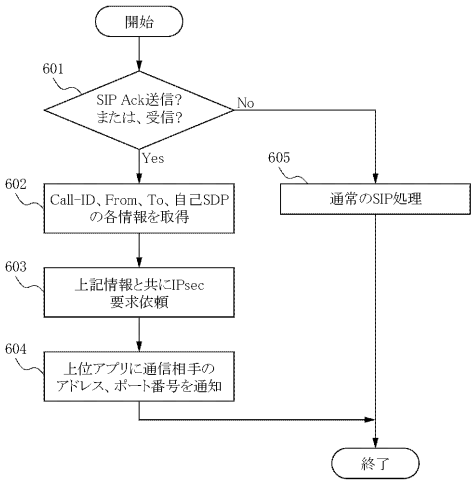
【図４】


101
プリンタ
103
セキュリティ管理サーバ
102
デジカメ
401
402
403
405
406
407
408
404
410
409
411

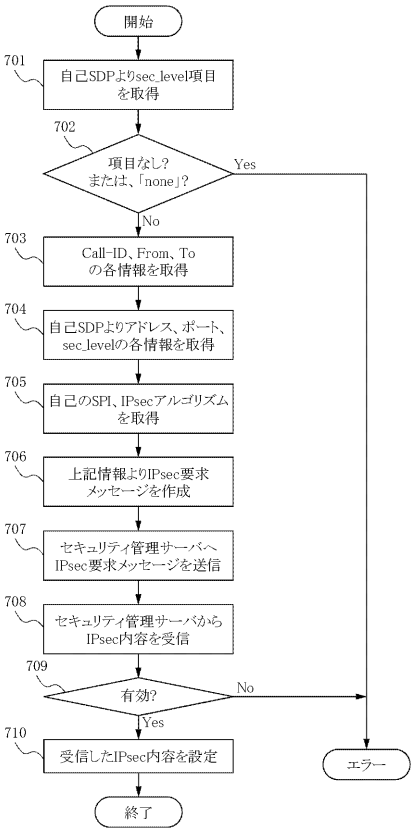
【図５】


501
session ID
2451861
502
host A
503
host B
504
request time
2003.07.11.12:03:36
505
status
generating
506
ID
DC101
507
address
2002:200::1
508
port
46127
509
sec_level
require
510
spi
0×834
511
ah_algo
hmac-sha1
hmac-md5
512
esp_algo
blowfish-cbc
3des-cbc
521
522
523
ID
DJ001
address
3ffe:514::1
port
80
sec_level
require
spi
0×44c
ah_algo
hmac-sha1
hmac-md5
esp_algo
3des-cbc

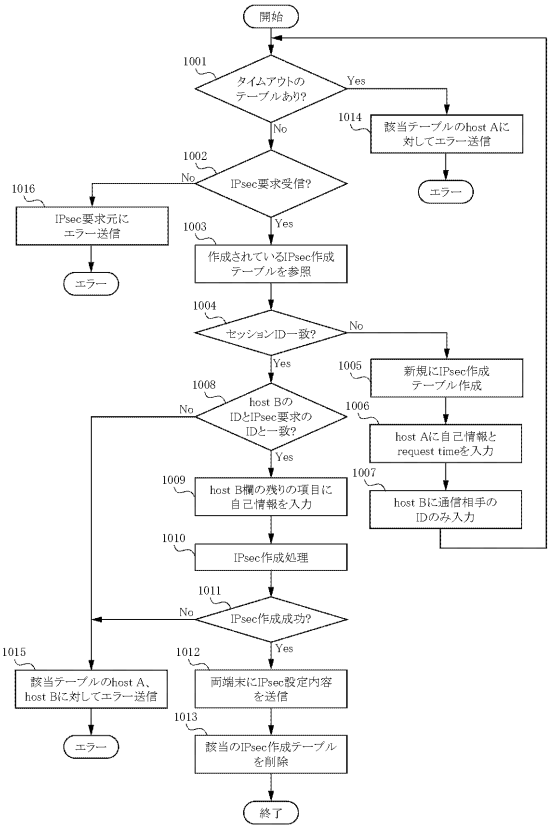
【図６】


開始
601
SIP Ack送信?
または、受信?
No
Yes
605
通常のSIP処理
602
Call-ID、From、To、自己SDP
の各情報を取得
603
上記情報と共にIPsec
要求依頼
604
上位アプリに通信相手の
アドレス、ポート番号を通知
終了

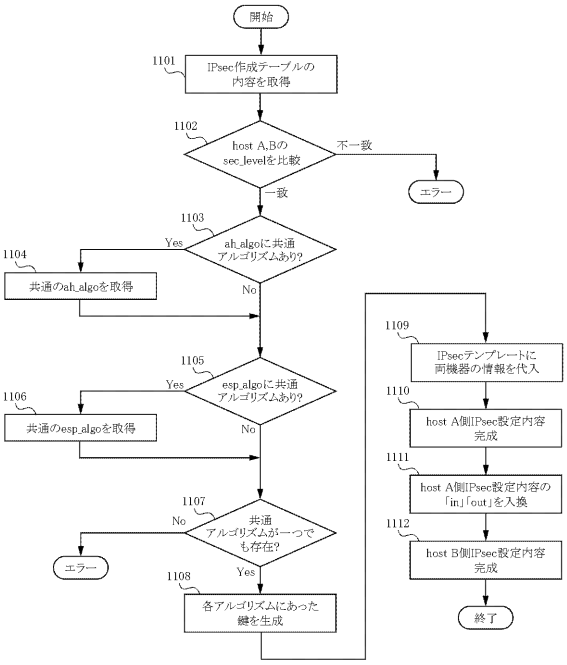
【図７】



【図８】



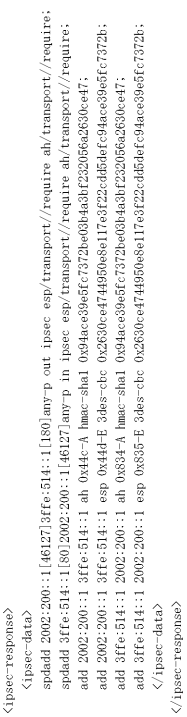
【図９】



【図１０】

spdadd<A_addr>[<A_port>]<B_addr>[<B_port>]any-P out ipsec<sec_type>/transport//<sec_level>...;
spdadd<B_addr>[<B_port>]<A_addr>[<A_port>]any-P in ipsec<sec_type>/transport//<sec_level>...;
add<A_addr><B_addr>ah<B_spi>-A<ah_algo><ah_key>;
add<A_addr><B_addr>esp<B_spi>-E<esp_algo><esp_key>;
add<B_addr><A_addr>ah<A_spi>-A<ah_algo><ah_key>;
add<B_addr><A_addr>esp<A_spi>-E<esp_algo><esp_key>;

【図１１】


<ipsec-response>
<ipsec-data>
spdadd 2002:200::1[46127]3ffe:514::1[180]any-p out ipsec esp/transport//require ah/transport//require;
spdadd 3ffe:514::1[80]2002:200::1[46127]any-p in ipsec esp/transport//require ah/transport//require;
add 2002:200::1 3ffe:514::1 ah 0x44c-A hmac-sha1 0x94ace39e5fc7372be03b4a3bf232056a2630ce47;
add 2002:200::1 3ffe:514::1 esp 0x44d-E 3des-cbc 0x2630ce4744950e8e117e3f22cdd5def c94ace39e5fc7372b;
add 3ffe:514::1 2002:200::1 ah 0x834-A hmac-sha1 0x94ace39e5fc7372be03b4a3bf232056a2630ce47;
add 3ffe:514::1 2002:200::1 esp 0x835-E 3des-cbc 0x2630ce4744950e8e117e3f22cdd5def c94ace39e5fc7372b;
</ipsec-data>
</ipsec-response>

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

審査官　土居　仁士

(56)参考文献　特開２００１－２９８４４９（ＪＰ，Ａ）
特開２００１－３３３１１０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８