

(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2005-295038

(P2005-295038A)

(43) 公開日 平成17年10月20日(2005.10.20)

(51) Int.Cl.⁷

H04L 12/28

F 1

H04L 12/28 200Z

テーマコード(参考)

5KO33

審査請求 有 請求項の数 15 O L (全 26 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)

(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】 提供装置、提供方法、通信装置、通信方法、及び、プログラム

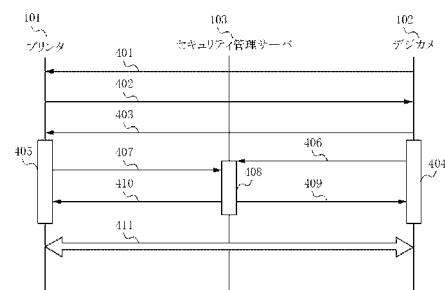
(57) 【要約】

【課題】 セキュリティを確保することは、困難だった

。

【解決手段】 セキュリティ管理サーバ103は、デジカメ102、プリンタ101からIPsec要求メッセージ406、407を受信し、IPsec設定内容を作成して、デジカメ102、プリンタ101にIPsec設定内容409、410を返信する。IPsec要求メッセージ406、407は、セッションID、IPsecレベル(use、require、uniqueのいずれか)、認証アルゴリズム、暗号化アルゴリズムを含む。IPsec設定内容409、410は、認証アルゴリズム、暗号化アルゴリズム、認証用の鍵、暗号用の鍵を含む。

【選択図】 図4



【特許請求の範囲】**【請求項 1】**

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、第1の装置及び第2の装置から受信する受信手段と、

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する生成手段と、

前記生成手段により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、前記第1の装置及び第2の装置に送信する送信手段とを有することを特徴とする提供装置。

10

【請求項 2】

第1の装置と第2の装置がセキュリティの確保された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、

第1の装置と第2の装置間の通信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、第1の装置及び第2の装置から受信する受信手段と、

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する生成手段と、

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前記生成手段により生成された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の装置に送信する送信手段とを有することを特徴とする提供装置。

20

【請求項 3】

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方法であって、

セキュリティ通信を行うためのパラメータの候補を、第1の装置及び第2の装置から受信し、

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、前記第1の装置及び第2の装置に送信することを特徴とする提供方法。

30

【請求項 4】

第1の装置と第2の装置がセキュリティの確保された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方法であって、

第1の装置と第2の装置間の通信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、第1の装置及び第2の装置から受信し、

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、

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前記生成された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の装置に送信することを特徴とする提供方法。

40

【請求項 5】

請求項3の提供方法を実現するためのプログラム。

【請求項 6】

請求項4の提供方法を実現するためのプログラム。

【請求項 7】

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、提供装置に送信する送信手段と、

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受信手段と、

前記受信手段により提供装置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セキュリティ確保手段とを有することを特徴とする通信装置。

50

【請求項 8】

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提供装置から受け取る通信装置であって、

通信相手との間で確立された通信を識別する識別子、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、提供装置に送信する送信手段と、

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受信手段と、

前記受信手段により提供装置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セキュリティ確保手段とを有することを特徴とする通信装置。

【請求項 9】

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提供装置から受け取る通信方法であって、

セキュリティを確保するためのパラメータの候補を、提供装置に送信し、

セキュリティを確保するために必要な情報を、提供装置から受信し、

前記提供装置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ことを特徴とする通信方法。

【請求項 10】

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提供装置から受け取る通信方法であって、

通信相手との間で確立された通信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、提供装置に送信し、

セキュリティを確保するために必要な情報を、提供装置から受信し、

前記提供装置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ことを特徴とする通信方法。

【請求項 11】

請求項 9 の提供方法を実現するためのプログラム。

【請求項 12】

請求項 10 の提供方法を実現するためのプログラム。

【請求項 13】

セキュリティを確保するためのパラメータの候補は、セキュリティを確保するための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 1 又は 2 の提供装置、請求項 3 又は 4 の提供方法、請求項 5 又は 6 のプログラム、請求項 7 又は 8 の通信装置、請求項 9 又は 10 の通信方法、もしくは、請求項 11 又は 12 のプログラム。

【請求項 14】

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 の提供装置、請求項 3 又は 4 の提供方法、請求項 5 又は 6 のプログラム、請求項 7 又は 8 の通信装置、請求項 9 又は 10 の通信方法、もしくは、請求項 11 又は 12 のプログラム。

【請求項 15】

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鍵であることを特徴とする請求項 1 又は 2 の提供装置、請求項 3 又は 4 の提供方法、請求項 5 又は 6 のプログラム、請求項 7 又は 8 の通信装置、請求項 9 又は 10 の通信方法、もしくは、請求項 11 又は 12 のプログラム。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、第 1 の装置と第 2 の装置がセキュリティの確保された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、提供方法、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提供装置から受け取る通信装置、通信方法、及び、提供方法又は通信方法を実現するためのプログラムに関する。

【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れる。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(Diffe-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(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。

【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】**

本発明の提供装置、方法、プログラムは、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、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、前記第1の装置及び第2の装置に送信することを特徴とする。

【0009】

また、本発明の通信装置、方法、プログラムは、セキュリティを確保するためのパラメータの候補を、提供装置に送信し、セキュリティを確保するために必要な情報を、提供装置から受信し、前記提供装置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ことを特徴とする。

10

20

30

40

50

【発明の効果】**【0010】**

以上述べたように、セキュリティを確保するための処理を軽減することができる。

【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。10

【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104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。20

【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。30

【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。40

【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。50

【 0 0 1 8 】

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。

【 0 0 1 9 】

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。

10

【 0 0 2 0 】

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。

20

【 0 0 2 1 】

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。

【 0 0 2 2 】

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。

【 0 0 2 3 】

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。

30

【 0 0 2 4 】

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104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。

40

【 0 0 2 5 】

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ーフェースカード(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ーフェースカード1506を介して接続される。

50

【 0 0 2 6 】

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、システムバス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

50

等として機能する。D C 1 5 0 5 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H D 1 5 0 7 、およびF D 1 5 0 8 とのアクセスを制御する。N I C 1 5 0 6 は、インターネット1 0 0 を通じてI P v 6 通信プロトコルを用いた相互通信をする。

【 0 0 2 7 】

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）1 0 2 とプリンタ（第2の装置）1 0 1 に提供する提供装置であるセキュリティ管理サーバ1 0 3 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1 0 2 及びプリンタ1 0 1 から受信するN I C 1 5 0 6 と、デジカメ1 0 2 及びプリンタ1 0 1 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C P U 1 5 0 1 とを有する。また、N I C 1 5 0 6 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1 0 2 及びプリンタ1 0 1 に送信する送信手段である。N I C 1 5 0 6 は、デジカメ1 0 2 がプリンタ1 0 1 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（I n v i t e 要求メッセージ）を受信し、C P U 1 5 0 1 は、セッション要求メッセージに含まれるプリンタ1 0 1 の機器I D（識別子）をプリンタ1 0 1 のI P アドレスに変換し、デジカメ1 0 2 とプリンタ1 0 2 の間のセッション（通信）が確立されるのを仲介する。10

【 0 0 2 8 】

更に、セキュリティ管理サーバ1 0 3 のN I C 1 5 0 6 は、デジカメ1 0 2 とプリンタ1 0 1 間の通信を識別する識別情報を、デジカメ1 0 2 及びプリンタ1 0 1 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1 0 2 及びプリンタ1 0 1 に送信する。20

【 0 0 2 9 】

プリンタ1 0 1 、デジカメ1 0 2 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）1 0 3 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1 0 3 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N I C 1 5 0 6 と、N I C 1 5 0 6 によりセキュリティ管理サーバ1 0 3 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C P U 1 5 0 1 とを有する。30

【 0 0 3 0 】

プリンタ1 0 1 、デジカメ1 0 2 のN I C 1 5 0 6 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1 0 3 に送信し、C P U 1 5 0 1 は、セキュリティ管理サーバ1 0 3 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1 0 2 のN I C 1 5 0 6 は、プリンタ1 0 1 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（I n v i t e 要求メッセージ）を、セキュリティ管理サーバ1 0 3 に送信する。

【 0 0 3 1 】

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。40

【 0 0 3 2 】

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。

【 0 0 3 3 】

図3は、プリンタ1 0 1 とセキュリティ管理サーバ1 0 3 のモジュール構成図である。3 0 1 ~ 3 0 5 はセキュリティ管理サーバ1 0 3 内に搭載されたモジュールであり、3 1 1 ~ 3 1 6 はプリンタ1 0 1 内に搭載されたモジュールである。なお、デジカメ1 0 1 も、プリンタ1 0 1 と同様のモジュール構成を有する。50

【0034】

301は通信モジュールであり、ネットワークインターフェースカード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。

10

【0035】

311は通信モジュールであり、ネットワークインターフェースカード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。

20

【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。

20

【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。

30

【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SIPURI(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SIPURIとそのIPv6アドレスを登録する。登録されたプリンタ101のSIPURIを用いて、デジカメ102がセッション要求メッセージ(SIPInvite)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。

40

【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(SIPRegister)は既に完了している状態であり、デジカメ1

50

02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。10

【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のレスポンスマ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のレスポンスマッセージとしては、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、レスポンスマッセージ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102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。20

【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。30

【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。40

【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50

求メッセージを送信する。なお、上記の I P s e c 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I P s e c 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】

I P s e c 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I P s e c 要求メッセージ内容がそろってから、408にてI P s e c 要求メッセージの解析、I P s e c 設定内容の作成、そして、各機器に対するI P s e c 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I P s e c 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、I P s e c 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、I P s e c 設定内容を、デジカメ102及びプリンタ101に送信する。

10

【0048】

408で作成された各機器のI P s e c 設定内容は、409、410にてデジカメ102とプリンタ101にI P s e c 要求メッセージの返信としてそれぞれ送信される。409のI P s e c 設定内容を受信したデジカメ102では、I P s e c を設定する。同様に、410のI P s e c 設定内容を受信したプリンタ101でも、I P s e c を設定する。両機器とも、I P s e c 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、I P s e c 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I P s e c 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。

20

30

【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I P S E C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I n v i t e 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マッチングメッセージ(接続応答メッセージ)402を中継する。

40

【0051】

セキュリティ管理サーバ103は、デジカメ102からのI P s e c 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I P s e c 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I P s e c 要求メッセージ406とプリンタ101からのI P s e c 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I P s e c 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】

50

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つた場合(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つた場合)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が読出しができるように、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な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

10

20

30

40

50

るレスポンスマッセージ(409、410)を受信し、レスポンスマッセージ内から、IPsec設定内容を取得する。なお、受信したレスポンスマ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、レスポンスマッセージ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 3ff: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「3ff: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1508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-address>
<port>46127</port>
<level>require</level>
<spi>0x834</spi>
```

10

20

30

40

50

```

<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-adddress>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6、図7は、コンピュータであるCPU1501が読出しができるように、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、その後にプリンタ102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

10

20

30

40

50

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。

10

【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を、デジカメ102及びプリンタ101から受信する。

20

【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。

30

【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

40

50

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102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1

10

20

30

40

50

012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 알고리즘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 알고리즘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】

10

20

30

40

50

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。10

【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。20

【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。30

【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「esp」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。40

【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50

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host A側機器のSPI(Security Parameter Index)を代入し、<B_spi>にはhost B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、host A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、<ipsecresponse>タグ内の<ipsecdat>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。

10

20

30

40

50

【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。

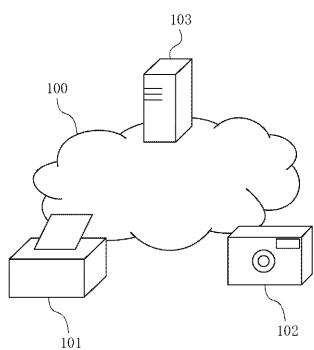
10

【符号の説明】

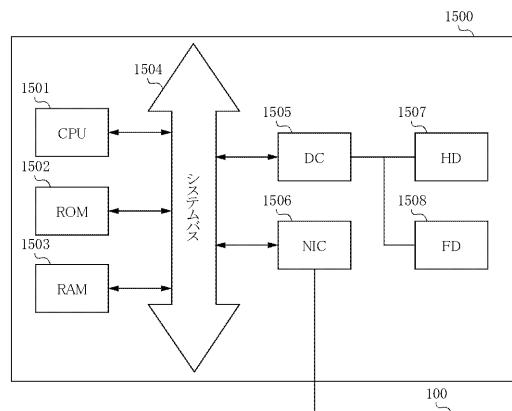
【0105】

- 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

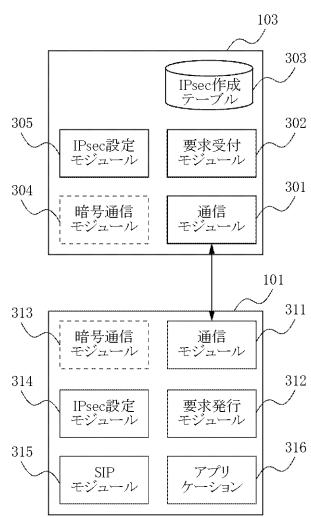
【図1】



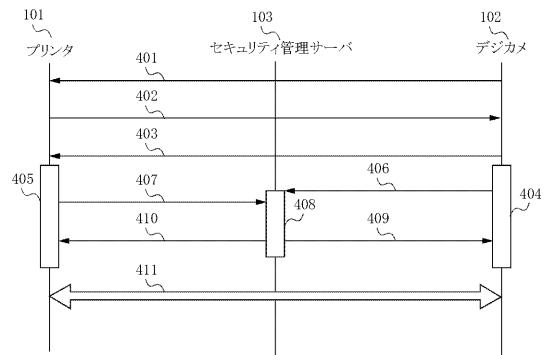
【図2】



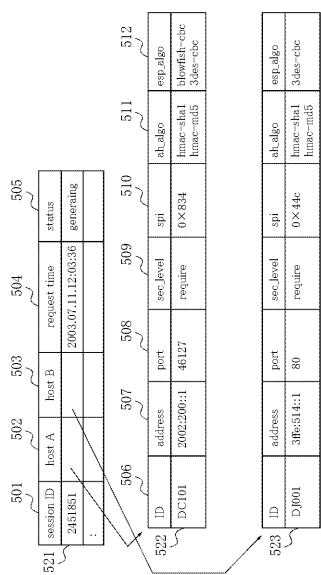
【図3】



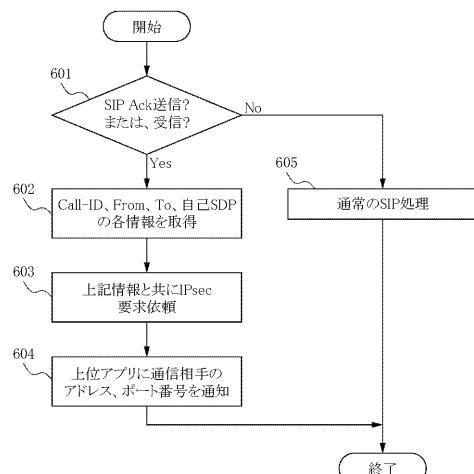
【図4】



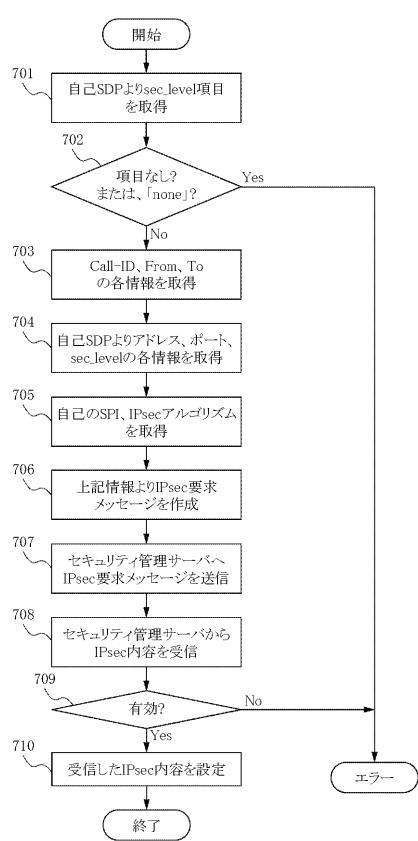
【図5】



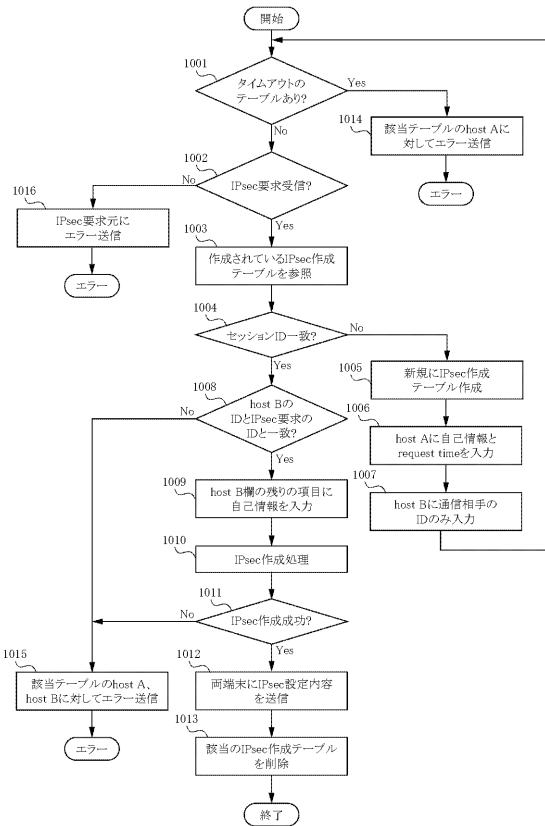
【図6】



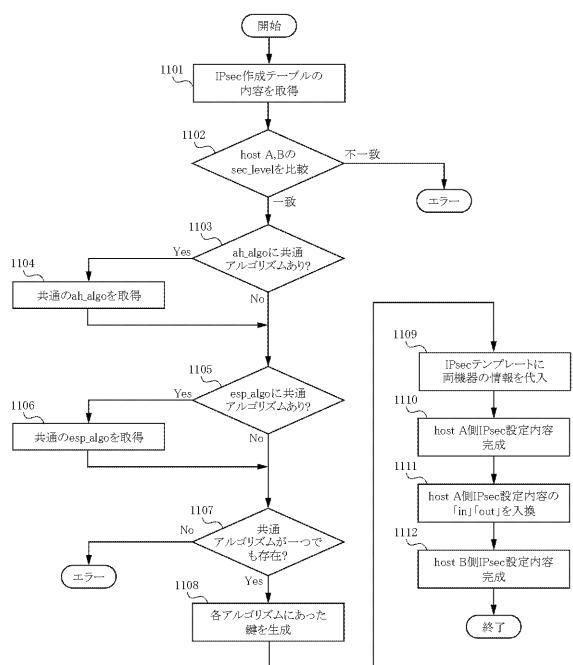
【図7】



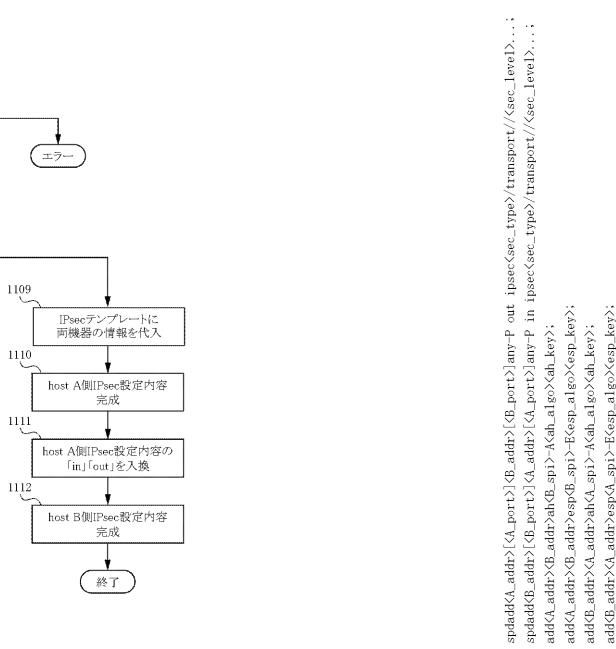
【図8】



【図9】



【図10】



【図 11】

```

<ipsec-response>
  <ipsec-data>
    spadd 2002:200::1[46127]3fe:514::1[180].any-p out ipsec esp/transport//require ah/transport//require;
    spadd 3fe:514::1[80]2002:200::1[46127].any-p in ipsec esp/transport//require ah/transport//require;
    add 2002:200::1 3fe:514::1 ah 0x44c-A hmac-sha1 0xface395fc73720e03d43ef232d5a2630ce47;
    add 2002:200::1 3fe:514::1 esp 0x44c-E 3des-cbc 0x2630e4749b0a8e117c5322cd45defc94cc39efcf7372b;
    add 3fe:514::1 2002:200::1 ah 0x834-A hmac-sha1 0x94ace395fc73720e03d43ef232d5a2630ce47;
    add 3fe:514::1 2002:200::1 esp 0x835-B 3des-cbc 0x2630e4749b0a8e117c3f22cd45defc94ace39efcf7372b;
  </ipsec-data>
</ipsec-response>

```

【手続補正書】

【提出日】平成17年2月16日(2005.2.16)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【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。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正の内容】

【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。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0033

【補正方法】変更

【補正の内容】

【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。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0042

【補正方法】変更

【補正の内容】

【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のレスポンスマ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に対し送信する。この402のレスポンスマッセージとしては、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、レスポンスマッセージ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。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0068

【補正方法】変更

【補正の内容】

【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:51
4 :: 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。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0072

【補正方法】変更

【補正の内容】

【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 が読出しができるように、ROM 1502、HD1507、あるいは FD1508 に格納されたプログラムの一部を示す。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0073

【補正方法】変更

【補正の内容】

【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。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0079

【補正方法】変更

【補正の内容】

【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。

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) 5K033 AA08 CC01 DA01 DB12