(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2012-175121
(P2012-175121A)
(43)公開日　平成24年9月10日(2012.9.10)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	2C061
H04L 12/28	(2006.01)	H04L	12/28	200M	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5J104
G06F 3/12	(2006.01)	G06F	3/12	A	5K033
B41J 29/00	(2006.01)	B41J	29/00	Z	

審査請求 未請求　請求項の数 5　ＯＬ　（全 12 頁）　最終頁に続く

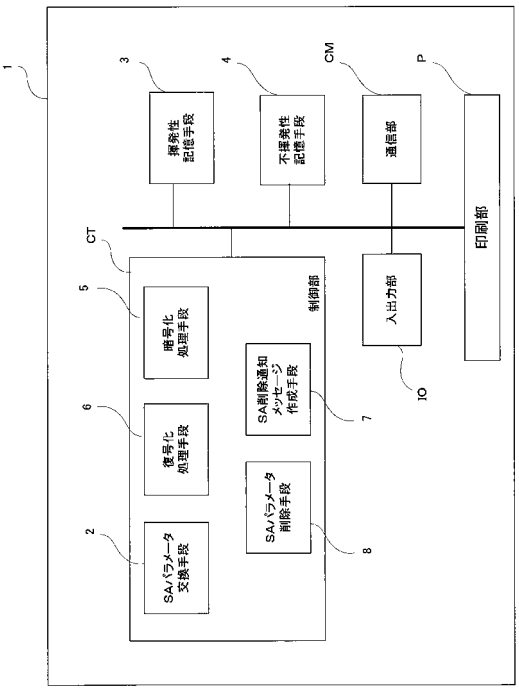
(21)出願番号　特願2011-31720 (P2011-31720)
(22)出願日　平成23年2月17日 (2011.2.17)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100095728
弁理士　上柳　雅誉
(74)代理人　100107261
弁理士　須澤　修
(74)代理人　100127661
弁理士　宮坂　一彦
(72)発明者　緒方　英昭
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
(72)発明者　▲高▼橋　陽一
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

最終頁に続く

(54)【発明の名称】印刷装置及び印刷装置のＳＡ確立方法

(57)【要約】
【課題】ＩＰｓｅｃ通信を迅速に再開させることができる印刷装置及び印刷装置のＳＡ確立方法を提供する。
【解決手段】本発明の印刷装置１及び印刷装置１のＳＡ確立方法においては、ＳＡ削除パラメータ・セットが不揮発性記憶部４に恒久的に保存されている。また、揮発性記憶部３にＳＡパラメータ・セットが保存されておらず、かつ、不揮発性記憶部４にＳＡ削除パラメータ・セットが保存されている状態になった場合に、ＳＡ削除通知メッセージ作成手段７がＳＡ削除パラメータ・セットに基づいて作成したＳＡ削除通知メッセージをＳＡパラメータ交換手段２が相手側通信装置１０に対して送信するようになっている。
【選択図】図１



【特許請求の範囲】
【請求項１】
ＩＰｓｅｃ通信が可能な印刷装置であって、
相手側通信装置との間でＩＰｓｅｃ通信を行うための各種パラメータとなるＳＡ（セキュリティ・アソシエーション）パラメータ・セットを相互に交換することよりセキュア化された仮想通信路であるＳＡの構築及び削除を行うＳＡパラメータ交換手段と、
前記ＳＡパラメータ・セットの一部であって前記ＳＡの削除に用いるＳＡ削除パラメータ・セットを保存する不揮発性記憶手段と、
前記印刷装置を初期化するときに、前記不揮発性記憶手段に前記ＳＡ削除パラメータ・セットが保存されていれば、前記ＳＡの削除を依頼するためのＳＡ削除通知メッセージを、前記不揮発性記憶手段に保存された前記ＳＡ削除パラメータ・セットに基づいて作成するＳＡ削除通知メッセージ作成手段と、を備え、
前記作成されたＳＡ削除通知メッセージが前記相手側通信装置へ送信されることを特徴とする印刷装置。
【請求項２】
前記ＳＡ削除パラメータ・セットは、少なくとも、ＩＳＡＫＭＰ＿ＳＡパラメータである相手ＩＰアドレス、ＩＳＡＫＭＰ＿ＳＡ識別子、暗号化アルゴリズム及び暗号鍵並びにＩＰｓｅｃ＿ＳＡパラメータであるＩＰｓｅｃ＿ＳＡ識別子により、構成されている
ことを特徴とする請求項１に記載の印刷装置。
【請求項３】
前記ＳＡ削除通知メッセージの送信後、前記不揮発性記憶手段から前記ＳＡ削除パラメータ・セットを削除するＳＡパラメータ削除手段を、さらに備える
ことを特徴とする請求項１または請求項２に記載の印刷装置。
【請求項４】
前記ＳＡ削除パラメータ・セットの作成後であってその保存前に、前記ＳＡパラメータ・セットに係る暗号化アルゴリズムとは異なる暗号化アルゴリズムを用いた暗号化処理を前記ＳＡ削除パラメータ・セットに対して行う暗号化処理手段と、
前記ＳＡ削除通知メッセージの作成前に、前記暗号化処理された前記ＳＡ削除パラメータ・セットの復号化処理を行う復号化処理手段と
をさらに備えることを特徴とする請求項１から請求項３のいずれか１項に記載の印刷装置。
【請求項５】
相手側通信装置と印刷装置との間でＩＰｓｅｃ通信を用いたセキュア通信を行うための各種パラメータとなるＳＡ（セキュリティ・アソシエーション）パラメータ・セットを相互に交換することによりセキュア化された仮想通信路であるＳＡを前記相手側通信装置と前記印刷装置との間に構築するＳＡ構築行程と、
前記ＳＡ構築行程において交換された前記ＳＡパラメータ・セットを前記印刷装置に設けられた揮発性記憶手段に一時的に保存する第１の記憶行程と、
前記ＳＡパラメータ・セットの一部であって前記ＳＡの削除に用いるＳＡ削除パラメータ・セットを前記印刷装置に設けられた不揮発性記憶手段に保存する第２の記憶行程と、
前記印刷装置を初期化するときに、前記ＳＡ削除パラメータ・セットが前記不揮発性記憶手段に保存されていれば、前記印刷装置から前記相手側通信装置に対して前記ＳＡの削除を依頼するために送信されるＳＡ削除通知メッセージを前記ＳＡ削除パラメータ・セットに基づいて作成するＳＡ削除通知メッセージ作成行程と、
前記作成されたＳＡ削除通知メッセージが前記相手側通信装置へ送信される送信工程とを備えていることを特徴とする印刷装置のＳＡ確立方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、印刷装置及び印刷装置のＳＡ確立方法に係り、特に、ＩＰｓｅｃ通信に対応

するプリンタに好適に利用できる印刷装置及び印刷装置のＳＡ確立方法に関する。
【背景技術】
【０００２】
従来の印刷装置においては、外部のパーソナル・コンピュータなどの相手側通信装置と通信する際、セキュアなＩＰ通信の一例であるＩＰｓｅｃ通信が用いられている。ＩＰｓｅｃ通信の利点は、盗聴・改ざん・なりすまし・否認の脅威を防ぐため、暗号化、署名、認証といったセキュリティ関連手法を上位プロトコルの変更をせずに利用できる点にある。このセキュアなＩＰ通信を実現するため、ＩＰｓｅｃ通信においては、ＡＨ（ＩＰ認証ヘッダ）、ＥＳＰ（ＩＰ暗号化ペイロード）及びＩＫＥ（インターネット鍵交換）と称される３つのプロトコル、鍵管理やセキュアプロトコルを使うためのつながり又はセキュアな仮想通信路といった意味のＳＡ（セキュリティ・アソシエーション）並びに認証及び暗号化アルゴリズムといった技術が用いられる。
【０００３】
従来の印刷装置１０１は、図５に示すように、相手側通信装置１１０とＩＰｓｅｃ通信を行う際にＳＡを生成するため、ＩＫＥプロトコルを使用する（時間Ｔ１００→時間Ｔ１０１：ＩＫＥ＿ＳＡパラメータ交換中）。このＩＫＥプロトコルを利用するのは、認証用のセッション鍵（ＨＭＡＣ）と暗号化用のセッション鍵のこれら両方の鍵の生成、交換、更新が自動で行われるからである。
【０００４】
ＩＫＥによるＳＡの生成行程においては、フェーズ１とフェーズ２の２ステップがある。フェーズ１においては、ＳＡ送信側（イニシエータ）となる相手側通信装置１１０とＳＡ受信側（レスポンダ）となる印刷装置１０１との間においてＩＳＡＫＭＰ＿ＳＡパラメータの一群であるＩＳＡＫＭＰ＿ＳＡパラメータ・セットを相互に交換することにより、ＩＳＡＫＭＰ＿ＳＡを生成する。また、フェーズ２においては、暗号化や認証に用いられる鍵を含むＩＰｓｅｃ＿ＳＡパラメータの一群であるＩＰｓｅｃ＿ＳＡパラメータ・セットを、フェーズ１において生成されたＩＳＡＫＭＰ＿ＳＡを介して相互に交換することにより、いわゆるＳＡと称されるＩＰｓｅｃ＿ＳＡを生成する。
【０００５】
なお、図５においては、透明横長円筒ｖｒ１を用いてＩＳＡＫＭＰ＿ＳＡによる通信セキュア化を視覚的に表現しており、透明横長円筒ｖｒ２を用いてＩＰｓｅｃ＿ＳＡによる通信セキュア化を視覚的に表現している。また、
【０００６】
そして、このＩＰｓｅｃ＿ＳＡを用いてＩＰｓｅｃパケットの送受信を行うことにより、印刷関連データのセキュア通信を実現することができる（時間Ｔ１０１→時間Ｔ１０２：セキュア通信中）。
【０００７】
また、ＩＰｓｅｃ通信の安全性を高めるため、ＳＡには有効期限が設けられている（時間Ｔ１００→時間Ｔ１０４：ＳＡ有効期限）。この有効期限が経過した場合、今まで使用されたＳＡパラメータ・セットを互いに消去し（時間Ｔ１０４→時間Ｔ１０５：旧ＳＡ消去中）、ＩＰｓｅｃ＿ＳＡパラメータ・セットに含まれる暗号鍵を再設定することにより、相手側通信装置１１０及び従来の印刷装置１０１は自動的にＳＡの再構築を行う（時間Ｔ１０５→時間Ｔ１０６：ＩＫＥ＿ＳＡパラメータ交換中（ＳＡ再構築））。
【０００８】
ここで、図示はしないが、この有効期限が経過する前であっても相手側通信装置１１０又は従来の印刷装置１０１のいずれか一方が正常に終了又は再起動する際、正常に終了又は再起動する一方の装置から他方の装置に対してＳＡ削除通知メッセージを送信し、今まで使用したＳＡを互いに消去することにより、ＩＰｓｅｃ通信の安全性を低下させる一因となるＳＡの再利用を防止していた（特許文献１の背景技術を参照）。
【先行技術文献】
【特許文献】

【０００９】
【特許文献１】特開２００９－２１９１０６号公報
【発明の概要】
【発明が解決しようとする課題】
【００１０】
しかしながら、従来の印刷装置１０１においては、その印刷装置１０１が停電などの理由により正常に終了せずに突如終了した場合（時間Ｔ１０２：印刷装置１０１の突如終了時）、印刷装置１０１をすぐに再起動させたとしても（時間Ｔ１０３：印刷装置１０１の再起動時）、ＩＰｓｅｃ通信を迅速に再開させることができないという問題があった（時間Ｔ１０２→時間Ｔ１０５：ＩＰｓｅｃ通信不能中）。
【００１１】
この問題は、印刷装置１０１の突如終了によって印刷装置１０１が保有するＳＡパラメータ・セットが消去してしまうにもかかわらず相手側通信装置１１０が保有するＳＡパラメータ・セットは消去されていないため（時間Ｔ１０２→時間Ｔ１０３：印刷装置１０１の電源切断中）、相手側通信装置１１０のＳＡパラメータ・セットの有効期限が経過するまで相手側通信装置１１０がＩＰｓｅｃ通信を回復させようとそのＳＡパラメータ・セットを印刷装置１０１に送り続けることに起因する（時間Ｔ１０３→時間Ｔ１０４：相手側通信装置１１０によるＳＡパラメータ送信中）。
【００１２】
ＩＰｓｅｃ通信を迅速に再開させるためには、ＳＡパラメータ・セットからＳＡの消去に必要なＳＡ削除パラメータ・セットを選択し、そのＳＡ削除パラメータ・セットに基づいて作成されたＳＡ削除通知メッセージを印刷装置１０１から相手側通信装置１１０に送信すればよい。しかし、印刷装置１０１の突如終了時にＳＡパラメータ・セットは消えてしまっているため、印刷装置１０１の再起動後にＳＡ削除通知メッセージを作成することはできない。
【００１３】
そこで、本発明はこれらの点に鑑みてなされたものであり、ＩＰｓｅｃ通信を迅速に再開させることができる印刷装置及び印刷装置のＳＡ確立方法を提供することを本発明の目的としている。
【課題を解決するための手段】
【００１４】
本発明の一つの実施態様に従うＩＰｓｅｃ通信が可能な印刷装置は、相手側通信装置との間でＩＰｓｅｃ通信を行うための各種パラメータとなるＳＡ（セキュリティ・アソシエーション）パラメータ・セットを相互に交換することよりセキュア化された仮想通信路であるＳＡの構築及び削除を行うＳＡパラメータ交換手段と、前記ＳＡパラメータ・セットの一部であって前記ＳＡの削除に用いるＳＡ削除パラメータ・セットを保存する不揮発性記憶手段と、前記印刷装置を初期化するときに、前記不揮発性記憶手段に前記ＳＡ削除パラメータ・セットが保存されていれば、前記ＳＡの削除を依頼するためのＳＡ削除通知メッセージを、前記不揮発性記憶手段に保存された前記ＳＡ削除パラメータ・セットに基づいて作成するＳＡ削除通知メッセージ作成手段と、を備え、前記作成されたＳＡ削除通知メッセージが前記相手側通信装置へ送信される。
【００１５】
これにより、不揮発性記憶手段にＳＡ削除パラメータ・セットが保存されているため、印刷装置が突然終了したことにより揮発性記憶手段に保存されていたＳＡパラメータ・セットが失われたときであっても、印刷装置の再起動後にＳＡ削除通知メッセージを送信することができる。
【００１６】
好適な実施形態では、前記ＳＡ削除パラメータ・セットは、少なくとも、ＩＳＡＫＭＰ＿ＳＡパラメータである相手ＩＰアドレス、ＩＳＡＫＭＰ＿ＳＡ識別子、暗号化アルゴリズム及び暗号鍵並びにＩＰｓｅｃ＿ＳＡパラメータであるＩＰｓｅｃ＿ＳＡ識別子により

、構成されていてもよい。
【００１７】
不揮発性記憶手段に保存するパラメータ・セットを上記のＳＡ削除パラメータ・セットに限定することにより、ＳＡ削除通知メッセージの送信を実現しつつ、不揮発性記憶手段への保存に必要な容量を最小限に抑えることができる。
【００１８】
好適な実施形態では、前記ＳＡ削除通知メッセージの送信後、前記不揮発性記憶手段から前記ＳＡ削除パラメータ・セットを削除するＳＡパラメータ削除手段を、さらに備えていてもよい。
【００１９】
これにより、すでに不要となったＳＡ削除パラメータ・セットが不揮発性記憶手段に蓄積することを防止できる。
【００２０】
好適な実施形態では、前記ＳＡ削除パラメータ・セットの作成後であってその保存前に、前記ＳＡパラメータ・セットに係る暗号化アルゴリズムとは異なる暗号化アルゴリズムを用いた暗号化処理を前記ＳＡ削除パラメータ・セットに対して行う暗号化処理手段と、前記ＳＡ削除通知メッセージの作成前に、前記暗号化処理された前記ＳＡ削除パラメータ・セットの復号化処理を行う復号化処理手段とをさらに備えていてもよい。
【００２１】
例えば暗号化ファイルシステム（ＥＦＳ）等の技術を利用することにより、ＳＡ削除パラメータ・セットに含まれる暗号鍵その他の重要なパラメータが漏洩したとしても、悪意のある第三者からＩＰｓｅｃ通信が妨害されることを防止することができる。
【発明の効果】
【００２２】
本発明の印刷装置及び印刷装置のＳＡ確立方法によれば、印刷装置の再起動後にＳＡ削除通知メッセージを送信することができるなどの種々の作用を生じるので、装置間の通信安全性を確保しつつ、ＩＰｓｅｃ通信を迅速に再開させることができる。
【図面の簡単な説明】
【００２３】
【図１】本発明の一実施形態に係る印刷装置の構成を示すブロック図
【図２】本実施形態の印刷装置と相手側通信装置との間の通信手順を示すシーケンス図
【図３】本実施形態の印刷装置におけるＳＡ削除パラメータ・セットの保存に関する処理手順を示すフローチャート
【図４】本実施形態の印刷装置におけるＳＡの削除処理に関する手順を示すフローチャート
【図５】従来の印刷装置と相手側通信装置との間の通信手順を示すシーケンス図
【発明を実施するための形態】
【００２４】
以下、本発明の印刷装置１及び印刷装置１のＳＡ確立方法をその一実施形態により説明する。はじめに、本実施形態の印刷装置１を以下に説明する。
【００２５】
本実施形態の印刷装置１は、図１に示すように、インクジェット・プリンタ・ヘッドなどの印刷部Ｐ、印刷部の制御を行うＣＰＵなどの制御部ＣＴ、揮発性メモリなどの揮発性記憶部３、不揮発性メモリなどの不揮発性記憶部４、ＷＡＮやＬＡＮなどを用いてインターネット通信を行う通信部ＣＭ及び手動入力や各種信号の入出力を行う入出力部ＩＯを有する。制御部ＣＴは、処理のコンピュータプログラムを実行することにより、以下に説明する複数の手段を実現する。すなわち、制御部ＣＴは、ＳＡパラメータ交換手段２、暗号化処理手段５、復号化処理手段６、ＳＡ削除通知メッセージ作成手段７及びＳＡパラメータ削除手段８を備えている。
【００２６】

ＳＡパラメータ交換手段２は、ＳＡ（セキュリティ・アソシエーション）パラメータ・セットを相互に交換することより、ＳＡの構築及び削除を行う手段であり、従来の印刷装置１０１に設けられたＳＡ生成手段と同様のものである。

【００２７】

ＩＰｓｅｃ通信においては、従来と同様、ＡＨ（ＩＰ認証ヘッダ）、ＥＳＰ（ＩＰ暗号化ペイロード）及びＩＫＥ（インターネット鍵交換）の３つのプロトコル、鍵管理やセキュアプロトコルを使うためのつながり又はセキュアな仮想通信路といった意味のＳＡ並びに認証及び暗号化アルゴリズムが用いられる。

【００２８】

また、ＩＫＥによるＳＡの生成手法においても、従来と同様、ＩＳＡＫＭＰ＿ＳＡを生成するフェーズ１とＩＰｓｅｃ＿ＳＡを生成するフェーズ２の２ステップがある。なお、図２においては、記号ｖｒ１が示す透明横長円筒を用いてＩＳＡＫＭＰ＿ＳＡによる通信セキュア化を視覚的に表現しており、記号ｖｒ２が示す透明横長円筒を用いてＩＰｓｅｃ＿ＳＡによる通信セキュア化を視覚的に表現している。

【００２９】

また、ＳＡパラメータ・セットは、相手側通信装置１０との間でＩＰｓｅｃ通信を用いたセキュア通信を行うための各種のパラメータである。ＳＡパラメータの一例としては、ＳＰＩ（セキュリティ・パラメータ・インデックス）、シーケンス番号カウンタ、オーバフローフラグ、リプレイ防御ウィンドウ、ＥＳＰ暗号化アルゴリズム、ＡＨ／ＥＳＰ認証アルゴリズム、暗号鍵、ＳＡ有効期間、ＩＰｓｅｃモード（トランスポートモード又はトンネルモード）、ステートフルフラグメントチェックフラグ、バイパスＤＦビット、Ｐａｔｈ＿ＭＴＵ、ＤＳＣＰ、バイパスＤＳＣＰ、トンネルモード始点アドレス、終点アドレスなどが挙げられる。

【００３０】

ここで、相手先のＩＰアドレス（以下、「相手ＩＰアドレス」という。）及び印刷装置１のＩＰアドレスはＩＰｓｅｃモードのフラグメント化に際してペイロード及びＡＨ／ＥＳＰヘッダの前にＩＰヘッダとして付与される。また、暗号化アルゴリズムについては、アルゴリズムそのものがパラメータとして含まれるよりも、識別子などにより既存の暗号化アルゴリズムを指定することが好ましい。そのため、ＳＡパラメータとして暗号化アルゴリズムを指定する場合、その代わりにその暗号化アルゴリズムを特定する識別子をＳＡパラメータとしてもよい。また、イニシエータ・クッキー（Ｃｏｏｋｉｅ）又はレスポンダ・クッキーは、イニシエータ側又はレスポンダ側のＩＳＡＫＭＰ＿ＳＡヘッダに含まれている。

【００３１】

揮発性記憶部３は、ＳＡパラメータ・セットを一時的に保存する手段である。つまり、揮発性記憶部３に保存されたＳＡパラメータ・セットは、印刷装置１の終了時に自動的に消去される。

【００３２】

不揮発性記憶部４は、ＳＡ削除パラメータ・セットを恒久的に保存する手段である。ＳＡ削除パラメータ・セットとは、ＳＡパラメータ・セットの一部であって、ＳＡの削除に用いられるパラメータの一群である。

【００３３】

本実施形態のＳＡ削除パラメータ・セットとしては、少なくとも、相手ＩＰアドレス、ＩＳＡＫＭＰ＿ＳＡ識別子（例えばクッキー）、暗号化アルゴリズム、暗号鍵、ＩＰｓｅｃ＿ＳＡ識別子（例えばＳＰＩ）が挙げられる。なお、相手ＩＰアドレス、ＩＳＡＫＭＰ＿ＳＡ識別子、暗号化アルゴリズムはＩＳＡＫＭＰに用いられるＳＡパラメータ（以下、「ＩＳＡＫＭＰ＿ＳＡパラメータ」という。）であり、ＩＰｓｅｃ＿ＳＡ識別子はＩＰｓｅｃに用いられるＳＡパラメータ（以下、「ＩＰｓｅｃ＿ＳＡパラメータ」という。）である。

【００３４】

この暗号化処理手段５は、ＳＡ削除パラメータ・セットに対して暗号化処理を行う手段である。この暗号化処理は、ＳＡ削除パラメータ・セットの作成後であってその保存前に行われる。また、この暗号化処理に用いられる暗号化アルゴリズムは、ＳＡパラメータ・セットに係る暗号化アルゴリズムとは異なるものを用いている。暗号化処理手法の具体例としては、例えば暗号化ファイルシステム（ＥＦＳ）などが挙げられる。

【００３５】

復号化処理手段６は、不揮発性記憶部４に保存されたＳＡ削除パラメータ・セットが暗号化処理されていた場合、ＳＡ削除通知メッセージの作成前にそのＳＡ削除パラメータ・セットの復号化処理を行う手段である。復号化処理手法は暗号化処理手法に基づいて選択すればよい。なお、暗号化処理手段５及び復号化処理手段６は、存在しなくてもよい任意の構成である。

【００３６】

ＳＡ削除通知メッセージ作成手段７は、不揮発性記憶部４に保存されたＳＡ削除パラメータ・セットに基づいて、ＳＡ削除通知メッセージを作成する手段である。ＳＡ削除通知メッセージとは、ＳＡパラメータ交換手段２が相手側通信装置１０に対して新たなＳＡを再構築する前に、その再構築以前のＳＡの削除を依頼するために送信するメッセージである。このＳＡ削除通知メッセージは、印刷装置１の正常終了時に揮発性記憶部３にＳＡパラメータ・セットが保存されている場合、又は、印刷装置１の突発的な終了後の再起動時において揮発性記憶部３にＳＡパラメータ・セットが保存されておらず、かつ、不揮発性記憶部４にＳＡ削除パラメータ・セットが保存されている状態になった場合のいずれかの場合に作成される。なお、ＳＡ削除通知メッセージの送信は、ＳＡパラメータの交換に関連するため、ＳＡパラメータ交換手段２により行われる。

【００３７】

ＳＡパラメータ削除手段８は、ＳＡ削除通知メッセージの送信後、不揮発性記憶部４から再構築以前のＳＡ削除パラメータ・セットを削除する手段である。

【００３８】

次に、本実施形態の印刷装置１のＳＡ確立方法を以下に説明する。

【００３９】

本実施形態の印刷装置１のＳＡ確立方法は、例えば本実施形態の印刷装置１により実現される。この印刷装置１のＳＡ確立方法は、ＳＡ構築行程、第１の記憶行程、暗号化処理行程、第２の記憶行程、復号化処理行程、ＳＡ削除通知メッセージ作成行程及びＳＡパラメータ削除行程を備えている。

【００４０】

はじめに、図２及び図３を用いて、本実施形態の印刷装置におけるＳＡ削除パラメータ・セットの保存に関する処理手順を説明する。

【００４１】

ＳＡ構築行程においては、図２及び図３に示すように、ＳＡパラメータ・セットを相互に交換し、相手側通信装置１０と印刷装置１との間にＳＡを構築する（図２の時間Ｔ０→時間Ｔ１：ＩＫＥ_ＳＡパラメータ交換中、図３のＳ０１→Ｓ０２）。従来と同様、ＳＡにはフェーズ１のＩＳＡＫＭＰ＿ＳＡ及びフェーズ２のＩＰｓｅｃ＿ＳＡがあり、その順にＳＡの確立が行われる。

【００４２】

また、第１の記憶行程は、図２及び図３に示すように、ＳＡ構築行程において交換されたＳＡパラメータ・セットを印刷装置１に設けられた揮発性記憶部３に一時的に保存する（図２の時間Ｔ０→時間Ｔ１：ＩＫＥ_ＳＡパラメータ交換中、図３のＳ０１）。

【００４３】

暗号化処理行程においては、ＳＡパラメータ・セットの一部であってＳＡの削除に用いるＳＡ削除パラメータ・セットに暗号化処理を行う（図３のＳ０３、Ｓ０４）。その時期は、ＳＡ削除パラメータ・セットの作成後であってその保存前である。なお、図３に示すように、印刷装置１に暗号化処理手段５が存在しない場合、暗号化処理を行わないことも

可能である（図３のＳ０３→Ｓ０５）。

【００４４】

第２の記憶行程は、図２及び図３に示すように、ＳＡ削除パラメータ・セットを印刷装置１の不揮発性記憶部４に恒久的に保存する（図２の時間Ｔ１、図３のＳ０５）。図２に示すとおり、ＳＡ削除パラメータ・セットは、少なくとも、ＩＳＡＫＭＰ＿ＳＡパラメータである相手ＩＰアドレス、ＩＳＡＫＭＰ＿ＳＡ識別子、暗号化アルゴリズム及び暗号鍵並びにＩＰｓｅｃ＿ＳＡパラメータであるＩＰｓｅｃ＿ＳＡ識別子により、構成されている。

【００４５】

ＩＰｓｅｃ＿ＳＡが生成されると、図２に示すように、それを介して印刷関連データが相手側通信装置１０及び印刷装置１の間でＩＰｓｅｃパケットを利用して送受信される（時間Ｔ１→時間Ｔ２：セキュア通信中）。

【００４６】

次に、図２及び図４を用いて、本実施形態の印刷装置における正常状態又はそれ以外の状態のＳＡの削除に関する処理手順を説明する。図４に示すＳＡの削除処理フローは、例えば、ＩＰｓｅｃ通信を正常に終了する場合、及び印刷装置を初期化するときに、その初期化処理中で実行される。

【００４７】

印刷装置１がＩＰｓｅｃ通信を正常に終了する場合、図４に示すように、印刷装置１の揮発性記憶部３にＳＡパラメータ・セットが記憶されているので（Ｓ１１）、ＳＡパラメータ・セットに基づいてＳＡ削除通知メッセージが作成される（Ｓ１２）。

【００４８】

しかし、図２に示すように、ＩＰｓｅｃ通信中に停電などの何らかの予定しない原因で印刷装置１が突如シャットダウンしてしまった場合（時間Ｔ２）、印刷装置１の揮発性記憶部３に記憶されたＳＡパラメータ・セットが消去されてしまうので、ＩＰｓｅｃ通信が途絶えてしまう（時間Ｔ２→時間Ｔ３：電源切断中）。そのため、図２に示すように印刷装置１を再起動したときは（時間Ｔ３）、その印刷装置の初期化処理の一部として図４に示す処理が実行される。つまり、その印刷装置１の揮発性記憶部３にＳＡパラメータ・セットが記憶されていないときは、不揮発性記憶部４にＳＡ削除パラメータ・セットが記憶されていないかを確かめる（Ｓ１１→Ｓ１３）。

【００４９】

不揮発性記憶部４にＳＡ削除パラメータ・セットが記憶されているときは、さらにＳＡ削除パラメータ・セットが暗号化されているか否かを判定し、暗号化されている場合は、その復号化処理を行う（Ｓ１４、Ｓ１５）。

【００５０】

ＳＡ削除通知メッセージ作成行程においては、図２及び図４に示すように、印刷装置１から相手側通信装置１０に対してＳＡ削除通知メッセージをＳＡ削除パラメータ・セットに基づいて作成する（図２の時間Ｔ３→時間Ｔ４：旧ＳＡ消去中、図４のＳ１６）。そして、ＳＡ削除通知メッセージが作成されると、ＳＡ削除通知メッセージはＳＡパラメータ交換手段２により相手側通信装置１０に送信される（図２の時間Ｔ３→時間Ｔ４：旧ＳＡ消去中、図４のＳ１７）。

【００５１】

ＳＡパラメータ削除行程においては、ＳＡ削除通知メッセージの送信後、不揮発性記憶部４から再構築以前のＳＡ削除パラメータ・セットを削除する（図２の時間Ｔ４→時間Ｔ５：ＩＫＥ_ＳＡパラメータ交換中（ＳＡ再構築）、図４のＳ１８）。

【００５２】

次に、本実施形態の印刷装置１及び印刷装置１のＳＡ確立方法の作用効果を説明する。

【００５３】

本実施形態の印刷装置１及び印刷装置１のＳＡ確立方法においては、ＳＡ削除パラメータ・セットが不揮発性記憶部４に恒久的に保存されており、揮発性記憶部３にＳＡパラメ

ータ・セットが保存されておらず、かつ、不揮発性記憶部４にＳＡ削除パラメータ・セットが保存されている状態になった場合に、ＳＡ削除通知メッセージ作成手段７がＳＡ削除パラメータ・セットに基づいて作成したＳＡ削除通知メッセージをＳＡパラメータ交換手段２が相手側通信装置１０に対して送信するようになっている。そのため、印刷装置１が停電等により突然シャットダウン（切断）したとしても、印刷装置１の再起動後であればＳＡの有効期限前であってもＳＡの再構築をすばやく行うことができる。

【００５４】

また、本実施形態の印刷装置１及び印刷装置１のＳＡ確立方法においては、不揮発性記憶部４に保存するパラメータ・セットを上記のＳＡ削除パラメータ・セットに限定することにより、ＳＡ削除通知メッセージの送信を実現しつつ、不揮発性記憶部４への保存に必要な容量を最小限に抑えることができる。

【００５５】

また、本実施形態の印刷装置１及び印刷装置１のＳＡ確立方法においては、ＳＡ削除通知メッセージの送信後、不揮発性記憶部４から再構築以前のＳＡ削除パラメータ・セットを削除するようになっている。そのため、新たなＳＡの消去に必要なＳＡ削除パラメータ・セットからみて不要な旧ＳＡ削除パラメータ・セットの蓄積を抑制することができる。

【００５６】

また、本実施形態の印刷装置１及び印刷装置１のＳＡ確立方法においては、ＳＡ削除パラメータ・セットの保存に際して暗号化処理を行い、ＳＡ削除通知メッセージの作成の際に復号化処理を行うようになっている。そのため、例えば暗号化ファイルシステム（ＥＦＳ）等の技術を利用することにより、ＳＡ削除パラメータ・セットに含まれる暗号鍵その他の重要なパラメータが漏洩したとしても、悪意のある第三者からＩＰｓｅｃ通信が妨害されることを防止することができる。

【００５７】

すなわち、本実施形態の印刷装置及び印刷装置のＳＡ確立方法によれば、印刷装置の再起動後にＳＡ削除通知メッセージを送信することができるなどの種々の作用を生じるので、装置間の通信安全性を確保しつつ、ＩＰｓｅｃ通信を迅速に再開させることができるという効果を奏する。

【００５８】

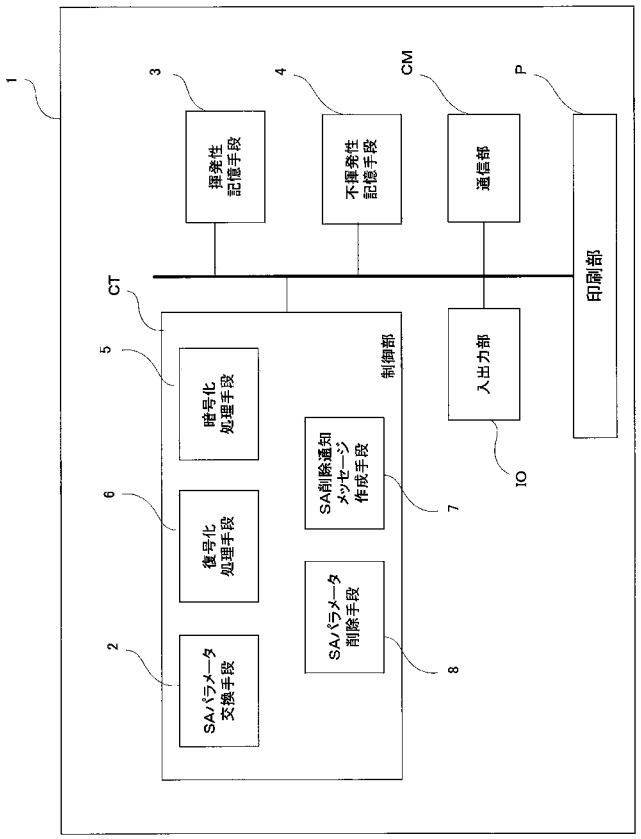
なお、本発明は、前述した実施形態などに限定されるものではなく、必要に応じて種々の変更が可能である。

【符号の説明】

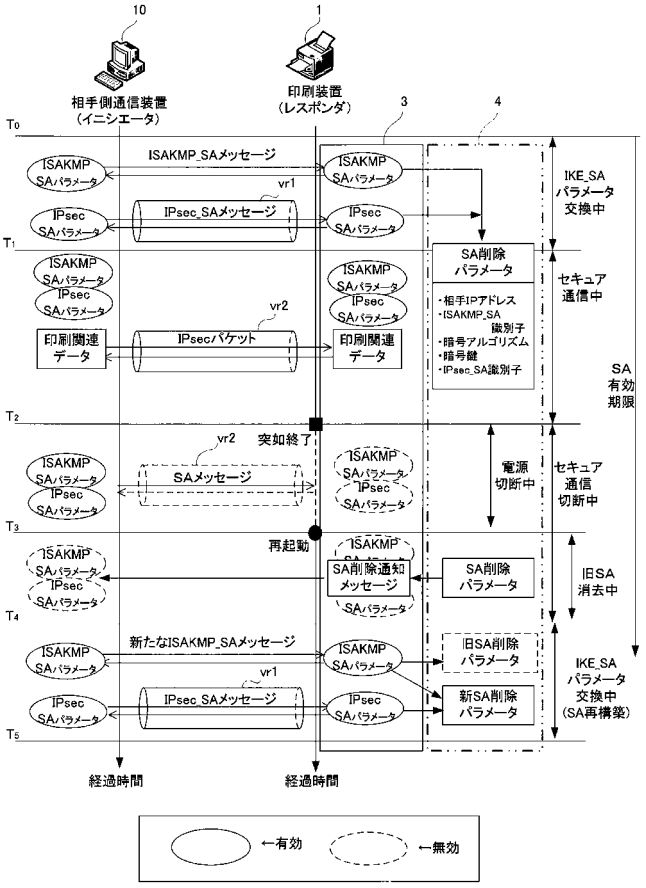
【００５９】

１　印刷装置
２　ＳＡパラメータ交換手段
３　揮発性記憶部
４　不揮発性記憶部
５　暗号化処理手段
６　復号化処理手段
７　ＳＡ削除通知メッセージ作成手段
８　ＳＡパラメータ削除手段
１０　相手側通信装置
ｖｒ１　ＩＳＡＫＭＰ＿ＳＡ
ｖｒ２　ＩＰｓｅｃ＿ＳＡ

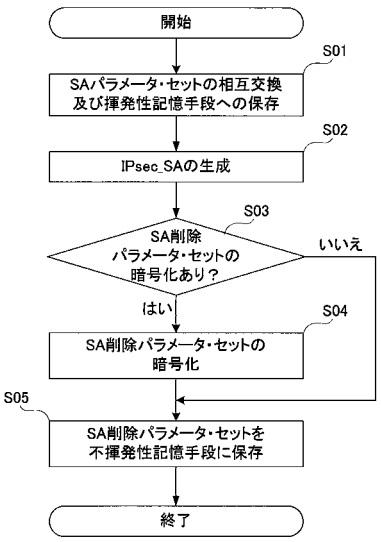
【図１】


1
3
4
CM
P
揮発性記憶手段
不揮発性記憶手段
通信部
印刷部
CT
制御部
5
暗号化処理手段
6
復号化処理手段
2
SAパラメータ交換手段
SA削除通知メッセージ作成手段
7
SAパラメータ削除手段
8
入出力部
IO

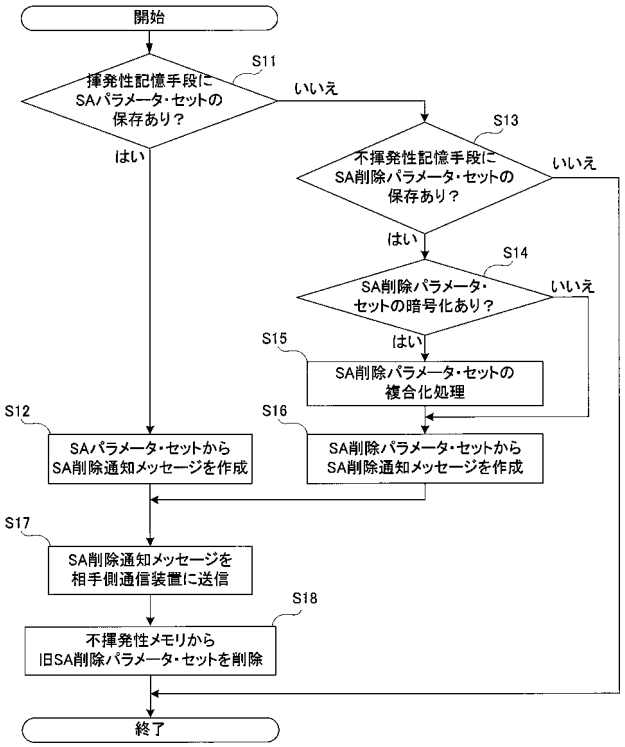
【図２】


10
1
相手側通信装置（イニシエータ）
印刷装置（レスポンダ）
3
4
T0
ISAKMP_SAメッセージ
ISAKMP SAパラメータ
IPsec SAパラメータ
vr1
IPsec_SAメッセージ
IKE_SA パラメータ 交換中
T1
SA削除パラメータ
・相手IPアドレス
・ISAKMP_SA識別子
・暗号アルゴリズム
・暗号鍵
・IPsec_SA識別子
セキュア通信中
印刷関連データ
vr2
IPsecパケット
SA有効期限
T2
突如終了
SAメッセージ
電源切断中
セキュア通信切断中
T3
再起動
SA削除通知メッセージ
旧SA消去中
T4
新たなISAKMP_SAメッセージ
旧SA削除パラメータ
新SA削除パラメータ
IKE_SA パラメータ 交換中 (SA再構築)
T5
経過時間
経過時間
←有効
←無効

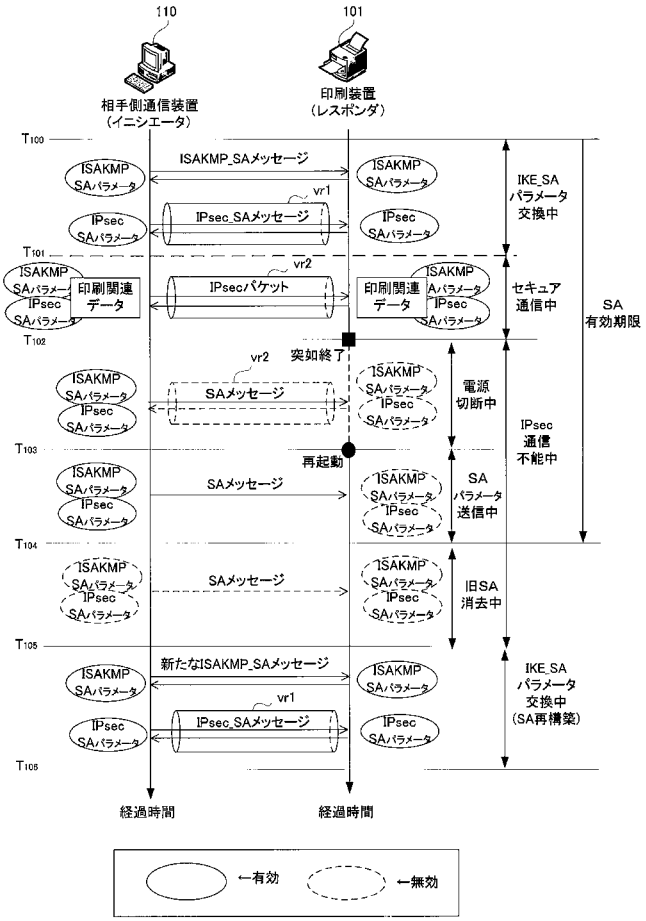
【図３】


開始
S01
SAパラメータ・セットの相互交換及び揮発性記憶手段への保存
S02
IPsec_SAの生成
S03
SA削除パラメータ・セットの暗号化あり？
いいえ
はい
S04
SA削除パラメータ・セットの暗号化
S05
SA削除パラメータ・セットを不揮発性記憶手段に保存
終了

【図４】


開始
S11
揮発性記憶手段にSAパラメータ・セットの保存あり？
いいえ
はい
S13
不揮発性記憶手段にSA削除パラメータ・セットの保存あり？
いいえ
はい
S14
SA削除パラメータ・セットの暗号化あり？
いいえ
はい
S15
SA削除パラメータ・セットの複合化処理
S12
SAパラメータ・セットからSA削除通知メッセージを作成
S16
SA削除パラメータ・セットからSA削除通知メッセージを作成
S17
SA削除通知メッセージを相手側通信装置に送信
S18
不揮発性メモリから旧SA削除パラメータ・セットを削除
終了

【図５】


110
101
相手側通信装置
（イニシエータ）
印刷装置
（レスポンダ）
T100
T101
T102
T103
T104
T105
T106
ISAKMP_SAメッセージ
IPsec_SAメッセージ
IPsecパケット
SAメッセージ
SAメッセージ
新たなISAKMP_SAメッセージ
IPsec_SAメッセージ
vr1
vr2
vr2
vr1
ISAKMP SAパラメータ
IPsec SAパラメータ
印刷関連データ
突如終了
再起動
IKE_SA パラメータ 交換中
セキュア 通信中
SA 有効期限
電源 切断中
IPsec 通信 不能中
SA パラメータ 送信中
旧SA 消去中
IKE_SA パラメータ 交換中 （SA再構築）
経過時間
経過時間
←有効
←無効

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
Ｂ４１Ｊ 29/38	***(2006.01)***	Ｂ４１Ｊ	29/38	Ｚ	
Ｈ０４Ｌ 9/14	***(2006.01)***	Ｈ０４Ｌ	9/00	６４１	

Ｆターム(参考) 2C061 AP01 HJ08 HN15 HN21 HP00
5B285 AA04 BA07 CA42 DA05
5J104 AA01 AA16 AA32 EA04 EA18 JA03 NA02 NA06 NA37 PA07
5K033 AA08 CB01 CC01 DA13 DB12 EC01