(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2005-115519
(P2005-115519A)
(43)公開日　平成17年4月28日(2005.4.28)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 3/12	G06F 3/12	K	2C187
B41J 5/30	B41J 5/30	Z	5B021

審査請求 未請求　請求項の数 14　ＯＬ　（全 13 頁）

(21)出願番号　特願2003-346865 (P2003-346865)
(22)出願日　平成15年10月6日 (2003.10.6)

(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　100081880
弁理士　渡部　敏彦
(72)発明者　境　秀樹
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)　2C187 AC07 AC08 AD03 AD04 AE07 AE13 BF26 BH10 BH27 DB33 DD02 GB08 GD01
5B021 AA01 NN00

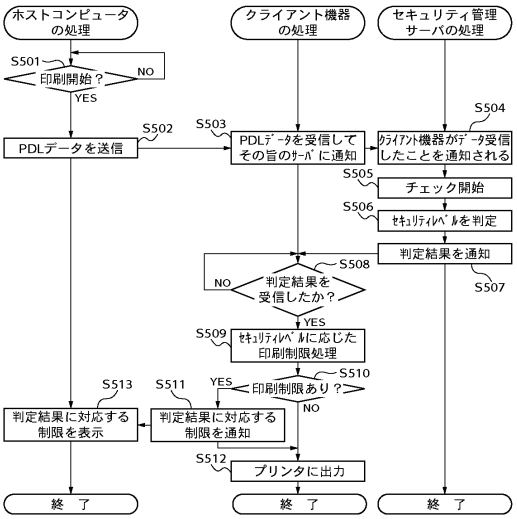
(54)【発明の名称】ネットワーク印刷システム、セキュリティ診断装置、データ処理装置、セキュリティ対策実施方法およびプログラム

(57)【要約】

【課題】　ネットワーク管理者の負荷を軽減して、ネットワーク上の印刷機能の不正使用に対する対策を実施することができるネットワーク印刷システムを提供する。

【解決手段】　クライアント機器１０２は、ホストコンピュータ１０４からのＰＤＬデータを受信すると、その旨をセキュリティ管理サーバ１０１に通知する（ステップＳ５０３）。この通知を受けたセキュリティ管理サーバ１０１においては、クライアント機器１０２のセキュリティレベルがチェックされ、そのセキュリティレベルが判定される（ステップＳ５０６）。この判定結果はクライアント機器１０２に通知され（ステップＳ５０７）、クライアント機器１０２は、上記判定結果に対応する制限に基づいて印刷処理を制御する（ステップＳ５０９）。

【選択図】　図５



【特許請求の範囲】
【請求項１】
印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワーク上に構築されるネットワーク印刷システムであって、
前記ネットワークのセキュリティ状態を診断するためのセキュリティ診断装置を備え、
前記セキュリティ診断装置は、前記データ処理装置から、前記ホストコンピュータからの印字データを受信した旨を示す通知を受け取ると、前記データ処理装置が前記印刷機能を用いて前記印字データを印刷出力する前に、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定手段と、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知手段とを有し、
前記データ処理装置は、前記セキュリティ診断装置の前記セキュリティレベル通知手段から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限手段を有することを特徴とするネットワーク印刷システム。
【請求項２】
印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワークのセキュリティ状態を診断するためのセキュリティ診断装置であって、
前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定手段と、
前記ホストコンピュータからの印字データを受信した旨を示す通知を前記データ処理装置から受け取るのに対して、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知手段と
を有することを特徴とするセキュリティ診断装置。
【請求項３】
前記判定手段は、前記ネットワークのセキュリティを突破するための動作を試行し、該試行の結果に基づいて前記ネットワークのセキュリティレベルを判定することを特徴とする請求項２記載のセキュリティ診断装置。
【請求項４】
前記判定手段は、前記試行の結果に基づいて、予め設定されている複数段階のセキュリティレベルのうち、いずれのセキュリティレベルにあるかを判定することを特徴とする請求項２記載のセキュリティ診断装置。
【請求項５】
印刷機能を有し、ホストコンピュータとネットワークを介して通信可能なデータ処理装置であって、
前記ホストコンピュータから印字データを受信すると、印字データを受信した旨を、前記ネットワークのセキュリティレベルを判定するセキュリティ診断装置に通知する通知手段と、
前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限手段と
を有することを特徴とするデータ処理装置。
【請求項６】
前記印刷制限手段は、前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、印刷部数、用紙サイズ、印字モードのうちの少なくとも１つを制限することを特徴とする請求項５記載のデータ処理装置。
【請求項７】
前記印刷制限手段により前記印字データの印刷に制限をかけた場合、その旨を前記ホストコンピュータに通知する通知手段を有することを特徴とする請求項５または６記載のデータ処理装置。
【請求項８】
印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワーク

のセキュリティを診断するセキュリティ診断装置を用いて、前記ネットワーク上に構築されるネットワーク印刷システムのセキュリティ対策を実施するためのセキュリティ対策実施方法であって、
前記セキュリティ診断装置は、
前記データ処理装置から、前記ホストコンピュータからの印字データを受信した旨を示す通知を受け取ると、前記データ処理装置が前記印刷機能を用いて前記印字データを印刷出力する前に、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定工程と、
前記セキュリティレベル判定工程により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知工程とを有し、
前記データ処理装置は、
前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限工程を有することを特徴とするセキュリティ対策実施方法。
【請求項９】
前記セキュリティレベル判定工程では、前記ネットワークのセキュリティを突破するための動作を試行し、該試行の結果に基づいて前記ネットワークのセキュリティレベルを判定することを特徴とする請求項８記載のセキュリティ対策実施方法。
【請求項１０】
前記セキュリティレベル判定工程では、前記試行の結果に基づいて、予め設定されている複数段階のセキュリティレベルのうち、いずれのセキュリティレベルにあるかを判定することを特徴とする請求項９記載のセキュリティ対策実施方法。
【請求項１１】
前記データ処理装置の印刷制限工程では、前記セキュリティ診断装置から通知されたセキュリティレベルに応じて印刷部数、用紙サイズ、印字モードなどを制限することを特徴とする請求項８ないし１０のいずれか１つに記載のセキュリティ対策実施方法。
【請求項１２】
前記データ処理装置は、前記受信した印字データの印刷に制限をかけた場合、その旨を前記ホストコンピュータに通知する通知工程を有することを特徴とする請求項８ないし１１のいずれか１つに記載のセキュリティ対策実施方法。
【請求項１３】
印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワークのセキュリティ対策に用いられる情報処理装置により実行されるプログラムであって、
前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定モジュールと、
前記ホストコンピュータからの印字データを受信した旨を示す通知を前記データ処理装置から受け取るのに対して、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知モジュールと
を有することを特徴とするプログラム。
【請求項１４】
印刷機能を有し、ホストコンピュータとネットワークを介して接続されるデータ処理装置により実行されるプログラムであって、
前記ホストコンピュータから印字データを受信すると、印字データを受信した旨を、前記ネットワークのセキュリティレベルを判定するセキュリティ診断装置に通知する通知モジュールと、
前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限モジュールと
を有することを特徴とするプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、プリンタ機能を有するクライアント装置およびホストコンピュータが接続されるネットワーク上に構築されるネットワーク印刷システム、それに用いられるセキュリティ診断装置、データ処理装置、セキュリティ対策実施方法およびプログラムに関する。
【背景技術】
【０００２】
従来のネットワークなどに接続され、複数のホストに共有されるプリンタにおいては、いずれかのホストから印字用データを受信すると、この印字用データで指定された部数、紙サイズ、印字モードに応じた印字出力が行われる（例えば、特許文献１）。
【特許文献１】特開平０７－０６８８４９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
近年、インターネットなどの世界的なネットワーク網の発展に伴い、ネットワークのセキュリティホールを攻撃する犯罪の件数が増加し、現状において、その攻撃対象の主なものとしては、サーバ、クライアントコンピュータである。
【０００４】
また、昨今、ネットワークに接続された（IP アドレスを持つ）クライアントとして、プリンタ機能を有する機器が増加しつつある。このような機器を収容するネットワーク環境下においては、ホスト同様に、上記のようなプリンタ機能を有する機器に対してセキュリティ対策を実施しないと、ネットワークを介して無用な文書の大量印刷が行われ、また、プリントに課金するような環境においては、不正に印刷が行われ、この不正な印刷の料金がユーザに請求されるなどの新たな犯罪（悪戯）の発生が考えられる。よって、セキュリティ対策が必須となる。
【０００５】
しかしながら、日々変化し、そして進化するネットワーク環境において、上記のような犯罪行為に対抗するために、ネットワーク管理者が常にホスト、プリンタなどに対して最新のセキュリティレベルを維持するようにすればよいが、これは管理者に大きな負荷を掛けることになる。
【０００６】
本発明の目的は、ネットワーク管理者の負荷を軽減して、ネットワーク上の印刷機能の不正使用に対する対策を実施することができるネットワーク印刷システム、セキュリティ診断装置、データ処理装置、セキュリティ対策実施方法およびプログラムを提供することにある。
【課題を解決するための手段】
【０００７】
本発明は、上記目的を達成するため、印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワーク上に構築されるネットワーク印刷システムであって、前記ネットワークのセキュリティ状態を診断するためのセキュリティ診断装置を備え、前記セキュリティ診断装置は、前記データ処理装置から、前記ホストコンピュータからの印字データを受信した旨を示す通知を受け取ると、前記データ処理装置が前記印刷機能を用いて前記印字データを印刷出力する前に、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定手段と、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知手段とを有し、前記データ処理装置は、前記セキュリティ診断装置の前記セキュリティレベル通知手段から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限手段を有することを特徴とする。
【０００８】
本発明は、上記目的を達成するため、印刷機能を有するデータ処理装置およびホストコ

ンピュータが接続されるネットワークのセキュリティ状態を診断するためのセキュリティ診断装置であって、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定手段と、前記ホストコンピュータからの印字データを受信した旨を示す通知を前記データ処理装置から受け取るのに対して、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知手段とを有することを特徴とする。

【０００９】

本発明は、上記目的を達成するため、印刷機能を有し、ホストコンピュータとネットワークを介して通信可能なデータ処理装置であって、前記ホストコンピュータから印字データを受信すると、印字データを受信した旨を、前記ネットワークのセキュリティレベルを判定するセキュリティ診断装置に通知する通知手段と、前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限手段とを有することを特徴とする。

【００１０】

本発明は、上記目的を達成するため、印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワークのセキュリティを診断するセキュリティ診断装置を用いて、前記ネットワーク上に構築されるネットワーク印刷システムのセキュリティ対策を実施するためのセキュリティ対策実施方法であって、前記セキュリティ診断装置は、前記データ処理装置から、前記ホストコンピュータからの印字データを受信した旨を示す通知を受け取ると、前記データ処理装置が前記印刷機能を用いて前記印字データを印刷出力する前に、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定工程と、前記セキュリティレベル判定工程により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知工程とを有し、前記データ処理装置は、前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限工程を有することを特徴とする。

【００１１】

本発明は、上記目的を達成するため、印刷機能を有するデータ処理装置およびホストコンピュータが接続されるネットワークのセキュリティ対策に用いられる情報処理装置により実行されるプログラムであって、前記ネットワークのセキュリティレベルを判定するセキュリティレベル判定モジュールと、前記ホストコンピュータからの印字データを受信した旨を示す通知を前記データ処理装置から受け取るのに対して、前記セキュリティレベル判定手段により判定された前記ネットワークのセキュリティレベルを前記データ処理装置に通知するセキュリティレベル通知モジュールとを有することを特徴とする。

【００１２】

本発明は、上記目的を達成するため、印刷機能を有し、ホストコンピュータとネットワークを介して接続されるデータ処理装置により実行されるプログラムであって、前記ホストコンピュータから印字データを受信すると、印字データを受信した旨を、前記ネットワークのセキュリティレベルを判定するセキュリティ診断装置に通知する通知モジュールと、前記セキュリティ診断装置から通知されたセキュリティレベルに応じて、前記印刷機能を用いた前記印字データの印刷に制限をかける印刷制限モジュールとを有することを特徴とする。

【発明の効果】

【００１３】

以上説明したように、本発明によれば、ネットワーク管理者の負荷を軽減して、ネットワーク上の印刷機能の不正使用に対する対策を実施することができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施の形態について図面を参照しながら説明する。

【００１５】

図１は本発明の一実施の形態に係る印刷システムの主要部構成を示すブロック図である。

【００１６】

本印刷システムは、図１に示すように、ネットワーク上に構築され、このネットワークにおいては、ホストコンピュータ１０４、クライアント機器１０２、他の複数のホストコンピュータ（図示せず）、複数のデバイス（図示せず）などがＬＡＮ（Local Area Network）１０５に接続されている。ここで、クライアント機器１０２は、プリンタ１０３が同じ筐体にあるような複写機（コピー機）、レーザビームプリンタ、インクジェットプリンタ、ＦＡＸ装置などの機器、またはプリンタ１０３を離脱可能に接続することができるホストコンピュータやパーソナルコンピュータであってもよい。クライアント機器１０２は、プリンタ１０３で印刷される印刷枚数、紙サイズ、印字モードを制御し、プリンタ１０３のステータスを後述するセキュリティ管理サーバ１０１に送信し、またプリンタ１０３を統括的に管理する。

【００１７】

プリンタ１０３は、ホストコンピュータ１０４からの印字データに基づいて、クライアント機器１０２を経由して展開されたイメージを記録用紙に印刷する。プリンタ１０３は、自身を特定するための機器番号を有しており、外部からの要求に応じて、当該機器番号を示すデータを転送することができる。

【００１８】

ＬＡＮ１０５は、クライアント機器１０２、ホストコンピュータ１０４などを接続するネットワークであり、通常は、オフィス内や所定の敷地内のネットワークに対応する。また、ＬＡＮ１０５には、ＷＡＮ（Wide Area Network）１０６が接続されている。ＷＡＮ１０６は、複数のＬＡＮが接続された広域なネットワークであり、複数のネットワークをさらに公衆網や専用回線等で相互接続したものである。これによって、遠隔にあるコンピュータ同士が、データのやり取りを行うことができる。

【００１９】

ＷＡＮ１０６には、セキュリティ管理サーバ１０１が接続されている。このセキュリティ管理サーバ１０１は、クライアント機器１０２からのデータに基づいて、クライアント機器１０２が接続されたネットワークのセキュリティレベルがどのような状態にあるかを判別し、プリンタ１０３のセキュリティを管理する。

【００２０】

なお、セキュリティ管理サーバ１０１は、ＬＡＮ１０５に接続されていてもよい。ただし、セキュリティ管理サーバ１０１は、ＷＡＮ１０６を介して、複数のＬＡＮと接続することにより、例えば、複数のオフィスや会社にそれぞれ置かれている複数のプリンタに対して、セキュリティ管理サービスを提供することができる。

【００２１】

次に、クライアント機器１０２とプリンタ１０３とが組み込まれている複写機について図２および図３を参照しながら説明する。図２は図１のクライアント機器１０２とプリンタ１０３とが組み込まれている複写機の外観図、図３は図２の複写機の制御構成を示すブロック図である。

【００２２】

クライアント機器１０２とプリンタ１０３とが組み込まれている複写機は、図２に示すように、画像入力デバイスであるスキャナ２０１、操作部２０２および画像出力デバイスであるプリンタ１０３を備える。

【００２３】

スキャナ２０１は、読み取る原稿をセットするトレイ２０３が設けられている原稿フィーダ２０４を有し、原稿フィーダ２０４から給送された原稿を照明し、ＣＣＤラインセンサ（図示せず）により上記原稿を走査することによって、原稿上の画像のラスターイメージデータを生成する。原稿の読み取りを行う際には、ユーザが原稿を原稿フィーダ２０４のトレイ２０３にセットして、操作部２０２から読み取りを指示する。上記読み取り指示

に応答して、装置全体を制御するＣＰＵ（図示せず）がスキャナ２０１に指示を与え、この指示に基づいて原稿フィーダ２０４からトレイ２０３上の原稿が１枚ずつフィードされる。そして、原稿フィーダ２０４から給送された原稿画像の読み取り動作が行われる。

【００２４】

プリンタ１０３は、ラスターイメージデータを用紙上の印刷する手段である。プリンタ１０３の印刷方式としては、感光体ドラムや感光体ベルトを用いた電子写真方式、微少ノズルアレイからインクを吐出して用紙上に直接画像を印字するインクジェット方式などがあるが、いずれの方式を用いてもよい。このプリンタ１０３の動作は、上記ＣＰＵからの指示によって起動される。プリンタ１０３は、異なる用紙サイズまたは異なる用紙向きを選択できるように複数の給紙段を有し、それぞれに対応する用紙カセット２０６，２０７，２０８が設けられている。また、印字された用紙を受ける排紙トレイ２０５が設けられている。

【００２５】

上記複写機に組み込まれているクライアント機器１０２は、図３に示すように、画像入力デバイスであるスキャナ２０１や画像出力デバイスであるプリンタ１０３を接続し、これらを制御する一方、ＬＡＮ１０５やＷＡＮ（公衆回線）１０６と接続され、これらを介して画像情報やデバイス情報の入出力を行うものである。

【００２６】

クライアント機器１０２は、プリンタ１０３を含むシステム全体を制御するコントローラとしての機能を実行するものである。クライアント機器１０２は、ＣＰＵ３０１を有し、ＣＰＵ３０１は、システムバス３０７を介して、ＲＡＭ３０２、ＲＯＭ３０３、ＨＤＤ（ハードディスク装置）３０４、画像バスＩ／Ｆ３０５、操作部Ｉ／Ｆ３０６、ネットワークＩ／Ｆ３０８およびモデム３０９と接続される。

【００２７】

ＲＡＭ３０２は、ＣＰＵ３０１の作業領域を提供するためのメモリであり、また、画像データを一時記憶するための画像メモリとしても使用される。ＲＯＭ３０３はブートＲＯＭであり、ＲＯＭ３０３には、システムのブートプログラムが格納されている。ＨＤＤ３０４には、システムソフトウェア、画像データなどが格納される。

【００２８】

操作部Ｉ／Ｆ３０６は、操作部（ＵＩ）２０２との間で入出力を行うためのインターフェースであり、操作部２０２に表示する画像データを操作部２０２に対して出力し、ユーザが操作部２０２を介して入力した情報を、ＣＰＵ３０１に伝送するなどの役割を果たす。

【００２９】

ネットワークＩ／Ｆ３０８は、ＬＡＮ１０５と接続され、ＬＡＮ１０６に対して情報の入出力を行う。モデム３０９は、ＷＡＮ（公衆回線）１０６と接続され、ＷＡＮ１０６に対して情報の入出力を行う。

【００３０】

画像バスＩ／Ｆ３０５は、システムバス３０７と画像データを高速で転送する画像バス３１０とを接続し、データ構造を変換するバスブリッジである。

【００３１】

画像バス３１０には、ＲＩＰ（ラスターイメージプロセッサ）３１１、デバイスＩ／Ｆ３１２、スキャナ画像処部３１３、プリンタ画像処理部３１４、画像回転部３１５および画像圧縮部３１６が接続されている。

【００３２】

ＲＩＰ３１１は、ＬＡＮ１５から受信されたＰＤＬコードをビットマップイメージに展開する。デバイスＩ／Ｆ３１２は、スキャナ２０１およびプリンタ１０３とクライアント機器１０２とを接続し、画像データの同期系／非同期系の変換を行う。スキャナ画像処理部３１３は、入力画像データに対し補正、加工、編集などを行う。プリンタ画像処理部３１４は、プリント出力画像データに対して、プリンタの補正、解像度変換などを行う。画

像回転部３１５は画像データの回転を行う。画像圧縮部３１６は、多値画像データに対してはJPEG圧縮伸長処理を行い、２値画像データに対してはJBIG, MMR, MHなどの圧縮伸長処理を行う。

【００３３】

次に、本実施の形態におけるプリンタ１０３に対するセキュリティ管理について図４を参照しながら説明する。図４は図１のプリンタ１０３に対するセキュリティ管理を実現するための機能構成を示す図である。

【００３４】

プリンタ１０３に対するセキュリティ管理は、図４に示すように、セキュリティ管理サーバ１０１とクライアント機器１０２により行われる。セキュリティ管理サーバ１０１は、機器構成情報管理部４０１、セキュリティチェックデータ格納部４０２、セキュリティ実行部４０３、セキュリティ基準格納部４０４およびセキュリティレベル判定部４０５を有し、これらは、予め保持されているプログラムを実行することによって構成されるものである。

【００３５】

機器構成情報管理部４０１は、セキュリティチェック対象となる機器の構成を示す情報を管理する。例えば、セキュリティチェック対象となる機器毎に、機器番号、オプションの有無、ネットワークアドレス（ＩＰアドレス）、所有者、設置場所などを示す情報がデータベース化されて管理される。セキュリティチェックデータ格納部４０２には、セキュリティチェック対象となる機器のセキュリティレベルをチェックするためのテストパターンが格納されている。セキュリティチェック実行部４０３は、セキュリティチェックデータ格納部４０２に格納されているテストパターンに基づいて機器のセキュリティレベルをチェックする。セキュリティ基準格納部４０４には、セキュリティレベルの判定において、ＯＫ（問題なし）とするかＮＧ（問題あり）とするかの尺度を示す情報が格納されている。例えば、ＯＫ（またはＮＧ）と判定するときのテストパターンやその許容範囲を示す情報が格納されている。セキュリティレベル判定部４０５は、セキュリティ基準格納部４０４に格納されているデータに基づいてセキュリティレベルの判定を行う。

【００３６】

クライアント機器１０２は、ユーザＩＤ格納部４０６、公開鍵／秘密鍵格納部４０７、機器特定情報格納部４０８、セキュリティ対応処理部４０９を有し、これらは、ＣＰＵ３０１がＨＤＤ３０４に格納されている対応プログラムを実行することによって構成されるものである。

【００３７】

ユーザＩＤ格納部４０６には、プリンタ１０３の所有者を識別するためのＩＤが格納されている。このＩＤは、セキュリティチェックのサービスを提供する提供先を特定するのに用いられる。公開鍵／秘密鍵格納部４０７には、セキュリティ管理サーバ１０１にデータを転送するときにこの転送データを暗号化するのに必要な公開鍵や秘密鍵などが格納されている。機器特定情報格納部４０８には、プリンタ１０３を識別するための情報、例えばプリンタ１０３の機器番号が格納されている。セキュリティ対応処理部４０９は、セキュリティ管理サーバ１０１から通知されたセキュリティレベルに応じて印刷処理の制限を行う。制限が行われた場合（セキュリティに問題がある場合）、その旨が、印字データ送信元のホストコンピュータ１０４に通知される。

【００３８】

次に、本実施の形態における印刷動作について図５を参照しながら説明する。図５は図１のネットワーク印刷システムの印刷動作の手順を示すフローチャートである。ここで、ステップＳ５０１，Ｓ５０２，Ｓ５１３は、ホストコンピュータ１０４による処理、スップＳ５０３，Ｓ５０８，Ｓ５０９，Ｓ５１０，Ｓ５１１，Ｓ５１２は、クライアント機器１０２による処理、ステップＳ５０４～Ｓ５０７は、セキュリティ管理サーバ１０１による処理である。これらの処理は、各ステップに対応するプログラムコードがそれぞれの装置のＣＰＵによって実行されることにより行われるものである。特に、ホストコンピュー

タ１０４による処理は、それに搭載されているプリンタドライバによるものである。
【００３９】
図５に示すように、まず、ホストコンピュータ１０４が、ユーザから印刷開始が指示されるのを監視する（ステップＳ５０１）。そして、印刷開始が指示されると、ホストコンピュータ１０４は、アプリケーションがディスプレイなどに表示する画像データをＰＤＬデータに変更し、このＰＤＬデータを、ＬＡＮ１０５を介してクライアント機器１０２へ送信する（ステップＳ５０２）。
【００４０】
次いで、クライアント機器１０２は、ホストコンピュータ１０４から送信されたＰＤＬデータを受信し、このＰＤＬデータを受信した旨を、ユーザＩＤ格納部４０６のＩＤ、公開鍵／秘密鍵格納部４０７の公開鍵を用いて、機器特定情報格納部４０８の機器番号とともにセキュリティ管理サーバ１０１に通知する（ステップＳ５０３）。そして、クライアント機器１０２は、セキュリティ管理サーバ１０１からの判定結果を待つ（ステップＳ５０８）。
【００４１】
セキュリティ管理サーバ１０１においては、クライアント機器１０２からＰＤＬデータを受信した旨が通知されると（ステップＳ５０４）、セキュリティチェック実行部４０３により、セキュリティチェックデータ格納部４０２に格納されているテストパターンに基づいてクライアント機器１０２のセキュリティレベルがチェックされる（ステップＳ５０５）。そして、セキュリティレベル判定部４０５により、セキュリティ基準格納部４０４に格納されているデータに基づいてセキュリティレベルの判定が行われる（ステップＳ５０６）。
【００４２】
セキュリティチェック実行部４０３によるセキュリティチェックの方法としては、例えば、
ａ）既知のセキュリティに関する問題点を試しに突いてみて、対策が取られているか否かを調べる、
ｂ）ネットワーク上の近くのホストコンピュータにランダムにアクセスし、攻撃に使用可能と推定されるポートが開いていないか否かを調べる、
ｃ）手持ちの辞書や知識データベースを使ってパスワードを推測し、システムへのログインを試みる、
などが一定時間内に実行され、それによりセキュリティが破られた場合の件数に応じてセキュリティのランク付けが行われる。例えば、１００件のテストを行った場合において、その結果セキュリティが破られた件数に応じて、セキュリティのレベルがＡ，Ｂ，Ｃの３段階に判定される。セキュリティが破られた件数が０件の場合はセキュリティレベルがＡ、１０件未満の場合はＢ、１０件以上の場合はＣとそれぞれ判定される。ここで、セキュリティレベルＡは「問題なし（制限なし）」、セキュリティレベルＢは「問題あり（小さな制限あり）」、セキュリティレベルＣは「問題あり（大きな制限あり）」である。
【００４３】
次いで、セキュリティ管理サーバ１０１は、上記判定結果を、機器構成情報管理部４０１に格納されている情報を用いてクライアント機器１０２に通知する（ステップＳ５０７）。
【００４４】
クライアント機器１０２は、上記判定結果を受信すると（ステップＳ５０８）、受信した判定結果すなわちセキュリティレベルに基づいて印刷制限処理を行う（ステップＳ５０９）。ここでは、受信した判定結果（セキュリティレベル）に応じて、ＰＤＬデータにより指定された印刷枚数、紙サイズ、印字モードなどに対する条件を制限する。このセキュリティレベルに応じた制限内容の詳細については後述する。
【００４５】
次いで、クライアント機器１２０は、印刷制限がされたか否かを判定し（ステップＳ５

１０）、印刷制限がされた場合、上記判定結果に対応する制限の内容をホストコンピュータ１０４に通知する（ステップＳ５１１）。そして、クライアント機器１０２は、上記ステップＳ５０９で制限された内容に応じた印刷処理を実行し、それにより得られたイメージデータをプリンタ１０３に出力する（ステップＳ５１２）。上記通知を受けたホストコンピュータ１０４は、通知された制限の内容をディスプレイ（図示せず）などに表示する（ステップＳ５１３）。

【００４６】

これに対し、クライアント機器１２０は、上記ステップＳ５１０で印刷制限がされていないと判定した場合、制限をかけることなく、受信されたＰＤＬデータに対応するイメージデータをプリンタ１０３に出力する（ステップＳ５１２）。

【００４７】

次に、上記ステップＳ５０９の処理の詳細について図６を参照しながら説明する。図６は図５のステップＳ５０９の処理の手順を詳細に示すフローチャートである。このステップＳ５０９の処理は、クライアント機器１０２のセキュリティ対応処理部４０９によって実行されるものである。

【００４８】

セキュリティ対応処理部４０９は、図６に示すように、まず、セキュリティ管理サーバ１０１から通知されたセキュリティレベルの判定結果（ステップＳ５０８）に基づいてセキュリティレベルがＡであるか否かを判定し（ステップＳ６０１）、セキュリティレベルがＡである場合、ＰＤＬデータにより指定された印刷枚数、紙サイズ、印字モードなどを制限しないことを設定する（ステップＳ６０３）。そして、セキュリティ対応処理部４０９は、本処理を終了する。

【００４９】

上記ステップＳ６０１でセキュリティレベルがＡでないと判定された場合、セキュリティ対応処理部４０９は、上記セキュリティレベルの判定結果（ステップＳ５０８）に基づいてセキュリティレベルがＢであるか否かを判定する（ステップＳ６０２）。ここで、セキュリティレベルがＢであると判定された場合、セキュリティ対応処理部４０９は、ＰＤＬデータにより指定された印刷枚数（一回当たりの印刷部数）を制限し、その制限された印刷枚数を設定する（ステップＳ６０４）。そして、セキュリティ対応処理部４０９は、本処理を終了する。

【００５０】

上記ステップＳ６０２でセキュリティレベルがＢでないと判定された場合、すなわちセキュリティレベルがＣである場合、セキュリティ対応処理部４０９は、カラーデータに対してはモノクロモードでの印刷をするように制限し、またモノクロデータに対しては縮小印刷を行うように制限する（ステップＳ６０５）。そして、セキュリティ対応処理部４０９は、本処理を終了する。

【００５１】

このように、本実施の形態によれば、セキュリティ管理サーバ１０１によりセキュリティが低いと判定されたネットワーク環境においては、そのセキュリティレベルに応じて、クライアント機器１０２で制限をかけて印刷処理が実行されるので、ネットワーク管理者に大きな負荷を掛けることなく、ネットワーク上のプリンタ１０３の不正使用に対する対策を実施することができる。また、印刷処理に制限がかけられた場合、その制限の内容がホストコンピュータ１０４を介してユーザに通知されるので、ユーザはその不都合を解消するためにシステム管理者にセキュリティ向上のための施策を講ずることを促すことができる。

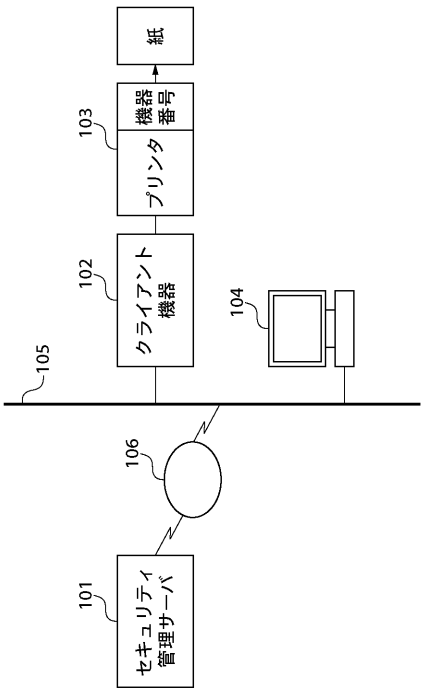
【００５２】

本実施の形態では、３段階のセキュリティレベルのうち、いずれかのレベルにあるかを判定するようにしているが、複数段階のセキュリティレベルのうち、いずれかのレベルにあるかを判定するようにしてもよい。この場合、印刷制限処理は、各段階のレベルに応じてものとすることができる。

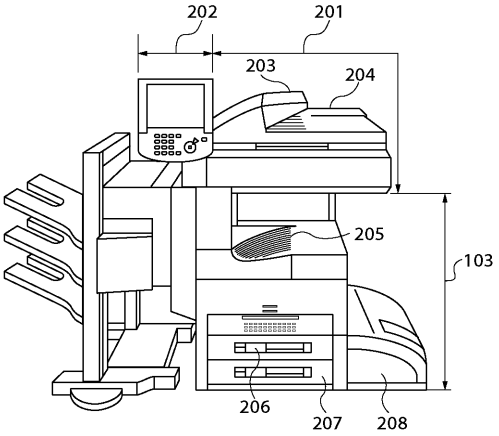
【００５３】
　また、本実施の形態では、セキュリティレベルに応じて制限をかけて印刷を行うようにしているが、これに代えて、クライアント機器１０２が、セキュリティ管理サーバ１０１から通知されたセキュリティレベルをホストコンピュータ１０４２通知し、印刷処理に関しては、印刷制限をかけることなく行うようにしてもよい。また、クライアント機器において、セキュリティレベルがＢまたはＣであるときには、警告メッセージを操作部２０２に表示し、印刷を保留してオペレータの操作部２０２からのキー操作による指示がない限り全く印刷させないようにしてもよい。
【００５４】
　また、セキュリティレベルがＣである場合は、クライアント機器１０２から管理者（またはホストコンピュータ１０４のユーザ）にその旨を通知し、自らネットワーク(ＬＡＮ)との回線を切断するように処理し、管理者（またはホストコンピュータ１０４のユーザ）の対応待ちにするようにしてもよい。
【００５５】
　なお、本発明の目的は、前述した実施の形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることはいうまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることはいうまでもない。
【００５６】
　さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることはいうまでもない。
【図面の簡単な説明】
【００５７】
【図１】本発明の一実施の形態に係る印刷システムの主要部構成を示すブロック図である。
【図２】図１のクライアント機器１０２とプリンタ１０３とが組み込まれている複写機の外観図である。
【図３】図２の複写機の制御構成を示すブロック図である。
【図４】図１のプリンタ１０３に対するセキュリティ管理を実現するための機能構成を示す図である。
【図５】図１のネットワーク印刷システムの印刷動作の手順を示すフローチャートである。
【図６】図５のステップＳ５０９の処理の手順を詳細に示すフローチャートである。
【符号の説明】
【００５８】
　１０１　セキュリティ管理サーバ
　１０２　クライアント機器
　１０３　プリンタ
　１０４　ホストコンピュータ
　１０５　ＬＡＮ

１０６　ＷＡＮ
３０１　ＣＰＵ
３０３　ＲＯＭ
３０４　ＨＤＤ
４０３　セキュリティチェック実行部
４０５　セキュリティレベル判定部
４０９　セキュリティ対応処理部

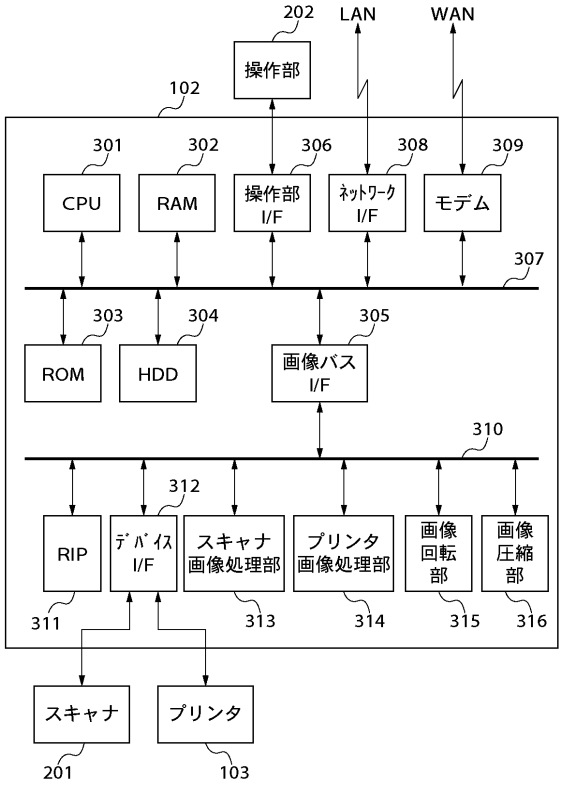
【図１】



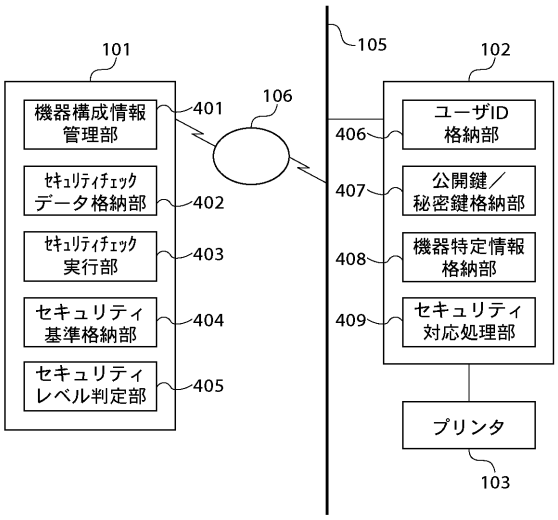
【図２】



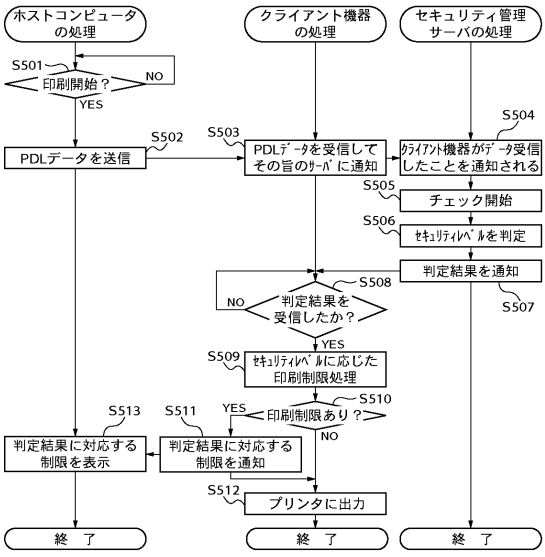
【図３】


202
LAN
WAN
操作部
102
301
302
306
308
309
CPU
RAM
操作部 I/F
ﾈｯﾄﾜｰｸ I/F
モデム
307
303
304
305
ROM
HDD
画像バス I/F
310
312
RIP
ﾃﾞﾊﾞｲｽ I/F
スキャナ 画像処理部
プリンタ 画像処理部
画像 回転 部
画像 圧縮 部
311
313
314
315
316
スキャナ
プリンタ
201
103

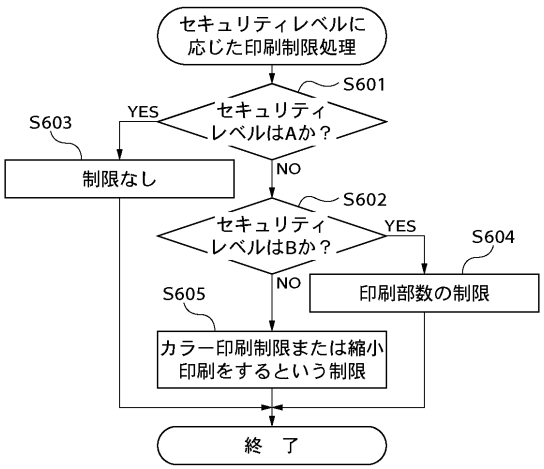
【図４】


101
105
102
機器構成情報 管理部
401
106
406
ユーザID 格納部
ｾｷｭﾘﾃｨﾁｪｯｸ データ格納部
402
407
公開鍵／ 秘密鍵格納部
ｾｷｭﾘﾃｨﾁｪｯｸ 実行部
403
408
機器特定情報 格納部
セキュリティ 基準格納部
404
409
セキュリティ 対応処理部
セキュリティ レベル判定部
405
プリンタ
103

【図５】


ホストコンピュータの処理
クライアント機器の処理
セキュリティ管理サーバの処理
S501
印刷開始？
NO
YES
S502
PDLデータを送信
S503
PDLﾃﾞｰﾀを受信してその旨のｻｰﾊﾞに通知
S504
ｸﾗｲｱﾝﾄ機器がﾃﾞｰﾀ受信したことを通知される
S505
チェック開始
S506
ｾｷｭﾘﾃｨﾚﾍﾞﾙを判定
判定結果を通知
S507
S508
NO
判定結果を受信したか？
YES
S509
ｾｷｭﾘﾃｨﾚﾍﾞﾙに応じた印刷制限処理
S510
YES
印刷制限あり？
NO
S513
S511
判定結果に対応する制限を表示
判定結果に対応する制限を通知
S512
プリンタに出力
終 了
終 了
終 了

【図６】


セキュリティレベルに応じた印刷制限処理
S601
YES
セキュリティレベルはAか？
S603
制限なし
NO
S602
セキュリティレベルはBか？
YES
S604
印刷部数の制限
NO
S605
カラー印刷制限または縮小印刷をするという制限
終 了