(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4208776号
(P4208776)

(45)発行日　平成21年1月14日(2009.1.14)　(24)登録日　平成20年10月31日(2008.10.31)

(51)Int.Cl.			F I		
G06F	3/12	(2006.01)	G06F	3/12	K
B41J	5/30	(2006.01)	B41J	5/30	Z
H04L	9/32	(2006.01)	H04L	9/00	675A

請求項の数 18　(全 14 頁)

(21)出願番号　特願2004-188488 (P2004-188488)
(22)出願日　平成16年6月25日 (2004.6.25)
(65)公開番号　特開2006-11857 (P2006-11857A)
(43)公開日　平成18年1月12日 (2006.1.12)
審査請求日　平成17年11月25日 (2005.11.25)

(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　100090273
弁理士　國分　孝悦
(72)発明者　浜田　昇
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　三好　洋治

(56)参考文献　特開２００１－２２３７３５（ＪＰ，Ａ）
特開２００２－１６９６８１（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】印刷クライアント、ネットワークプリンタ及び印刷システム

(57)【特許請求の範囲】

【請求項１】

印刷データを複数のデータブロックに分割するデータ分割手段と、

前記データ分割手段が前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付加手段と、

前記データ分割手段によって分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成手段と、

前記ハッシュ値生成手段が生成したハッシュ値の１つを、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加手段と、

前記電子署名付加手段が生成した１単位の送信データと、前記ハッシュ値付加手段が生成した複数単位の送信データとを、印刷処理を行う装置に送信するデータ送信手段と、を有することを特徴とする印刷クライアント。

【請求項２】

前記ハッシュ値生成手段が生成したハッシュ値をメモリに一時的に格納しておくハッシュ値格納手段を有し、

前記ハッシュ値付加手段は、前記ハッシュ値格納手段がメモリに格納しておいたハッシュ値を、前記ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して前記１単位の送信データを生成することを特徴とする請求項１に記載の印刷クライ

アント。
【請求項３】
前記ハッシュ値付加手段は、前記ハッシュ値格納手段がメモリに格納しておいたハッシュ値を、前記ハッシュ値を生成したデータブロックの次のデータブロックに付加して前記１単位の送信データを生成することを特徴とする請求項２に記載の印刷クライアント。
【請求項４】
前記ハッシュ値付加手段は、前記ハッシュ値生成手段が生成したハッシュ値のうち付加されるべきデータブロックがないハッシュ値を、前記印刷処理を行う装置が前記印刷データを処理する上で無意味なデータに付加することを特徴とする請求項１に記載の印刷クライアント。
【請求項５】
印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信手段と、
前記受信手段が受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成手段と、
前記ハッシュ値生成手段が前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し手段と、
前記ヘッダ取り出し手段によって取り出したヘッダと、前記ハッシュ値生成手段が生成したハッシュ値との一致を判断するデータ真正性判断手段と、
前記ヘッダ取り出し手段によって取り出されたヘッダと、前記ハッシュ値生成手段が生成したハッシュ値とが一致すると前記データ真正性判断手段が判断した場合に、前記ハッシュ値生成手段がハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理手段と、を有することを特徴とするネットワークプリンタ。
【請求項６】
前記ヘッダ取り出し手段は、前記ハッシュ値を生成するもとになった受信データブロックの次の受信データブロックからヘッダを取り出すことを特徴とする請求項５に記載のネットワークプリンタ。
【請求項７】
前記印刷処理手段は、前記ヘッダ取り出し手段が取り出したヘッダと、前記ハッシュ値生成手段が生成したハッシュ値とが一致しなかったと前記真正性判断手段が判断した場合には前記ハッシュ値生成手段がハッシュ値を生成した前記受信データブロックから取り出した印刷データに基づく印刷処理を中断することを特徴とする請求項５または６に記載のネットワークプリンタ。
【請求項８】
請求項１～４の何れか１項に記載の印刷クライアントと、請求項５～７の何れか１項に記載のネットワークプリンタとを有することを特徴とする印刷システム。
【請求項９】
印刷データを複数に分割したデータブロックの各々を外部から受信する受信手段と、
前記受信手段が受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成手段と、前記ハッシュ値生成手段が前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し手段と、
前記ヘッダ取り出し手段によって取り出したヘッダと、前記ハッシュ値生成手段が生成したハッシュ値との一致を判断するデータ真正性判断手段と、
前記ヘッダ取り出し手段によって取り出されたヘッダと、前記ハッシュ値生成手段が生成したハッシュ値とが一致すると前記データ真正性判断手段が判断した場合に、前記ハッシュ値生成手段がハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理手段と、を有することを特徴とする印刷処理装置。
【請求項１０】
印刷データを複数のデータブロックに分割するデータ分割工程と、

前記データ分割工程において前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付加工程と、
前記データ分割工程において分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成工程と、
前記ハッシュ値生成工程において生成したハッシュ値の１つを、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加工程と、
前記電子署名付加工程において生成した１単位の送信データと、前記ハッシュ値付加工程において生成した複数単位の送信データとを、印刷処理を行う装置に送信するデータ送信工程と、を有することを特徴とする印刷クライアント制御方法。
【請求項１１】
前記ハッシュ値生成工程において生成したハッシュ値をメモリに一時的に格納しておくハッシュ値格納工程を有し、
前記ハッシュ値付加工程は、前記ハッシュ値格納工程においてメモリに格納しておいたハッシュ値を、前記ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して前記１単位の送信データを生成することを特徴とする請求項１０に記載の印刷クライアント制御方法。
【請求項１２】
前記ハッシュ値付加工程は、前記ハッシュ値格納工程においてメモリに格納しておいたハッシュ値を、前記ハッシュ値を生成したデータブロックの次のデータブロックに付加して前記１単位の送信データを生成することを特徴とする請求項１１に記載の印刷クライアント制御方法。
【請求項１３】
前記ハッシュ値付加工程は、前記ハッシュ値生成工程において生成したハッシュ値のうち付加されるべきデータブロックがないハッシュ値を、前記印刷処理を行う装置が前記印刷データを処理する上で無意味なデータに付加することを特徴とする請求項１０に記載の印刷クライアント制御方法。
【請求項１４】
印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信工程と、
前記受信工程において受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成工程と、
前記ハッシュ値生成工程で前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し工程と、
前記ヘッダ取り出し工程において取り出したヘッダと、前記ハッシュ値生成工程で生成したハッシュ値との一致を判断するデータ真正性判断工程と、
前記ヘッダ取り出し工程において取り出されたヘッダと、前記ハッシュ値生成工程において生成したハッシュ値とが一致すると前記データ真正性判断工程において判断した場合に、前記ハッシュ値生成工程においてハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理工程と、を有することを特徴とする受信データ処理方法。
【請求項１５】
前記ヘッダ取り出し工程は、前記ハッシュ値を生成するもとになった受信データブロックの次の受信データブロックからヘッダを取り出すことを特徴とする請求項１４に記載の受信データ処理方法。
【請求項１６】
印刷データを複数のデータブロックに分割するデータ分割工程と、
前記データ分割工程において前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付

加工程と、
前記データ分割工程において分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成工程と、
前記ハッシュ値生成工程において生成した１つのハッシュ値を、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加工程と、
前記電子署名付加工程において生成した１単位の送信データと、前記ハッシュ値付加工程において生成した複数単位の送信データとを、印刷処理を行なう装置に送信するデータ送信工程と、をコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項１７】
印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信工程と、
前記受信工程において受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成工程と、
前記ハッシュ値生成工程で前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し工程と、
前記ヘッダ取り出し工程において取り出したヘッダと、前記ハッシュ値生成工程で生成したハッシュ値との一致を判断するデータ真正性判断工程と、
前記ヘッダ取り出し工程において取り出されたヘッダと、前記ハッシュ値生成工程において生成したハッシュ値とが一致すると前記データ真正性判断工程において判断した場合に、前記ハッシュ値生成工程においてハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理工程と、をコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項１８】
請求項１６または１７に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は印刷クライアント、ネットワークプリンタ及び印刷システムに関し、特に、パーソナルコンピュータ（ＰＣ）などの印刷クライアントから、例えばプリンタ装置などの印刷デバイスにネットワークを介して印刷ジョブを送信する際に、その印刷ジョブデータが途中で改ざんされることを防止するために用いて好適な技術に関する。
【背景技術】
【０００２】
従来、クライアントからネットワークを介して印刷データをプリンタに送って印刷する系においては、経路上で印刷データが改ざんされるという潜在的な脅威が存在している。
図１は、その脅威の存在を示すネットワークプリントシステムの概念を説明する図である。図１に示したように、印刷クライアント１０１からネットワークプリンタ１０２に対して、ネットワーク（ＬＡＮ）１０４を介して印刷データが送られるのであるが、途中で攻撃者１０３（例えば、プリンタドライバ）が、例えばネットワークプリンタ１０２のネットワークアドレスを詐称するなどの方法により印刷データを横取りし、それを改ざんした上でネットワークプリンタ１０２に送ることにより、印刷結果を改ざんすることが可能である。
【０００３】
従来、このような脅威に対抗するために、印刷ジョブに限らず、データの改ざん防止については、データ作成側においてハッシュ関数によってデータ全体のハッシュ値を計算した後、そのハッシュ値に電子署名を付加し、データ検証側で電子署名を検証することによってデータが改ざんされているかどうかをチェックすることが一般的である。ネットワーク１０４上を流れる印刷ジョブの改ざん防止についても、同様の手法でチェックをする方

法が開示されている（例えば、特許文献１参照）。
【０００４】
【特許文献１】特開２００３－０８４９６２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
図２は、ハッシュを計算する方法を簡単に説明した図である。
まず、印刷データ２０１が生成されるのを待ち、そのハッシュ値２０２を計算し、それを前記印刷データ２０１に付加した送信データ（ｄ１）２０３を作成する。ハッシュ値２０２は、例えば、印刷データを１方向性関数、例えばSHA-1やMD5といった既知のハッシュ関数を通すことによって得ることができる。
【０００６】
そして、前記送信データ（ｄ１）２０３を受信したネットワークプリンタにおいて、受信したデータのうち印刷データ部分からハッシュ値を計算して、受信したデータ（ｄ１）２０３に含まれていたハッシュ値２０２との一致を確認することにより、印刷データが途中で改ざんされているかどうかを判断できるようになっている。
【０００７】
ところが、このような方法で印刷データの正否を検証しようとすると、全部の印刷データが揃うまでハッシュ値の計算を行うことができず、データの送出が行えないので、印刷の開始（いわゆるファーストプリント）が遅れてしまう問題点があった。この問題は、特に印刷データが何百ページ分にも及ぶデータ量が多い場合に顕著に現れる。
【０００８】
本発明はこのような状況のもとでなされたものであり、ファーストプリントを素早く行うことができるようにするとともに、印刷データの改ざんを有効に防止できるようにすることを目的としている。
【課題を解決するための手段】
【０００９】
本発明の印刷クライアントは、印刷データを複数のデータブロックに分割するデータ分割手段と、前記データ分割手段が前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付加手段と、前記データ分割手段によって分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成手段と、前記ハッシュ値生成手段が生成したハッシュ値の１つを、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加手段と、前記電子署名付加手段が生成した１単位の送信データと、前記ハッシュ値付加手段が生成した複数単位の送信データとを、印刷処理を行う装置に送信するデータ送信手段と、を有することを特徴とする。
【００１０】
本発明のネットワークプリンタは、印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信手段と、前記受信手段が受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成手段と、前記ハッシュ値生成手段が前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し手段と、前記ヘッダ取り出し手段によって取り出したヘッダと、前記ハッシュ値生成手段が生成したハッシュ値との一致を判断するデータ真正性判断手段と、前記ヘッダ取り出し手段によって取り出されたヘッダと、前記ハッシュ値生成手段が生成したハッシュ値とが一致すると前記データ真正性判断手段が判断した場合に、前記ハッシュ値生成手段がハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理手段と、を有することを特徴とする。
【００１１】
本発明の印刷システムは、前記の何れか１項に記載の印刷クライアントと、前記の何れ

か１項に記載のネットワークプリンタとを有することを特徴とする。

【００１２】

本発明の印刷処理装置は、印刷データを複数に分割したデータブロックの各々を外部から受信する受信手段と、前記受信手段が受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成手段と、前記ハッシュ値生成手段が前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し手段と、前記ヘッダ取り出し手段によって取り出したヘッダと、前記ハッシュ値生成手段が生成したハッシュ値との一致を判断するデータ真正性判断手段と、前記ヘッダ取り出し手段によって取り出されたヘッダと、前記ハッシュ値生成手段が生成したハッシュ値とが一致すると前記データ真正性判断手段が判断した場合に、前記ハッシュ値生成手段がハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理手段と、を有することを特徴とする。

本発明の印刷クライアント制御方法は、印刷データを複数のデータブロックに分割するデータ分割工程と、前記データ分割工程において前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付加工程と、前記データ分割工程において分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成工程と、前記ハッシュ値生成工程において生成したハッシュ値の１つを、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加工程と、前記電子署名付加工程において生成した１単位の送信データと、前記ハッシュ値付加工程において生成した複数単位の送信データとを、印刷処理を行う装置に送信するデータ送信工程と、を有することを特徴とする。

【００１３】

本発明の受信データ処理方法は、印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信工程と、前記受信工程において受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成工程と、前記ハッシュ値生成工程で前記ハッシュ値を生成するもとになった受信データブロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し工程と、前記ヘッダ取り出し工程において取り出したヘッダと、前記ハッシュ値生成工程で生成したハッシュ値との一致を判断するデータ真正性判断工程と、前記ヘッダ取り出し工程において取り出されたヘッダと、前記ハッシュ値生成工程において生成したハッシュ値とが一致すると前記データ真正性判断工程において判断した場合に、前記ハッシュ値生成工程においてハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理工程と、を有することを特徴とする。

【００１４】

本発明のコンピュータプログラムは、印刷データを複数のデータブロックに分割するデータ分割工程と、前記データ分割工程において前記印刷データを複数のデータブロックに分割して得られる先頭のデータブロックに電子署名を付加して１単位の送信データを生成する電子署名付加工程と、前記データ分割工程において分割された複数のデータブロック各々のハッシュ値を生成するハッシュ値生成工程と、前記ハッシュ値生成工程において生成した１つのハッシュ値を、当該ハッシュ値を生成したデータブロックとは異なる所定のデータブロックに付加して１単位の送信データを生成する処理を複数のデータブロックに対して行うハッシュ値付加工程と、前記電子署名付加工程において生成した１単位の送信データと、前記ハッシュ値付加工程において生成した複数単位の送信データとを、印刷処理を行なう装置に送信するデータ送信工程と、をコンピュータに実行させることを特徴とする。

また、本発明のコンピュータプログラムの他の特徴とするところは、印刷データを複数に分割したデータブロックの各々を、ネットワークを介して受信する受信工程と、前記受信工程において受信した１つのデータブロックからハッシュ値を生成するハッシュ値生成工程と、前記ハッシュ値生成工程で前記ハッシュ値を生成するもとになった受信データブ

ロックとは異なる所定の受信データブロックからヘッダを取り出すヘッダ取り出し工程と、前記ヘッダ取り出し工程において取り出したヘッダと、前記ハッシュ値生成工程で生成したハッシュ値との一致を判断するデータ真正性判断工程と、前記ヘッダ取り出し工程において取り出されたヘッダと、前記ハッシュ値生成工程において生成したハッシュ値とが一致すると前記データ真正性判断工程において判断した場合に、前記ハッシュ値生成工程においてハッシュ値を生成した前記受信データブロックから印刷データを取り出して印刷処理を行う印刷処理工程と、をコンピュータに実行させることを特徴とする。

【００１５】

本発明の記録媒体は、前記に記載のコンピュータプログラムを記録したことを特徴としている。

【発明の効果】

【００１６】

本発明によれば、印刷データが大量であったとしても、データの送出を遅らせることなく、ファーストプリントを素早く行うことが可能となるとともに、印刷データの改ざんを有効に防止することができる。

【発明を実施するための最良の形態】

【００１７】

（第１の実施の形態）

図１は、本発明が実行されるネットワークプリントシステムの概念を説明する図であり、図２はハッシュの計算を行う方法を簡単に説明した図である。

図３は、一般的なコンピュータの内部構成を示したものであり、本実施の形態の印刷クライアント１０１、あるいはネットワークプリンタ１０２のコントローラも同様に構成されているものである。

【００１８】

図３において、３００はコンピュータ全体である。コンピュータ３００は、ＲＯＭ３０２あるいは例えばディスクコントローラ３０７により制御されるハードディスク３１１などの大規模記憶装置に記憶されたソフトウェアを実行するＣＰＵ３０１を備え、システムバス３０４に接続される各デバイスを総括的に制御する。

【００１９】

３０３はＲＡＭで、ＣＰＵ３０１の主メモリ、ワークエリア等として機能する。３０５は外部入力コントローラ（ＫＢＤ Ｃ）で、コンピュータに備えられた各種ボタンあるいはキーボード３０９等からの指示入力を制御する。３０６はディスプレイコントローラ（ＤＩＳＰＣ）で、表示モジュール（ＤＩＳＰＬＡＹ）３１０の表示を制御する。３０８はネットワークインタフェースカード（ＮＩＣ）で、ＬＡＮ１０４を介して、他のネットワーク機器あるいはファイルサーバ等と双方向にデータをやりとりする。３１２はタイマである。

【００２０】

図４は、本実施の形態における、印刷データからハッシュ値を計算し、送信する方法を示す図である。さらに、図６は、その手順を示したフローチャートである。以下、図６の手順に沿って、図４も用いながら、印刷データからハッシュ値を計算して付加し、ネットワークプリンタに送信する手順について説明する。

【００２１】

図６の手順は、印刷クライアント１０１上のＣＰＵ３０１によって実行される。さらに前提として、印刷すべき文書や画像等のデータは、プリンタドライバモジュールによってプリンタが読解可能な形式、すなわちＰＤＬデータに変換され、それが図６の手順を実施するモジュールに順次受け渡されるものとする。

【００２２】

印刷データの送出にあたっては、まずステップＳ６０１で乱数ＲＮＤ４１０を発生させる計算を行う。次に、ステップＳ６０２において、前記ステップＳ６０１で発生させた乱数のハッシュ値４２０を計算する。次に、ステップＳ６０３において、前記ステップＳ６

０２で計算したハッシュ値４２０に電子署名４４０を付加して、合わせてヘッダNとし、ＲＡＭ３０３に一時的に格納しておく。

【００２３】

次に、ステップＳ６０４に進み、プリンタドライバで順次生成されるＰＤＬデータのうち、最初の適当な長さの部分を分割してＰＤＬデータの断片（ｄ１）４１１として受け取り、ＲＡＭ３０３上の一時バッファに格納する。続くステップＳ６０５において、先ほどステップＳ６０３においてＲＡＭ３０３に一時的に格納しておいたヘッダNを取り出して、先のステップＳ６０５で一時バッファに格納しておいたＰＤＬデータの断片（ｄ１）にヘッダとして付加し、１単位の送信データ４３０を形成する。

【００２４】

続くステップＳ６０６において、ＮＩＣ３０８を制御して、ＬＡＮ１０４を介してネットワークプリンタ１０２に、送信データ４３０を送信する。続くステップＳ６０７において、一時バッファに格納してあるＰＤＬデータのハッシュ値を計算し、それを次のＰＤＬデータブロックに付加すべきヘッダNとして、ＲＡＭ３０３上に一時的に格納しておくとともに、ＰＤＬデータとヘッダとを合わせて送信データ４３０として格納していた一時バッファを解放する。

【００２５】

続くステップＳ６０８において、プリンタドライバから受け取るべき印刷データがもう無いかどうかを判断する。もし、ステップＳ６０８において、もう印刷データが無いと判断されたら、ステップＳ６０９に進み、ステップＳ６０７において一時的に格納しておいたヘッダ情報を取り出し、ＮＩＣ３０８を制御して、ＬＡＮ１０４を介してネットワークプリンタ１０２に、最終ヘッダNを送信する。

【００２６】

一方、ステップＳ６０８において、まだ印刷データがあると判断された場合には、ステップＳ６０４に戻り、次のＰＤＬデータの断片（ｄ２）４１２、ＰＤＬデータの断片（ｄ３）４１３を順次に受け取り、ＰＤＬデータのハッシュ値（ｈ１）４２１、ＰＤＬデータのハッシュ値（ｈ２）４２２、ＰＤＬデータのハッシュ値（ｈ３）４２３を生成する処理を続ける。

【００２７】

また、前記ＰＤＬデータのハッシュ値（ｈ１）とＰＤＬデータの断片（ｄ２）とを組み合わせて送信データ４３１を生成する。同様に、前記ＰＤＬデータのハッシュ値（ｈ２）とＰＤＬデータの断片（ｄ３）とを組み合わせて送信データ４３２を生成する。また、組み合わせるべきＰＤＬデータの断片が無い場合には、前記ＰＤＬデータのハッシュ値（ｈ３）とＰＤＬデータの無意味な断片（ＮＵＬＬ）とを組み合わせて送信データ４３３を生成する。なお、前述の処理において、ＰＤＬデータのハッシュ値を生成する処理タイミングと、ＰＤＬデータの断片を受け取るタイミングとを合わせるようにすることにより、前記ハッシュ値をバッファに一時的に格納する処理を省略することができる。

【００２８】

このような手順の処理を行うことにより、図４に示したように、前のＰＤＬデータブロックのハッシュ値を次のＰＤＬデータブロックに付加して送信データとし、順次送信していく。なお、最初の送信データにだけ署名（Ｓｉｇｎａｔｕｒｅ）を付加するのは、その送信データのすり替えを防ぐためである。最初の送信データのすり替えを防止できれば、あとはハッシュ値のチェインによって、PDLデータ全体のすり替えあるいは改ざんを確実に防止することができる。

【００２９】

ところで、ハッシュ値を次のデータブロックに付加するのは以下のような理由による。例えば、図５に示したように、計算したハッシュ値を元のＰＤＬデータ断片（ｄ１）５１１、（ｄ２）５１２、（ｄ３）５１３に付加した場合、データを改ざんしようとする攻撃者の立場から見ると、ハッシュ値が付加されたデータブロック（図５における５３１、５３２および５３３）を横取りすれば、改ざんしたデータに自分でハッシュ値（５２１，５

２２，５２３）を付加することができてしまう。送信データがすりかえられたとしても、受信側ではそれに気がつくことができなくなってしまうためである。

【００３０】

このすり替えを防ぐために、全ての送信データ断片にクライアント側で電子署名をつけることも解のひとつではあるが、電子署名は時間のかかる操作であるので、今度はパフォーマンスに悪影響が発生する。それに対して、本実施の形態では、電子署名は一回だけで済むので、こちらの方が有利である。

【００３１】

図７は、本実施の形態における、ネットワークプリンタ１０２のデータ受信動作の手順を示すフローチャートである。

図７に示した手順は、ネットワークプリンタ１０２上のＣＰＵ３０１によって実行される。

【００３２】

ネットワークプリンタ１０２のデータ受信動作においては、まずステップＳ７０１で、ＮＩＣ３０８を操作して、ＬＡＮ１０４から最初のデータ断片を受け取る。続くステップＳ７０２で受信データのヘッダに含まれる電子署名を検証する。

【００３３】

ステップＳ７０２の検証の結果、もし署名が正しければ、ステップＳ７０３に進む。ステップＳ７０３では、受信データの中からＰＤＬデータを取り出し、不図示の印刷エンジンに送ってそのＰＤＬデータの印刷処理を行う。続くステップＳ７０４で、受信データはこれで終わりかどうかを判断する。この判断の結果、もし終わりでは無いと判断されたら、ステップＳ７０５に進む。

【００３４】

ステップＳ７０５～ステップＳ７０８までは、受信したデータが改ざんされていないことを順次確認する手順である。

先ず、ステップＳ７０５では、ステップＳ７０３で印刷したＰＤＬデータのハッシュ値を計算し、一時記憶領域に格納しておく。続くステップＳ７０６でＮＩＣ３０８を操作して、ＬＡＮ１０４から次のデータ断片を受け取る。

【００３５】

続くステップＳ７０７で、先のステップＳ７０６で受信したデータの中からヘッダ部分を取り出す。そこには、クライアント側で計算した、ＰＤＬデータのハッシュ値が入っているはずである。続くステップＳ７０８において、先のステップＳ７０５で計算したハッシュ値と先のステップＳ７０７で取り出した値が同じであるかどうかによってデータが正しいかどうかを判断する。

【００３６】

この判断の結果、もし、ステップＳ７０８において、データが正しいと判断された場合にはステップＳ７０３に戻って印刷処理を続行する。また、ステップＳ７０８においてデータが正しくないと判断された場合には、ただちに印刷処理を中断すべく、処理を終了する。先のステップＳ７０２で署名が正しくないと判断された場合、ならびに先のステップＳ７０４でデータは終わりであると判断された場合も、受信データの印刷処理は終了である。

【００３７】

上記で説明した本実施の形態に係る印刷クライアント、あるいはネットワークプリンタのプログラムは、外部からインストールされるプログラムによって、印刷クライアント１０１あるいはネットワークプリンタ１０２の各デバイスによって遂行されても良い。その場合、そのプログラムはＣＤ－ＲＯＭやフラッシュメモリやフロッピー（登録商標）ディスクなどの記憶媒体により、あるいは電子メールやパソコン通信などのネットワークを介して、外部の記憶媒体からプログラムを含む情報群を印刷クライアント１０１あるいはネットワークプリンタ１０２の各デバイス上にロードすることにより、印刷クライアント１０１あるいはネットワークプリンタ１０２の各デバイスに供給される場合でも本発明は適

用されるものである。

【００３８】

図９は、記憶媒体の一例であるＣＤ－ＲＯＭのメモリマップを示す図である。図９において、９９９９はディレクトリ情報を記憶してある領域で、以降のインストールプログラムを記憶してある領域９９９８および印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域９９９７の位置を示している。

【００３９】

９９９８は、インストールプログラムを記憶してある領域である。９９９７は、印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域である。本実施の形態の印刷クライアントあるいはネットワークプリンタの制御プログラムが１０１あるいは１０２の各デバイスにインストールされる際には、まずインストールプログラムを記憶してある領域９９９８に記憶されているインストールプログラムがシステムにロードされ、ＣＰＵ３０１によって実行される。

【００４０】

次に、ＣＰＵ３０１によって実行されるインストールプログラムが、デバイス制御プログラムを記憶してある領域９９９７から印刷クライアントあるいはネットワークプリンタの制御プログラムを読み出して、ＲＯＭ３０２の内容を書き換えるか、あるいは大規模記憶装置（ＨＤ）３１１にインストールする。この場合、ＲＯＭ３０２は単純なマスクＲＯＭではなく、フラッシュＲＯＭなどの書き換え可能がＲＯＭである必要がある。

【００４１】

なお、本発明は、複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダなど）から構成されるシステムあるいは統合装置に適用してもよく、ひとつの機器からなる装置に適用してもよい。

【００４２】

また、前述した実施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、本発明の目的が達成されることは言うまでもない。

【００４３】

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本発明の新規な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。

【００４４】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ，ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００４５】

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って、前述した実施形態の機能が実現される他、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動しているＯＳなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【００４６】

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ボ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き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボ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、その処理によっても前述した実施形態の機能が実現され得る。

【００４７】

なお、本発明は、前述した実施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から、そのプログラムをパソコン通信など通信ラインを介して要求者

にそのプログラムを配信する場合にも適用できることは言うまでもない。

【００４８】

（第２の実施の形態）

上述した第１の実施の形態においては、ハッシュをとる元データとしてＰＤＬデータのデータ断片（（ｄ１）８１１、（ｄ２）８１２、（ｄ３）８１３）を対象としたが、例えば図８に示すように、ヘッダＮを含めた送信データ全体８３０のハッシュ値（ｈ１）８２１を計算して、それを次の送信データのヘッダに入れるようにしても良い。

【００４９】

同様に、ハッシュ値（ｈ１）とデータ断片（ｄ２）を含めた送信データ全体８３１のハッシュ値（ｈ２）８２２を計算して、それを次の送信データのヘッダに入れるようにしても良い。また、ハッシュ値（ｈ２）とデータ断片（ｄ３）を含めた送信データ全体８３２のハッシュ値（ｈ３）８２３を計算して、それを次の送信データのヘッダに入れるようにしても良い。さらに、ハッシュ値（ｈ３）とデータ断片（ＮＵＬＬ）を含めた送信データ全体８３３のハッシュ値を計算するようにしても良い。

【００５０】

（第３の実施の形態）

上述した第１の実施の形態においては、ハッシュ値を「次の」データ断片に付加するようにしたが、ハッシュ値を付加する場所は、「次の」データ断片に限定されるものではない。例えば、二つ先のデータ断片に付加するようにしても良い。要は、ハッシュ値を計算する元となったデータ断片以外のデータ断片に付加することが肝要である。

【図面の簡単な説明】

【００５１】

【図１】図経路上のデータ改ざんの脅威を示す概念を示す図である。

【図２】ハッシュ値の付加方法の一例を示す図である。

【図３】実施の形態の印刷クライアントあるいはプリンタの内部構成例を示すブロック図である。

【図４】実施の形態のハッシュ値付加方法を示す図である。

【図５】改ざんの脅威が残るハッシュ値付加方法を示す図である。

【図６】実施の形態の印刷クライアントの動作を説明するフローチャートである。

【図７】実施の形態のプリンタの動作を説明するフローチャートである。

【図８】第２の実施の形態におけるハッシュ値付加方法を示す図である。

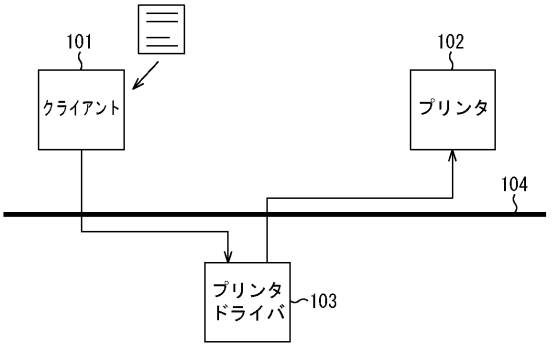
【図９】本実施の形態のソフトウェアの記憶媒体におけるメモリマップの一例を示す図である。

【符号の説明】

【００５２】

１０４　ＬＡＮ
３００　コンピュータ
３０１　ＣＰＵ
３０２　ＲＯＭ、
３０３　ＲＡＭ
３０４　システムバス
３０５　外部入力コントローラ（ＫＢＤ　Ｃ）
３０６　ディスプレイコントローラ（ＤＩＳＰＣ）
３０７　ディスクコントローラ
３０８　ネットワークインタフェースカード（ＮＩＣ）
３０９　キーボード
３１０　表示モジュール（ＤＩＳＰＬＡＹ）
３１１　ハードディスク
３１２　タイマ

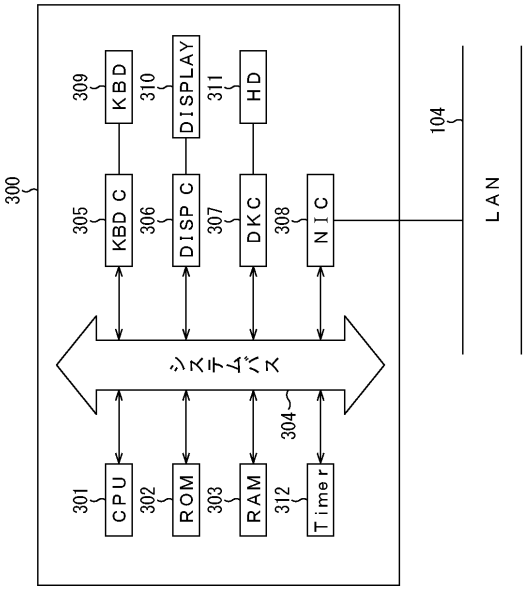
【図１】


101
クライアント
102
プリンタ
104
プリンタドライバ
103

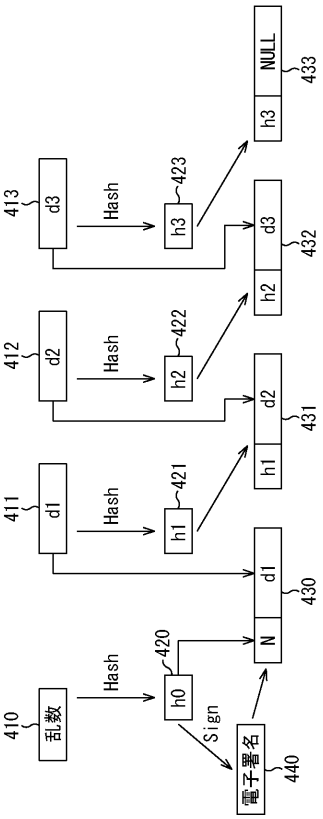
【図２】


印刷データ
201
Hash
h
202
h1
印刷データ d1
203

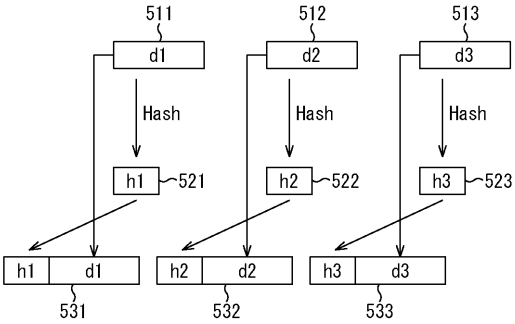
【図３】


300
309
KBD
310
DISPLAY
311
HD
104
LAN
305
KBD C
306
DISP C
307
DKC
308
NIC
システムバス
304
301
CPU
302
ROM
303
RAM
312
Timer

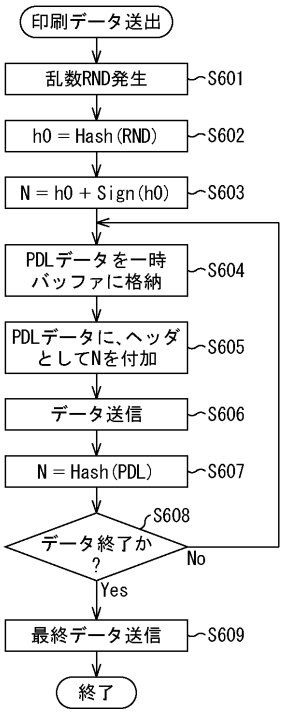
【図４】


410
乱数
Hash
420
h0
Sign
電子署名
440
N
d1
430
411
d1
Hash
421
h1
h1
d2
431
412
d2
Hash
422
h2
h2
d3
432
413
d3
Hash
423
h3
h3
NULL
433

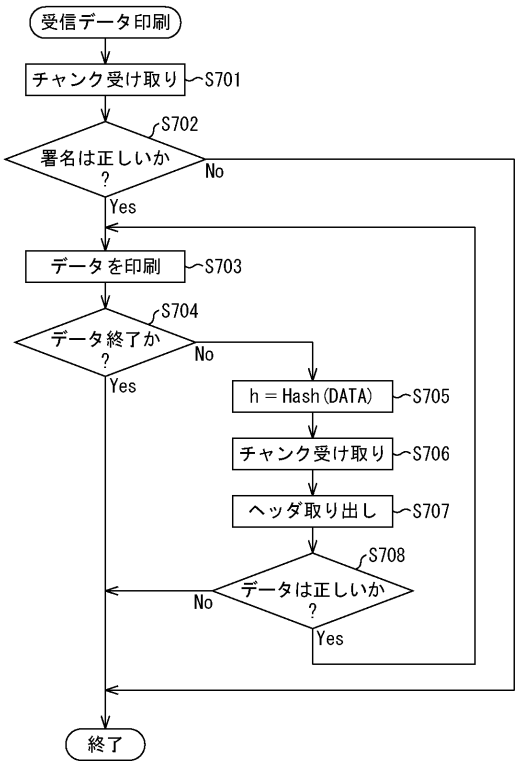
【図５】


511
d1
Hash
h1
521
h1
d1
531
512
d2
Hash
h2
522
h2
d2
532
513
d3
Hash
h3
523
h3
d3
533

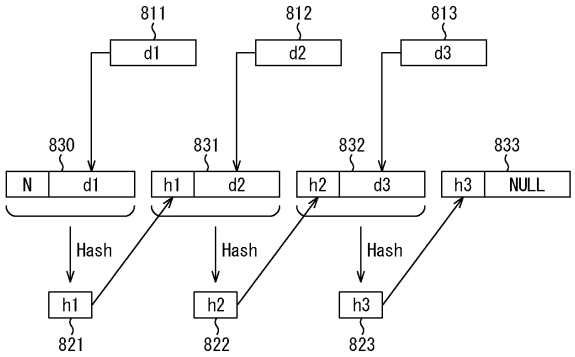
【図６】


印刷データ送出
乱数RND発生
S601
h0 = Hash(RND)
S602
N = h0 + Sign(h0)
S603
PDLデータを一時バッファに格納
S604
PDLデータに、ヘッダとしてNを付加
S605
データ送信
S606
N = Hash(PDL)
S607
データ終了か？
S608
No
Yes
最終データ送信
S609
終了

【図７】


受信データ印刷
チャンク受け取り
S701
署名は正しいか？
S702
No
Yes
データを印刷
S703
データ終了か？
S704
No
Yes
h = Hash(DATA)
S705
チャンク受け取り
S706
ヘッダ取り出し
S707
データは正しいか？
S708
No
Yes
終了

【図８】


811
812
813
d1
d2
d3
830
831
832
833
N
d1
h1
d2
h2
d3
h3
NULL
Hash
Hash
Hash
h1
h2
h3
821
822
823

【図９】


ディレクトリ情報
9999
…
インストールプログラム
9998
…
制御プログラム
9997
…

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)

Ｇ０６Ｆ	３／１２
Ｂ４１Ｊ	５／３０
Ｈ０４Ｌ	９／３２