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

特許第4527882号
(P4527882)

(45)発行日　平成22年8月18日(2010.8.18)　(24)登録日　平成22年6月11日(2010.6.11)

(51)Int.Cl.		F I		
G06Q 50/00	(2006.01)	G06F	17/60	142
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 17/30	(2006.01)	H04L	9/00	601A
H04L 9/10	(2006.01)	G06F	17/30	110F
		G06F	17/30	120A

請求項の数 9　(全 21 頁)　最終頁に続く

(21)出願番号	特願2000-575010 (P2000-575010)
(86)(22)出願日	平成11年10月7日 (1999.10.7)
(65)公表番号	特表2002-527009 (P2002-527009A)
(43)公表日	平成14年8月20日 (2002.8.20)
(86)国際出願番号	PCT/US1999/023474
(87)国際公開番号	WO2000/020950
(87)国際公開日	平成12年4月13日 (2000.4.13)
審査請求日	平成18年4月27日 (2006.4.27)
(31)優先権主張番号	09/167,888
(32)優先日	平成10年10月7日 (1998.10.7)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　501142489
アドビ・システムズ・インコーポレーテッド
アメリカ合衆国カリフォルニア州９５１１０－２７０４，サンノゼ，メイル・ステーション・ダブリューティ１４，パーク・アベニュー　３４５
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100071124
弁理士　今井　庄亮
(74)代理人　100076691
弁理士　増井　忠弐
(74)代理人　100075270
弁理士　小林　泰

最終頁に続く

(54)【発明の名称】データ項目に対するアクセスを配布する方法及びシステム

(57)【特許請求の範囲】

【請求項１】

出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法であって、

出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、

前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、

（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、

前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、

（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを

変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記エンドユーザー・コンピュータが、暗号化されないブック・データ項目を取得する際に、（ｉ）前記エンドユーザー・コンピュータが自己の公開鍵を前記小売業者コンピュータへ送るステップと、（ｉｉ）前記小売業者コンピュータが、前記エンドユーザー・コンピュータの公開鍵を用いて暗号化した前記機密鍵と前記機密鍵で暗号化されたブック・データ項目とを前記エンドユーザー・コンピュータへ送出するステップと、（ｉｉｉ）前記エンドユーザー・コンピュータが自己の秘密鍵を用いて前記機密鍵を取得し、取得した前記機密鍵を用いて前記暗号化されたブック・データ項目を解読するステップとが行われる方法。
【請求項２】
出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法であって、
出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、
前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、
（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、
前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記機密鍵が満了時間と関連付けられ、前記エンドユーザー・コンピュータが前記機密鍵を前記満了時間に達するまで使用できる方法。
【請求項３】

出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法であって、
出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、
前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、
（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、
前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記機密鍵が前記エンドユーザー・コンピュータに与えられると、前記機密鍵が前記小売業者コンピュータから消去される方法。
【請求項４】
出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用されるシステムであって、
Ａ台のエンドユーザー・コンピュータが、暗号化されたブック・データ項目に対するアクセスを取得することを許容する出版業者許可データを記憶する、出版業者コンピュータにおける記憶装置と、
前記出版業者許可データに基づいて、卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するよう構成された第１の許可提供部と、
前記出版業者許可データが、（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するように、前記出版業者許可データを変更する第１の許可変更装置と、
前記卸売業者許可データに基づいて、小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するよう構成された第２の許可提供部と、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者許可データを変更する第２の許可変更装置と、

前記小売業者許可データに基づいて、エンドユーザー・コンピュータに、エンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するよう構成された第３の許可提供部と、

（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者許可データを変更する第３の許可変更装置と、

を備え、

前記エンドユーザー・コンピュータが、暗号化されないブック・データ項目を取得するために、（ｉ）自己の公開鍵を前記第３の許可提供部へ送り、（ｉｉ）前記第３の許可提供部から、前記エンドユーザー・コンピュータの公開鍵を用いて暗号化した前記機密鍵と前記機密鍵で暗号化されたブック・データ項目とを取得し、（ｉｉｉ）自己の秘密鍵を用いて前記機密鍵を取得し、取得した前記機密鍵を用いて前記暗号化されたブック・データ項目を解読するよう動作するシステム。

【請求項５】

出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用されるシステムであって、

Ａ台のエンドユーザー・コンピュータが、暗号化されたブック・データ項目に対するアクセスを取得することを許容する出版業者許可データを記憶する、出版業者コンピュータにおける記憶装置と、

前記出版業者許可データに基づいて、卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するよう構成された第１の許可提供部と、

前記出版業者許可データが、（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するように、前記出版業者許可データを変更する第１の許可変更装置と、

前記卸売業者許可データに基づいて、小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するよう構成された第２の許可提供部と、

（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者許可データを変更する第２の許可変更装置と、

前記小売業者許可データに基づいて、エンドユーザー・コンピュータに、エンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するよう構成された第３の許可提供部と、

（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者許可データを変更する第３の許可変更装置と、

を備え、

前記機密鍵が満了時間と関連付けられ、前記エンドユーザー・コンピュータが前記機密鍵を前記満了時間に達するまで使用できるシステム。

【請求項６】

出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用されるシステムであって、

Ａ台のエンドユーザー・コンピュータが、暗号化されたブック・データ項目に対するアクセスを取得することを許容する出版業者許可データを記憶する、出版業者コンピュータにおける記憶装置と、

前記出版業者許可データに基づいて、卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するよう構成された第１の許可提供部と、
前記出版業者許可データが、（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するように、前記出版業者許可データを変更する第１の許可変更装置と、
前記卸売業者許可データに基づいて、小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するよう構成された第２の許可提供部と、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者許可データを変更する第２の許可変更装置と、
前記小売業者許可データに基づいて、エンドユーザー・コンピュータに、エンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するよう構成された第３の許可提供部と、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者許可データを変更する第３の許可変更装置と、
を備え、
前記機密鍵が前記エンドユーザー・コンピュータに与えられると、前記機密鍵が前記第３の許可提供部から消去されるシステム。
【請求項７】
出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な媒体であって、
前記方法が、
出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、
前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、
（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、
前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、

（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記エンドユーザー・コンピュータが、暗号化されないブック・データ項目を取得する際に、（ｉ）前記エンドユーザー・コンピュータが自己の公開鍵を前記小売業者コンピュータへ送るステップと、（ｉｉ）前記小売業者コンピュータが、前記エンドユーザー・コンピュータの公開鍵を用いて暗号化した前記機密鍵と前記機密鍵で暗号化されたブック・データ項目とを前記エンドユーザー・コンピュータへ送出するステップと、（ｉｉｉ）前記エンドユーザー・コンピュータが自己の秘密鍵を用いて前記機密鍵を取得し、取得した前記機密鍵を用いて前記暗号化されたブック・データ項目を解読するステップとが行われるコンピュータ読み取り可能な媒体。
【請求項８】
出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な媒体であって、
前記方法が、
出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、
前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、
（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、
前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記機密鍵が満了時間と関連付けられ、前記エンドユーザー・コンピュータが前記機密鍵を前記満了時間に達するまで使用できる、コンピュータ読み取り可能な媒体。
【請求項９】
出版業者から卸売業者及び小売業者を介してエンドユーザーにブック・データ項目に対するアクセスを配布するために使用される方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な媒体であって、

前記方法が、
出版業者コンピュータにおいて、機密鍵によって暗号化されたブック・データ項目に対するアクセスをＡ台のエンドユーザー・コンピュータが取得することを許容する出版業者許可データを格納するステップと、
前記出版業者許可データに基づいて、前記出版業者コンピュータが卸売業者コンピュータに、前記暗号化されたブック・データ項目に対するアクセスをＢ台のエンドユーザー・コンピュータが取得することを許容する卸売業者許可データを提供するステップと、
（Ａ－Ｂ）台（ただし、（Ａ－Ｂ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記出版業者許可データが許容するように、前記出版業者コンピュータが前記出版業者許可データを変更するステップと、
前記卸売業者許可データに基づいて、前記卸売業者コンピュータが小売業者コンピュータに、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスを取得することを許容する小売業者許可データを提供するステップと、
（Ｂ－Ｃ）台（ただし、（Ｂ－Ｃ）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記卸売業者許可データが許容するように、前記卸売業者コンピュータが前記卸売業者許可データを変更するステップと、
前記小売業者許可データに基づいて、前記小売業者コンピュータがエンドユーザー・コンピュータに、１台のエンドユーザー・コンピュータが前記暗号化されたブック・データ項目に対するアクセスを取得することを許容するエンドユーザー許可データを提供するステップと、
（Ｃ－１）台（ただし、（Ｃ－１）は負ではない）のエンドユーザー・コンピュータのみが前記暗号化されたブック・データ項目に対するアクセスを取得することを前記小売業者許可データが許容するように、前記小売業者コンピュータが前記小売業者許可データを変更するステップと、
を含み、
前記機密鍵が前記エンドユーザー・コンピュータに与えられると、前記機密鍵が前記小売業者コンピュータから消去される、コンピュータ読み取り可能な媒体。
【発明の詳細な説明】
【０００１】
発明の背景
オーディオ又はビデオの処理又はレコーディングを表わすブック又はデータ構成のテキストを含むファイルのようなコンピュータのデータ項目は、フロッピ・ディスケット又はＣＤ－ＲＯＭのような取外し可能な媒体を介して、或いはインターネットのようなコンピュータ・ネットワーク上でコピーし配布することができる。ある場合には、データ項目は、このデータ項目に対するアクセスに関して管理がほとんど或いは全く行われることなく、自由にコピーされ配布されることが意図される。他の場合は、アクセスに関する管理は、作られる多数の取外し可能媒体に対してある程度の管理を行うことにより、或いはデータ項目のコピーを作るコンピュータ能力を阻害するコピー保護方法によるなどの物理的手段によって試みられる。
【０００２】
図１に示されるように、現在ある電子ブック配布システムにおいては、ブックの内容（ブック・データ）を表わすデータ項目は、中央のソースからハブ／スポーク構成におけるブック読取り装置（すなわち、ブック閲覧装置）に対して（例えば、ネットワーク接続により）コピーされる。
【０００３】
発明の概要
一般に、本発明は、１つの特質において、データ項目に対する配布アクセスにおいて用いられる方法を特徴とする。当該方法は、データ項目に対するアクセスを取得する許可の１

回のインスタンスのコンピュータ間の多数の転送を許容することを含み、これらの転送は、データ接続時に生じ、第１のコンピュータと第２のコンピュータとの間の最初の転送と、第２のコンピュータと第３のコンピュータとの間の以降の転送とを含み、いかなる時点においても、１つのコンピュータのみが許可のインスタンスを保有し、データ項目に対するアクセスを取得する許可のインスタンスを行使することが可能である。

【０００４】

本発明の上記及び他の特質の実現は、下記の特徴の１つ以上を含み得る。この方法は、暗号化鍵を用いてデータ項目に対する不当なアクセスを阻止することを含む。少なくとも１つの許可の転送は、第１の暗号化鍵の転送を含み、当該方法は、転送に先立ち第２の暗号化鍵を用いて第１の暗号化鍵を暗号化することを含む。この第１の暗号化鍵は機密鍵を含み、第２の暗号化鍵は公開／秘密鍵セットにおける１つの鍵を含む。

【０００５】

当該方法は、高度な機密保持回路を用いて、いかなる時点においても唯一つのコンピュータがインスタンスを保有し且つこのインスタンスを使用することが可能であることの保証を助ける。高度な機密保持回路は、スマートカード・コンピュータ又は解読器を含む。当該方法は、高度な機密保持回路における暗号化鍵の記憶を含み、且つ高度な機密保持回路内でのみの暗号化鍵の使用を含む。当該方法は、コンピュータがデータ項目に対するアクセスを取得する許可のインスタンスを受取ることを許可されるか、或いは満了時間に従って、少なくとも１つの転送を一時的に行う。

【０００６】

当該方法は、データ項目へのアクセスの許可のインスタンスを受け取るようコンピュータが認可されているか否かを決定すること、又は、満了時間により、少なくとも一つの転送を放棄することを含む。

【０００７】

当該方法は、一時的な転送において、送出者コンピュータから受信者コンピュータへ暗号化鍵のコピーを送ること、及び、満了時間に受信者コンピュータから暗号化鍵のコピーを消去することを含む。

【０００８】

当該方法は、１つの転送において、送出者コンピュータから受信者コンピュータへ暗号化鍵のコピーを送ること、及び送出者コンピュータから暗号化鍵のコピーを消去することを含む。

【０００９】

当該方法は、少なくとも１回の転送を送金と関連付けること、或いはデータ項目に対するアクセスの取得の異なる許可インスタンス間を弁別することを含む。少なくとも１つのコンピュータが、ウェブ・サーバ・コンピュータ又はブック閲覧装置を含む。このブック閲覧装置は、閲覧スクリーンとデータ通信回路を含む。

【００１０】

一般に、本発明は、別の特質において、１つのデータ項目に特有であり且つ第１のコンピュータにより確立されたアクセス配布パラメータに従って、第２のコンピュータから第３のコンピュータへのデータ接続において、且つ第１のコンピュータとは独立的に、データ項目に対するアクセスの取得の許可を転送することを含む方法を特徴とする。

【００１１】

一般に、本発明は、別の特質において、１つのデータ項目に対するアクセスの取得許可のコンピュータ間のデータ接続転送とは独立に、前記データ項目に対するアクセスの取得を許されるコンピュータの数の変更を阻害することを含む方法を特徴とする。

【００１２】

一般に、本発明は、別の特質において、１つのデータ項目に対するアクセスの配布において使用される方法を特徴とする。当該方法は、第１のコンピュータにデータ項目に対するアクセスの取得の許可を与え、第１のコンピュータからの許可の取消しと実質的に同時に第２のコンピュータに対するデータ接続による許可を与え、且つ第２のコンピュータから

の許可の取消しと実質的に同時に第３のコンピュータに対するデータ接続により許可を与えることを含む。

【００１３】

一般に、本発明は、別の特質において、ブック・データに対するアクセスの取得をコンピュータに許容する許可データのインスタンスを経理的に代替可能にすることを含む方法を特徴とする。

【００１４】

一般に、本発明は、別の特質において、ブック・データ項目に対するアクセスの配布において使用される方法を特徴とする。当該方法は、高度な機密保持回路を、ブック・データ項目に対するアクセスの取得に必要であるアクセス・データの送受が可能である装置に関連付けることを含み、高度な機密保持回路はコンピュータ・プロセッサとプログラム・メモリとを含み、前記装置からのアクセス・データの不当な転送を実質的に阻止することが可能である。

【００１５】

一般に、本発明は、別の特質において、ブック・データ項目に対するアクセスの配布において使用される方法を特徴とする。当該方法は、出版業者コンピュータにおいて、ブック・データ項目に対するアクセスの取得をＡ台のエンドユーザー・コンピュータに許容する出版業者の許可データを記憶すること、出版業者の許可データに基いて、卸売業者コンピュータにブック・データ項目に対するアクセス取得をＢ台のエンドユーザー・コンピュータに許容する卸売業者の許可データを与えること、ブック・データ項目に対するアクセスの取得を出版業者の許可データが（Ａ－Ｂ）台のエンドユーザー・コンピュータのみに許容するように出版業者の許可データを変更すること、出版業者の許可データに基いて、Ｃ台のエンドユーザー・コンピュータがブック・データ項目に対するアクセスの取得を許容する小売業者の許可データを小売業者コンピュータに与えること、卸売業者の許可データがブック・データ項目に対するアクセスの取得を（Ｂ－Ｃ）台のエンドユーザー・コンピュータのみに許容するように卸売業者の許可データを変更すること、ブック・データ項目に対するアクセスの取得を１つのエンドユーザー・コンピュータに許容するエンドユーザーの許可データをエンドユーザー・コンピュータに与えること、及び小売業者の許可データがブック・データ項目に対するアクセスの取得を（Ｃ－１）台のエンドユーザー・コンピュータのみに許容するように小売業者の許可データを変更することを含む。

【００１６】

本発明の利点には、下記の１つ以上が含まれる。データ項目に対するアクセス（すなわち、データ項目の使用許可）は、ユーザー（例えば、消費者）にデータ項目の過大な負担をかけることなく、或いは伝統的なデータ・コピー手法による配布のスケーラビリティを過度に妨げることなく管理することができる。少なくとも一部の場合には、許可の下にデータ項目を取得することは、対応する物理的な処理（例えば、紙の書籍或いは音楽のコンパクト・ディスク）の取得より容易に可能であり、エンドユーザーにとって略々即時の満足が得られる。データ項目に対するアクセスは代替可能にすることができ、従って価値がある。作品（例えば、書籍、オーディオ・レコード、絵画）の配布は従来の物理的な製造に依存しないと数量が制限され得、この制限が作品の価値の維持に役立ち得る。アカウントは、データ項目に対してアクセスするエンドユーザー数で決めることができる。エンティティは、ちょうど図書館が書籍を貸出すように、データ項目をエンドユーザーへ供することができる。データ項目は、データ接続において転送することができるが、データ接続が使用時に利用可能であるかどうかとは無関係に完全に使用可能になる。データ項目に対するアクセスの配布において、インターネット及びワールド・ワイド・ウェブが全く或いは略々全く有利となる。

【００１７】

他の特徴及び利点については、図面を含む以降の記述及び請求の範囲から明らかになるであろう。

詳細な記述

図２は、起点コンピュータ（例えば、出版業者コンピュータ１６）が送出者コンピュータ（例えば、小売業者コンピュータ１２）から受信者コンピュータ（例えば、エンドユーザー・コンピュータ１４）への配布時に利用可能であるかどうかに拘わらず、起点コンピュータによって少なくとも部分的に決定される配布制御パラメータに従って、ブックのテキストを含むデータ（ブック・データ）のようなデータ項目が送出者コンピュータから受信者コンピュータへ配布される、制御されるデータ配布システム１０を示している。このように、少なくとも或る場合には、配布の特定のインスタンスについて何らかの情報を持つコンピュータのみが送出者コンピュータ及び受信者コンピュータであるから、配布は不自由であるばかりでなく個人的なものでもある。

【００１８】

図３は、ブック・データ項目のオリジナル・コピー１８が、１０，０００台までのエンドユーザー・コンピュータ（例えば、ブックの読者のコンピュータ）がブック・データ項目に対してアクセスを行うことを許容する許可データ２０を有する出版業者コンピュータに保持される一般例を示している。このような場合、出版業者コンピュータは卸売業者コンピュータ２２にブック・データ項目のコピー２４と１，０００台のエンドユーザー・コンピュータによるアクセスを許容する許可データ２６とを与え、これにより、許可データを有する出版業者コンピュータは９，０００台のエンドユーザー・コンピュータによるアクセスの許容を放置する。更に、卸売業者コンピュータは小売業者コンピュータにブック・データ項目のコピー２８と５０台のエンドユーザー・コンピュータによるアクセスを許容する許可データ３０とを与え、小売業者コンピュータはエンドユーザー・コンピュータ１４にブック・データ項目のコピー３２とアクセスを許容する許可データ３４を与える。このように、出版業者、卸売業者、小売業者及びエンドユーザーのコンピュータは、ちょうど印刷された書籍の配布システムにおいて出版業者から消費者へ印刷された書籍が配布されると同じように、許可が出版業者コンピュータからエンドユーザー・コンピュータへ配布される配布ネットワークを形成する。許可されたアクセスは、ブック・データ項目へのアクセス取得を許容される最大数のエンドユーザー・コンピュータが配布により影響を受けることがないように固定リソースと見なすことができる。

【００１９】

図４に示されるように、先に述べたような制御された配布は階層的に（例えば、出版業者コンピュータからエンドユーザー・コンピュータへ）生じる必要はなく、図５に示される使用許可転送手順３６に従って実行する任意の２つのコンピュータ間に生じ得る（更に詳細な事例は、図８ないし図１４に関して以下に述べる）。送出者コンピュータ（例えば、ユーザーＡのコンピュータ３８）では、受信者コンピュータ（例えば、ユーザーＢのコンピュータ４０）が、データ項目を利用するための装置を認証する機関により認証されているかどうかが判定され、従って、データ項目（例えば、項目４２）に対するアクセスが与えられるよう許可される（ステップ１０１０）。この機関の目的は、この機関の規則に合致する装置のみが機関と関連するデータ項目に対するアクセスの取得を許容されることの保証を助けることである。例えば、当該機関は、高度な機密保持クロック又は高度な機密保持プログラム・メモリを持たない装置、或いは暗号化ツールを信頼性をもって使用することを証明されなかった装置は認証しない。

【００２０】

受信者コンピュータが認証されると、送出者コンピュータが許可データ（例えば、使用許可データＡに基く使用許可データＢ）を高度な機密保持方法で受信者コンピュータへ送信する（ステップ１０２０）。データ項目のコピーが送出者コンピュータに格納されているならば、データ項目（例えば、データ項目４４）のコピーが高度な機密保持方法で送出者コンピュータから受信者コンピュータへ送信される（ステップ１０３０）。受信者コンピュータは、許可データに従ってデータ項目に対するアクセスを取得する（ステップ１０４０）。

【００２１】

許可データの様式及び送信は、高度な機密保持方法で行われることが重要である。これは

、配布に対する管理が認証された条件下でのみ行われるこのような様式及び送信に依存しているからである。重要なリソースに対する特定の行為者による不当な行為（例えば、常習的な窃盗）を完全に阻止することは不可能であるが、他人（例えば、学生ハッカー）を阻喪させることを助け、且つ、配布が管理される意図で行われ、データ項目をパブリック・ドメインに追加する意図は無いことを明瞭にすることを助けるのに、高度な機密保持策が有効であり得る。

【００２２】

高度な機密保持策の保証を助長するため、送出者コンピュータと受信者コンピュータの各々は、機密鍵及び公開／秘密鍵セットとして知られる暗号化装置に依存しており、１つ以上の鍵又は鍵セット、或いは暗号化データ又は暗号化されないデータ、或いはその双方を取扱う高度な機密保持機構を含んでいる。機密鍵（対称鍵としても知られる）は、他のデータを同じ機密鍵を用いて暗号化することを可能にする方法で他のデータの暗号化に用いられる１つのデータ・ストリング（例えば、４０ビット）である。公開鍵／秘密鍵セットは、いずれからも導出することができず且つ２つのストリングのいずれか一方を用いて暗号化された他のデータを２つのストリングの他方を用いることによってのみ解読できる２つのデータ・ストリング（例えば、それぞれ１０２４ビット）を含む。典型的には、２つのストリングの一方（公開鍵）は秘密に保持されることがなく、２つのストリングの他方（秘密鍵）は高度に秘密保持される。「公開鍵暗号規格（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｓｔａｎｄａｒｄｓ）」（Ｓｅｃｕｒｉｔｙ Ｄｙｎａｍｉｃｓ社ＲＳＡ研究所、１９９３年１１月）及び「ＲＳＡ公開鍵暗号系（ＲＳＡ Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏ Ｓｙｓｔｅｍ）」（Ｓｅｃｕｒｉｔｙ Ｄｙｎａｍｉｃｓ社ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ Ｄｉｖｉｓｉｏｎ、１９８２年）参照。

【００２３】

従来の汎用コンピュータは、機密鍵及び公開鍵／秘密鍵セットを生成するため用いることができ、これら鍵及び鍵セットは、１つ以上の鍵を用いることにより暗号化され或いはその目的で意図されるデータが可能であるように、従来のコンピュータ・ファイルに格納することができる。少なくとも或る場合には、高度な機密保持機構がこれら鍵を取扱い、しかも、この機密保持機構がスマートカード・コンピュータ４６（図６）（例えば、Ｇｅｍｐｌｕｓ ＧｅｍＸｐｒｅｓｓｏ）を含むならば、機密保持が強化される。スマートカード・コンピュータ４６は内部素子への不当なアクセスを阻止するように物理的に封印されており、スマートカード・コンピュータ外部の回路とデータを交換するための唯一の認証手段を提供する接続回路４８を備える。スマートカード・コンピュータはまた、プログラム・メモリ５０と、データ・メモリ５２と、接続回路と通信してプログラム・メモリに格納されたソフトウエアに従って実行し公開鍵／秘密鍵セット暗号器５６と公開鍵／秘密鍵セット解読器５８と機密鍵暗号器６０と機密鍵解読器６２とを実現するプロセッサ５４とを有する。許可データ・バンク６４と、公開鍵６６と、秘密鍵６８と、ディジタル署名７０とは、（例えば、スマートカード・コンピュータが作られるとき）データ・メモリに格納される。ディジタル署名（暗号化されたダイジェストとも呼ばれる）は、公開鍵のダイジェスト・バージョンを生成してグループの秘密鍵（図７）を用いてダイジェスト・バージョンを暗号化することにより（例えば、公開鍵に対するハッシュ機能を与えることにより）生じる結果である。

【００２４】

各スマートカード・コンピュータの公開鍵／秘密鍵セットは異なる（すなわち、固有である）が、群秘密鍵は１つの群内の各スマートカード・コンピュータに対して同じものである。特定の実施の形態においては、スマートカード・コンピュータはまた、スマートカード・コンピュータが関連付けられるエンティティが出版業者、卸売業者或いは小売業者であるならば、前記エンティティの識別を格納し、且つこのエンティティがエンドユーザー（例えば、消費者）であるならば、匿名通し番号を代わりに格納して、エンドユーザーのプライバシの保護に役立てる。特定の実施の形態の代替バージョンにおいては、ディジタル署名は、群秘密鍵を用いて識別を暗号化することにより生成される結果であるディジタ

ル認証により補充或いは置換される。
【００２５】
スマートカード・コンピュータは、Ｊａｖａ（登録商標）として知られるプログラミング言語に従ってフォーマットされたソフトウエア・プログラムを実行することができる。
【００２６】
特定の実施の形態においては、（例えば、他のコンピュータは暗号化データ項目の起点ではないので）出版業者コンピュータのみが機密鍵暗号器が設けられ、（例えば、他のコンピュータはデータ項目の表示或いは他の有効な利用を行わないので）エンドユーザー・コンピュータのみが機密鍵解読器が設けられる。
【００２７】
図８ないし図１４は、使用許可転送手順の詳細な事例７２を示している。機密鍵７４（例えば、ランダムに生成された４０桁の数）を用いてブック・データ７６を暗号化し、機密鍵で暗号化されたブック・データ７８を生成し（ステップ２０１０）、これが送出者コンピュータに格納される（ステップ２０２０）。（特定の実施の形態においては、機密鍵もまた、機密鍵で暗号化されたブック・データに付属される。）
暗号化されたダイジェスト及び受信者コンピュータ固有の公開鍵は、受信者コンピュータから送出者コンピュータへ送信される（ステップ２０５０、２０６０）。送出者コンピュータでは、群公開鍵８４を用いて暗号化ダイジェストを解読し、解読結果８６を生成し（ステップ２０７０）、ダイジェストの結果８８が受信者固有の公開鍵から生成される（ステップ２０８０）。送出者コンピュータでは、ダイジェストの結果が解読結果と比較されて、受信者コンピュータが先に述べたように認証されたかどうか、従ってブック・データを受取ることが認可されるかどうかを判定し（ステップ２０９０）、受信者コンピュータが認証されなかったと判定されるならば、受信者コンピュータのブック・データ要求は拒否される（ステップ２１００）。
【００２８】
図１０に示されるように、ブック・データの要求９０及び受信者コンピュータ固有の公開鍵が、受信者コンピュータから送出者コンピュータへ送信される（ステップ２１１０、２１２０）。（特定の実施の形態においては、この要求は、受信者コンピュータにおいて、固有の通し番号と、送出者コンピュータからの応答が時間内に受取られなければ要求満了時間で要求が取消される、例えば６０秒などの要求満了時間とに関連付けられ、送出者コンピュータから受信者コンピュータへの任意の応答が受信者コンピュータにおける要求に一致し得るように、この応答が同じ固有の要求通し番号と関連付けられる。）送出者コンピュータでは、機密鍵暗号化ブック・データと、機密鍵及び要求に対応する証明書とが選択され（ステップ２１３０）、受信者固有の公開鍵を用いて、公開鍵で暗号化された機密鍵及び証明書９４を生成し（ステップ２１４０）、これが機密鍵で暗号化されたブック・データと共に送出者コンピュータから受信者コンピュータへ送られる（ステップ２１５０、２１６０）。
【００２９】
受信者コンピュータ（図１１）では、受信者固有の秘密鍵を用いて機密鍵及び証明書９８を生成し（ステップ２１８０）、この機密鍵を用いて、機密鍵で暗号化されたブック・データから、暗号化されないブック・データ１００を生成する（ステップ２１９０）。この時点で、暗号化されないブック・データは、受信者コンピュータに表示され、或いは他の方法で使用される。
【００３０】
少なくとも幾つかの場合では、暗号化されないブック・データが、指定した方法で（例えば、アドビ表示ソフトウエアにより）データを表示させるけれどもデータ又はデータのリフォーマットの印刷は難しいか不可能にするフォーマット（例えば、移植可能なドキュメント・フォーマットすなわち「ＰＤＦ」として知られる、アドビ・フォーマットの一バージョン）であるならば、有利である。「移植可能ドキュメント・フォーマットの参照マニュアル」バージョン第１．２号、１９９６年１１月（Ａｄｏｂｅ　Ｓｙｓｔｅｍｓ社）を

参照されたい。このように、暗号化されないブック・データの創始者（例えば、出版業者）は、ブック・データの保全が配布後も存続し、ブック・データが起点の意図通りに（例えば、意図されたフォント及び印字サイズで、意図された行及び頁の送りで）表示されるという高度の信頼性を持つことができる。

【００３１】

使用許可転送手順は、データ項目の使用の許可が（例えば、図書館により）貸出され、賃貸しされ、（例えば、誕生日のプレゼントとして）贈られ、或いは（例えば、書籍店により）販売されるときに適用される。この許可が貸出され或いは賃貸しされるならば、送出者コンピュータと受信者コンピュータにおいて、前記手順は機密鍵が合致する満了時間１０２Ｓ、１０２Ｒ（例えば、それぞれ２週間の期間に相当）とそれぞれ関連付けられ、送出者コンピュータにおいて満了時間１０２Ｓに達するまで機密鍵を使用できない（従って、データ項目も使用できない）ようにし、受信者コンピュータにおいては満了時間１０２Ｒに達するまで使用できるようにすることも規定する。このように、当該許可は、満了時間になると、受信者コンピュータから送出者コンピュータへ有効に戻される。送出者コンピュータ又は受信者コンピュータが、同じデータ項目に対して複数のエンドユーザー・コンピュータに対する許可データを有するならば（例えば、多数のエンドユーザー・コンピュータへ貸出しが可能である図書館の場合）、異なる許可のインスタンスが相互に弁別できるように、合致する通し番号１０４Ｓ、１０４Ｒが貸出し又は賃貸のトランザクション毎に保持される。証明書は、満了時間と通し番号を規定し、また受信者コンピュータが１つ以上のエンドユーザー・コンピュータのデータ項目に対するアクセス取得を許容する許可データを与えられるならば（例えば、出版業者コンピュータが卸売業者コンピュータに５０台のエンドユーザー・コンピュータに関する許可データを与える場合）、数量１０６を規定する。証明書はまた、貸出し又は賃貸の期間中に受信者コンピュータが、別の受信者コンピュータによる使用許可転送手順において規定されたデータ項目に対して送出者コンピュータとして働くことを許可されるかどうかも規定する（例えば、許可の有効な再貸出し或いは再賃貸のため）。

【００３２】

贈答或いは販売の場合は、受信者コンピュータは、機密鍵を不明確に保持する資格、及び以後のトランザクションにおいて送出者コンピュータとして働く資格が与えられる。贈答又は販売の関係における使用許可転送手順の実行の開始時に、送出者コンピュータがエンドユーザー・コンピュータの１つ（例えば、それ自体）のみがデータ項目に対するアクセスを取得することを許容する許可データを持っていたならば、受信者コンピュータが機密鍵を与えられた後に、この機密鍵は送出者コンピュータにおいて消去される。

【００３３】

賃貸又は販売の場合は、許可は、使用許可転送手順とは完全に独立に送達が取扱われる料金の交換時に与えられ、或いは料金が支払われる前には許可が与えられないことの保証に役立つように使用許可転送手順に連携される別の手順により取扱われる。送出者コンピュータは、収入会計を可能にする監査ファイルの生成も行う。

【００３４】

使用許可転送手順に従って、データ項目、データ項目へのアクセス、或いはその両方をコンピュータ間（例えば、エンドユーザー・コンピュータ間）に転送することができるゆえに、自動車が代替可能であり且つ再販価値がを持つように、アクセス或いはデータ項目或いはその両方が代替可能であり、再販価値を有する。例えば、使用許可転送手順は、エンドユーザーが５ドルで小売業者からブック・データ項目へのアクセスのインスタンスを購入或いは賃借りし、ブック・データ項目を（例えば、ブック・データ項目のテキストを読むことにより）楽しみ、次にこのアクセスのインスタンスを別のエンドユーザーへ（例えば、インスタンスが品薄などの理由で価格が高騰したか或いは破損したデータに対する保証がないなどの理由から減価したかに従って、５ドル以上又は以下で）売渡すことを可能にする。

【００３５】

少なくとも或る場合には、送出者コンピュータ及び受信者コンピュータの各々における少なくとも監査ファイル、機密鍵、公開鍵／秘密鍵セット、許可データ・バンク、群秘密鍵及び解読器が高度な機密保持方法、例えば先に述べたスマートカード・コンピュータにおいて格納され使用されるならば、有利である。スマートカード・コンピュータ４６が使用されるものとして、群秘密鍵及びスマートカード・コンピュータ固有の秘密鍵がどんな形態でもスマートカード・コンピュータ外へは決して送信されなければ（すなわち、接続回路に決して提供されなければ）、且つ、機密鍵が暗号化されない形態では決して送信されないならば、機密保持は強化される。暗号化されたデータ項目は、鍵とは別個に（例えば、スマートカード・コンピュータ内の制限されたデータ記憶スペースのためスマートカード・コンピュータ外のハード・ディスクのような耐久性の高いメモリに）格納される。いずれの場合も、暗号化データ項目が必要に応じて一時に個々に（例えば、表示の目的のため一時に１頁）のみ解読されるならば、機密保持は更に強化される。

【００３６】

機密保持は、送出者コンピュータと受信者コンピュータ間の機密保持ネットワーク接続の使用によっても強化される。例えば、特定の実施の形態においては、送出者コンピュータは、少なくとも部分的にＨＴＭＬ、ＨＴＴＰ及びＴＣＰ／ＩＰ（インターネットのネットワーク）のようなインターネット規格に合致するネットワークを介して受信者コンピュータが接続されるウェブ・サーバを含む。ハイパーテキスト転送プロトコル（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）－ＨＴＴＰ １．１．ＲＰＣ２０６８を参照されたい。このような場合は、送出者コンピュータと受信者コンピュータとの間のインターネットのネットワーク接続が機密保持ソケット・レイヤ（ＳＳＬ）規格に従って動作するならば、機密保持が強化される。機密保持ソケット・レイヤ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）仕様書３．０（Ｎｅｔｓｃａｐｅ社）を参照されたい。ウェブ・サーバは、（例えば、出版業者、卸売業者、或いは小売業者に対する）デマンド駆動型配布センターとして働き、ここから（例えば、卸売業者、小売業者又はエンドユーザーに対する）受信者コンピュータは（例えば、ウェブ・ブラウザを走らせている）受信者コンピュータにおいて（例えば、ウェブ・サーバのウェブ・ページを介して）選択可能であるデータ項目をダウンロードできる。受信者コンピュータは、送出者コンピュータから、ソフトウエア（例えば、表示ソフトウエア、或いは使用許可の転送手順の少なくとも一部を実現するソフトウエア）をダウンロードすることができる。

【００３７】

送出者コンピュータと受信者コンピュータとの間の接続は、１つ以上の有線或いは無線のデータ転送手法（例えば、電話回線、セルラー電話、或いは赤外線送信におけるモデム・ダイアルアップ）によって達成することができる。

【００３８】

特定の実施の形態においては、送出者コンピュータ又は受信者コンピュータは、次に記述するような特殊目的のブック閲覧コンピュータ１１０（図１５）（ブック・リーダ）を含む。このブック・リーダは、ブック・データ（テキスト情報を含む）を明瞭に表示するのに使用できる手持ち型のバッテリ駆動装置であり、マイクロソフト社のＷｉｎｄｏｗｓ（登録商標）ＣＥ２．１のようなオペレーティング・システムを走らせる３２ビットのマイクロコンピュータ（例えば、フィリップス・セミコンダクタ社のＰＲ３７１００、ＭＩＰＳプロセッサ、或いはインテル社のＳｔｒｏｎｇＡＲＭ １１００プロセッサ、及びＵＣＢ１２００周辺制御チップ）を含む。支援用電子装置を用いるポートレート・モードの液晶ディスプレイ（ＬＣＤ）のスクリーン１１２（例えば、ＰＲ３７１００プロセッサが用いられる場合、Ｓ－ＭＯＳシステムＳＥＤ１３５５ビデオ・コントローラ・チップにより駆動されるシャープのＨＲ－ＴＦＴ ＬＱ０８４Ｖ２ＤＳ０１ ８．４インチＶＧＡ（６４０×４８０）反射型ＴＦＴカラーＬＣＤ）もまた、キーボードとマウスのないブック・リーダに含まれる。このブック・リーダは、防眩コーティングを備えた４線式抵抗タッチ・スクリーン、１６ＭＢのＤＲＡＭ、オペレーティング・システム用の８ＭＢのフラッシュＲＯＭ、及び組込みソフトウエア、ブック・データの記憶のための８ＭＢフラッシュ・

メモリ・カードを装填したコンパクトなフラッシュ・メモリ・スロット、及びパーソナル・コンピュータの接続のためのマイクロコンピュータの組込み能力の使用が可能なＩｒＤＡ赤外線インターフェースをも有する。更に、このブック・リーダは、ＲＪ－１１電話ジャック、マイクロコンピュータの組込み能力及び直結インターネット接続用のＳｏｆｔｍｏｄｅｍソフトウエアを使用するＤＡＡ及びモデム・インターフェース、「Ｎｅｘｔ　Ｐａｇｅ」、「Ｐｒｅｖ　Ｐａｇｅ」、「Ｍｅｎｕ」、「Ｅｎｔｅｒ」及び「Ｒｅｓｅｔ」の押しボタン、及び「Ｏｆｆ」、「Ｒｅａｄ」、「Ｂｏｏｋｓ」、「Ｌｉｂｒａｒｙ」Ａｎｄ「Ｂｏｏｋｓｔｏｒｅ」の位置を持つスライド型のモード・スイッチを有する。ブック・リーダには、４つのＡＡバッテリ（アルカリ電池ならば、４０時間以上の動作が可能）、（例えば、マイクロコンピュータに対する）電力節減モードをサポートするＡＣアダプタ電源、高品質のタッチ・スクリーン・スタイラス、及びスマートカード・コンピュータ用のスマートカード・スロットもまた含まれる。

【００３９】

当該ブック・リーダは、革で装丁された書籍に似た或いはこれを示唆するようにパッケージされ、高さが８インチ、幅が５．２５インチであり、内蔵された構成要素の観点から実用的なように薄く軽量（例えば、１．５ポンド）である。このＬＣＤスクリーンは、縦方向に配向され（すなわち、４８０×６４０）、ＬＣＤスクリーン周囲のＬＣＤ枠は耐久性を不当に損なうことなく実用的な小ささである。「Ｎｅｘｔ　Ｐａｇｅ」及び「Ｐｒｅｖ　Ｐａｇｅ」の押しボタンは、くぼみがあり、ＬＣＤ枠の左右側の略々中心に置かれている。「Ｍｅｎｕ」及び関連する押しボタンは、ＬＣＤ枠の底部に配置される。これら押しボタンは、押すのが快適且つ容易であり、略々完全に無騒音でありながら、押されたとき充分な反動感を生じる。スライド型モード・スイッチは、くぼみがあり、ブック・リーダの右側に配置されている。Ｒｅｓｅｔボタンは、Ｒｅｓｅｔボールの付勢を生じるのにボール・ペン又は類似の用具を必要とするように深いくぼみがある。赤外線トランシーバの枠は、ブック・リーダの最上縁部に配置され、ＲＪ－１１及びＡＣ電源アダプタ・ジャックはブック・リーダの底縁部に配置され、コンパクトなフラッシュ・メモリ・スロットはブック・リーダの背面に配置されている。ブック・リーダの外部はマグネシウムで造られ、ブック・リーダの美観と耐久性を強化し、ブック・リーダ及びブック・リーダのＬＣＤスクリーンの保護のため連結された折り畳み用レザー・カバー１１４により覆われている。

【００４０】

少なくとも或る場合には、美しい細部によりブック・リーダが視覚的にエレガントで豊かに見える素材（例えば、レザー、ガラス、マグネシウム）及びプラスチック・ラバー状のハンド・グリップを持ち、実質的に耐候性がある（例えば、ディスプレイ及びボタン周りにガスケットを備える）ならば好ましい。

【００４１】

他の特定の実施の形態においては、送出者コンピュータ又は受信者コンピュータは、ノートブック・コンピュータ或いはデスクトップ・コンピュータを含む。いずれの場合も、高度な機密保持機構は、高度な機密保持データ・ファイル或いは高度な機密保持ソフトウエア、或いはその両方を含み、或いは（例えば、直列、並列或いはＵＳＢポートに取付けられ、或いはＰＣＭＣＩＡスマートカード・アダプタへ差込まれ、或いはマザーボードに埋設されたデバイスの形態で集積された）スマートカード・コンピュータを含む。

【００４２】

当該技法（すなわち、先に述べた手順）は、ハードウエア又はソフトウエアいおいて、或いはその両方の組合わせにおいて実現される。少なくともある場合には、当該技法は、それぞれプロセッサ、プロセッサにより読出し可能な記憶媒体（揮発性及び非揮発性メモリ及び／又は記憶素子を含む）、キーボードなどの少なくとも１つの入力装置、及び少なくとも１つの出力装置を含むプログラム可能なコンピュータ（例えば、マイクロソフト社のＷｉｎｄｏｗｓ（登録商標）９５、９８又はＮＴ、或いはマッキントッシュＯＳを走らせ或いはこれを走らせることができるパーソナル・コンピュータ）上で実行するコンピュー

タ・プログラムにおいて実現されるならば好ましい。プログラム・コードは、入力装置を用いて入力されるデータへ与えられ、先に述べた方法を実施し、出力情報を生成する。この出力情報は、コンピュータの表示スクリーンのような１つ以上の出力装置へ与えられる。

【００４３】

少なくとも或る場合には、各プログラムは、コンピュータ・システムと通信するためＪａｖａ（登録商標）又はＣ＋＋のような高レベルの手順又はオブジェクト指向のプログラミング言語で実現される。しかし、プログラムは、必要ならばアセンブリ言語又は機械言語で実現することができる。いずれの場合も、この言語はコンパイルされた又は解釈された言語でよい。

【００４４】

少なくとも或る場合には、記憶媒体又は記憶装置が本文に述べた手順を実行するためコンピュータにより読出されるとき、コンピュータを構成して動作させるための汎用又は特殊目的のプログラム可能なコンピュータ読出し可能なこのような各コンピュータ・プログラムが記憶媒体又は記憶装置（例えば、ＲＯＭ又は磁気ディスケット）に格納されるならば、有利である。システムもまた、コンピュータ・プログラムにより構成されたコンピュータ可読な記憶媒体として実現されると考えられ、この場合このように構成された記憶媒体はコンピュータを特定の予め規定された方法で動作させる。

【００４５】

他の実施の形態は請求の範囲内に含まれる。例えば、受信者コンピュータは、先に述べたようなスマートカード・コンピュータにより行われる諸機能の少なくとも一部を実行することを助ける回路（例えば、コンピュータのポート、或いはメモリ・デバイスがエポキシに埋設されたプラグイン又はＰＣＭＣＩＡカードに取付けるドングル）を含むデスクトップ・コンピュータ又は携帯可能なコンピュータを含む。このような場合は、データ項目は、デスクトップ・コンピュータ又は携帯可能なコンピュータの表示スクリーン上に表示される。

【００４６】

スマートカード・コンピュータにより行われる諸機能の少なくとも一部は、代わりに、完全に又は実質的にソフトウェアで実行されるが、これはスマートカード・コンピュータの使用ほど安全な配置ではない。

【００４７】

データ項目は、定期刊行物（例えば、雑誌）のテキスト、オーディオ・データ（例えば、音楽）或いは視覚的データ（例えば、スチール写真又はビデオ）を含む任意の形式のデータを含む。

【００４８】

他の手法は、群秘密鍵の不当な流布或いはこのような流布の好ましからざる結果の阻止に資するために用いられる。例えば、群秘密鍵が複雑なスペクトラム拡散無線転送手法によってのみ検索可能であり、或いは他の方法でハードウエアにおいて更に保護され、或いは一時的にのみ有効であるように処置される。

【００４９】

送出者コンピュータと受信者コンピュータとの間のトランザクション時間の短縮のような理由のため、許可データのみを送出者コンピュータから受信者コンピュータへ送るだけで済むように、暗号化データ項目は公衆がアクセス可能な場所（例えば、インターネット上）に格納される。このような場合、暗号化データ項目はだれでも自由に転送しコピーすることができるが、許可データは使用許可の転送手順の制御下でのみ送られる。

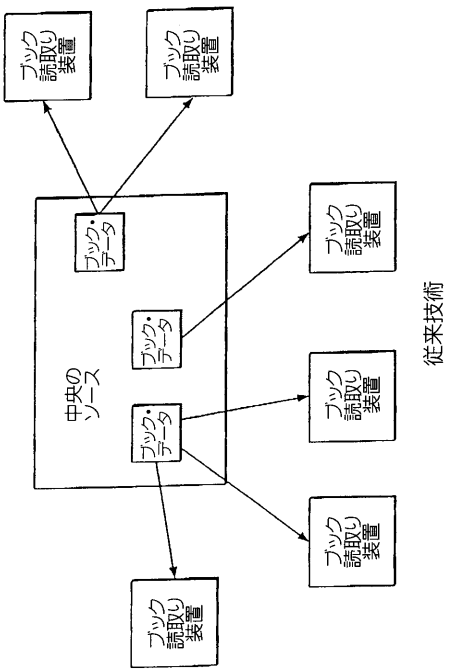
【図面の簡単な説明】

【図１】　ブック読取り装置がブック・データを中央のソースから受取る従来技術のブック・データ配布システムを示すブロック図である。

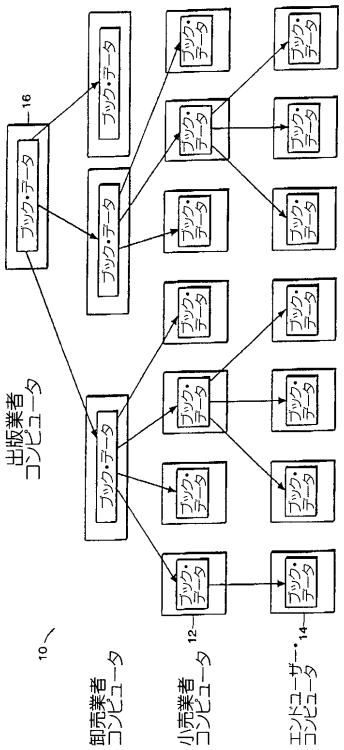
【図２】　ブック・データが出版業者コンピュータから卸売業者コンピュータへ、更に小売業者コンピュータへ、更にはエンドユーザー・コンピュータへ送られるブック・データ

配布システムを示すブロック図である。
【図３】　出版業者、卸売業者、小売業者及びエンドユーザーのコンピュータ間の許可の転送を示すブロック図である。
【図４】　ユーザー・コンピュータ間の許可データの転送を示すブロック図である。
【図５】　使用許可転送手順を示すフロー図である。
【図６】　スマートカード・コンピュータを示すブロック図である。
【図７】　群及び秘密鍵を示すブロック図である。
【図８】　使用許可転送手順におけるデータ・フローを示すブロック図である。
【図９】　使用許可転送手順におけるデータ・フローを示すブロック図である。
【図１０】　使用許可転送手順におけるデータ・フローを示すブロック図である。
【図１１】　使用許可転送手順におけるデータ・フローを示すブロック図である。
【図１２】　使用許可転送手順を示すフロー図である。
【図１３】　使用許可転送手順を示すフロー図である。
【図１４】　使用許可転送手順を示すフロー図である。
【図１５】　ブック閲覧装置を示す図である。

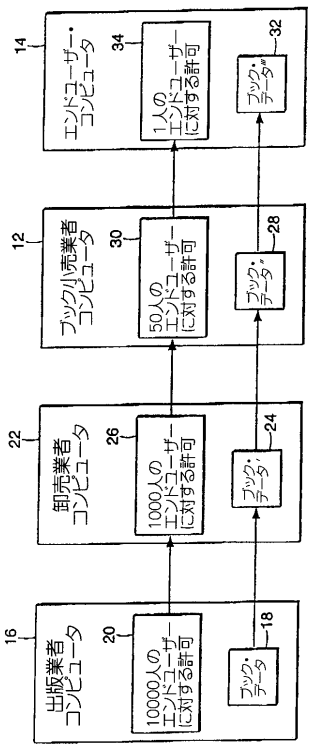
【図１】



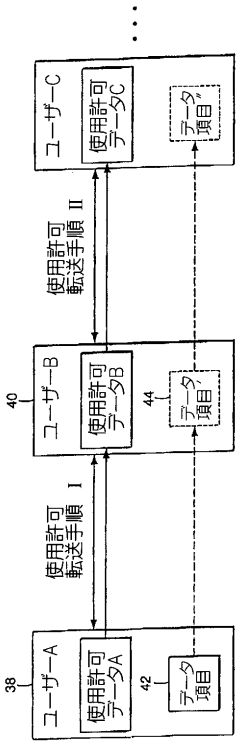
【図２】



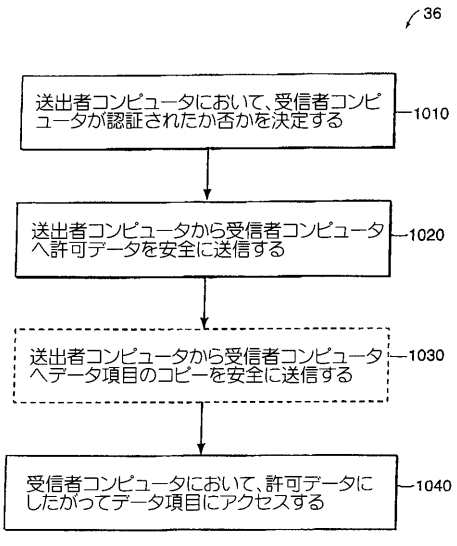
【図３】


14
エンドユーザー・コンピュータ
34
1人のエンドユーザーに対する許可
32
ブック・データ"
12
ブック小売業者コンピュータ
30
50人のエンドユーザーに対する許可
28
ブック・データ'
22
卸売業者コンピュータ
26
1000人のエンドユーザーに対する許可
24
ブック・データ'
16
出版業者コンピュータ
20
10000人のエンドユーザーに対する許可
18
ブック・データ

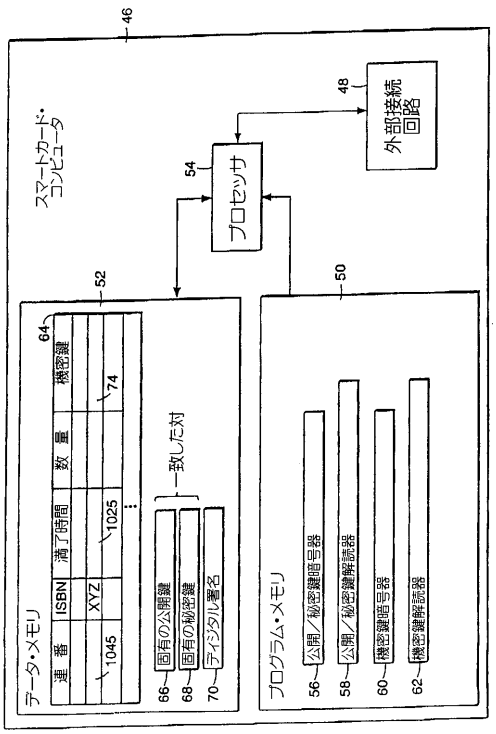
【図４】


ユーザーC
使用許可データC
データ項目"
使用許可転送手順 II
40
ユーザーB
使用許可データB
44
データ項目'
使用許可転送手順 I
38
ユーザーA
使用許可データA
42
データ項目

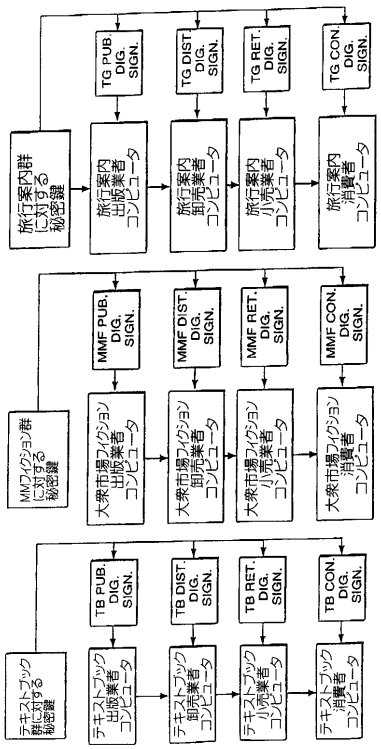
【図５】


36
送出者コンピュータにおいて、受信者コンピュータが認証されたか否かを決定する
1010
送出者コンピュータから受信者コンピュータへ許可データを安全に送信する
1020
送出者コンピュータから受信者コンピュータへデータ項目のコピーを安全に送信する
1030
受信者コンピュータにおいて、許可データにしたがってデータ項目にアクセスする
1040

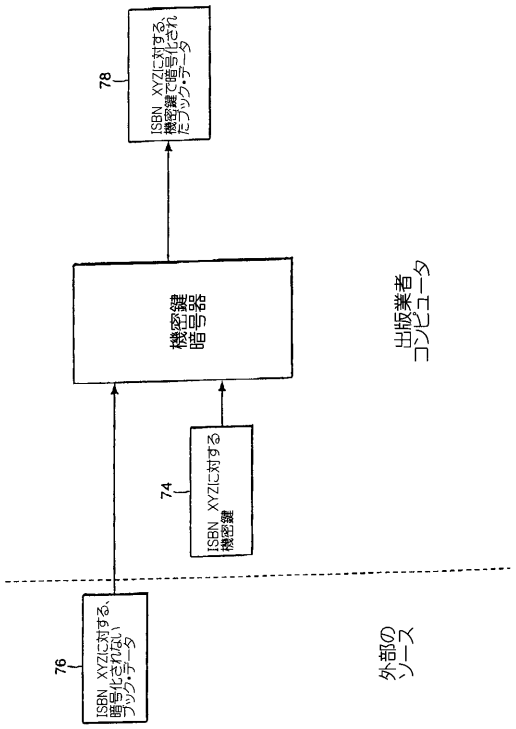
【図６】


46
スマートカード・コンピュータ
48
外部接続回路
54
プロセッサ
52
50
データ・メモリ
連番
ISBN
満了時間
数量
機密鍵
1045
XYZ
1025
74
64
66 固有の公開鍵
68 固有の秘密鍵
70 ディジタル署名
一致した対
プログラム・メモリ
56 公開／秘密鍵暗号器
58 公開／秘密鍵解読器
60 機密鍵暗号器
62 機密鍵解読器

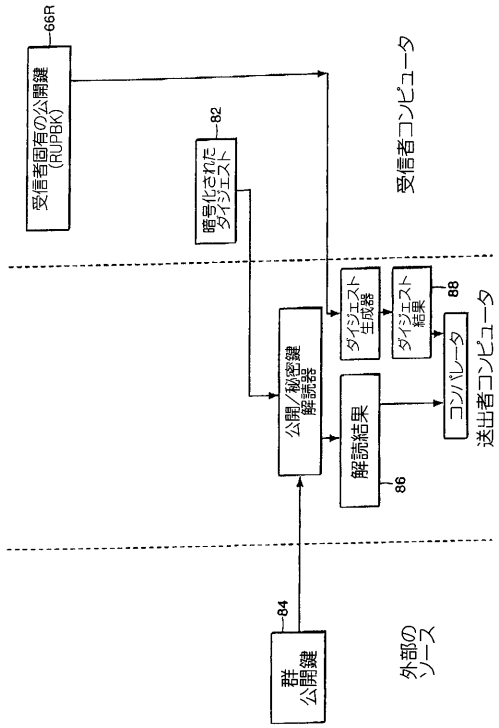
【図７】


旅行案内群に対する秘密鍵
TG PUB. DIG. SIGN.
TG DIST. DIG. SIGN.
TG RET. DIG. SIGN.
TG CON. DIG. SIGN.
旅行案内出版業者コンピュータ
旅行案内卸売業者コンピュータ
旅行案内小売業者コンピュータ
旅行案内消費者コンピュータ
MMフィクション群に対する秘密鍵
MMF PUB. DIG. SIGN.
MMF DIST. DIG. SIGN.
MMF RET. DIG. SIGN.
MMF CON. DIG. SIGN.
大衆市場フィクション出版業者コンピュータ
大衆市場フィクション卸売業者コンピュータ
大衆市場フィクション小売業者コンピュータ
大衆市場フィクション消費者コンピュータ
テキストブック群に対する秘密鍵
TB PUB. DIG. SIGN.
TB DIST. DIG. SIGN.
TB RET. DIG. SIGN.
TB CON. DIG. SIGN.
テキストブック出版業者コンピュータ
テキストブック卸売業者コンピュータ
テキストブック小売業者コンピュータ
テキストブック消費者コンピュータ

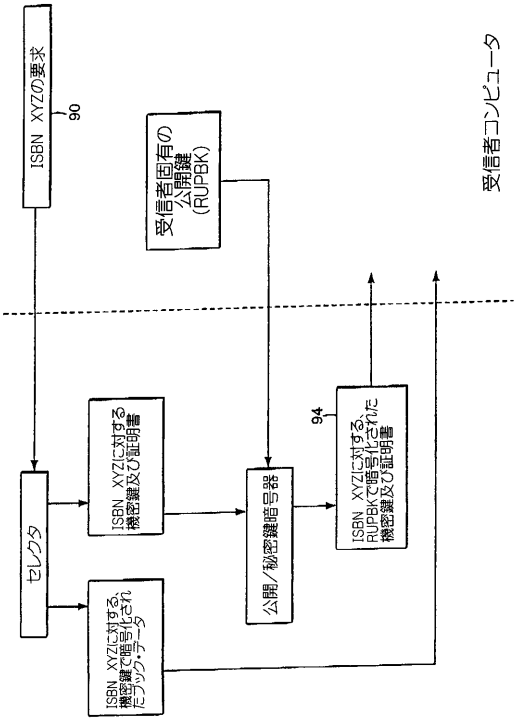
【図８】


78
ISBN XYZに対する機密鍵で暗号化されたブック・データ
機密鍵暗号器
出版業者コンピュータ
74
ISBN XYZに対する機密鍵
76
ISBN XYZに対する暗号化されないブック・データ
外部のソース

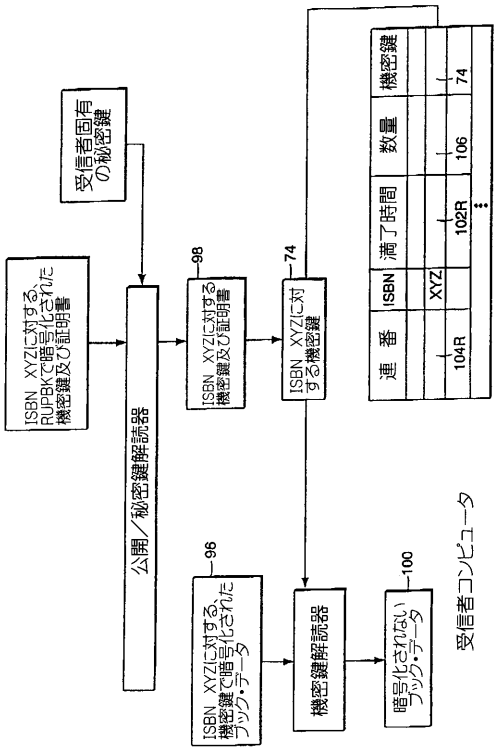
【図９】


66R
受信者固有の公開鍵(RUPBK)
82
暗号化されたダイジェスト
受信者コンピュータ
公開／秘密鍵解読器
ダイジェスト生成器
ダイジェスト結果
コンパレータ
88
解読結果
86
送出者コンピュータ
84
群公開鍵
外部のソース

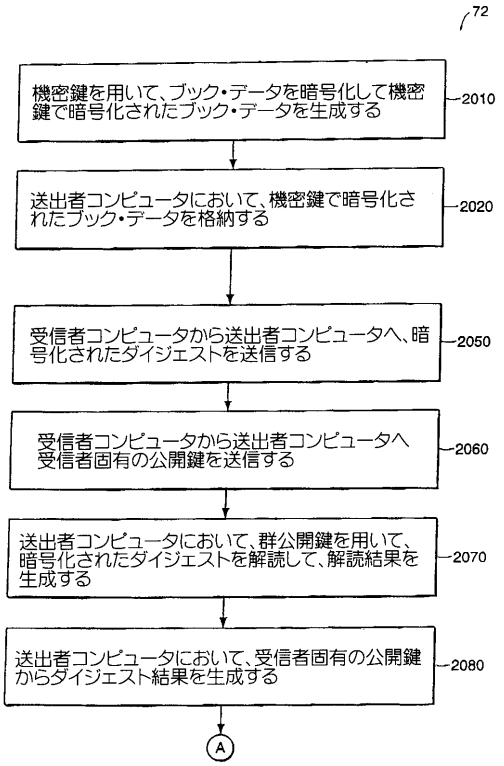
【図１０】


ISBN XYZの要求
90
受信者固有の公開鍵(RUPBK)
セレクタ
ISBN XYZに対する機密鍵及び証明書
ISBN XYZに対する機密鍵で暗号化されたブック・データ
公開／秘密鍵暗号器
94
ISBN XYZに対するRUPBKで暗号化された機密鍵及び証明書
受信者コンピュータ

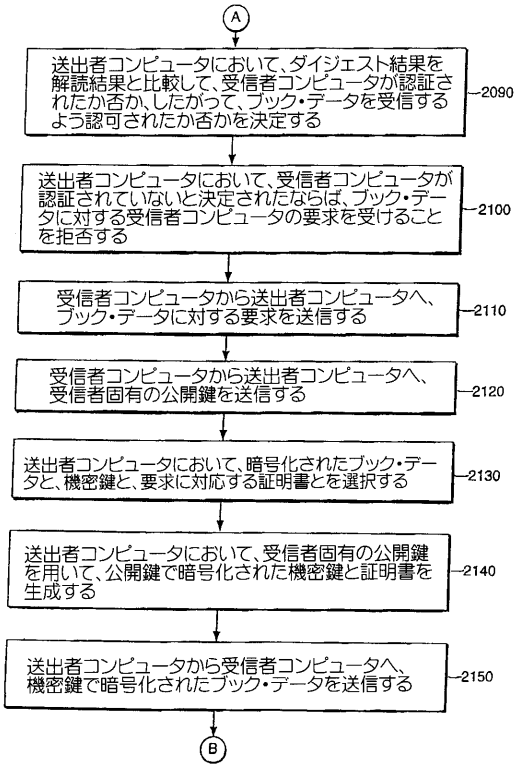
【図１１】



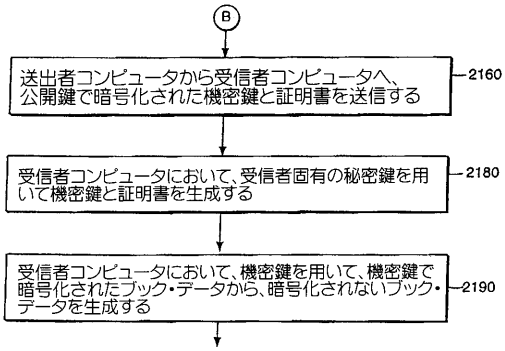
【図１２】



【図１３】



【図１４】



フロントページの続き

(51)Int.Cl. FI
G06F 17/30 170Z
H04L 9/00 621A

(74)代理人 100096013
弁理士 富田 博行
(74)代理人 100091063
弁理士 田中 英夫
(72)発明者 ケイウェル, レオナルド・エム, ジュニア
アメリカ合衆国マサチューセッツ州, コンコルド
(72)発明者 ディアス, トーマス・アール
アメリカ合衆国マサチューセッツ州, レキシントン
(72)発明者 ハイネン, メアリー・エレン
アメリカ合衆国マサチューセッツ州, コンコルド
(72)発明者 ハイネン, ロジャー・ジェイ, ジュニア
アメリカ合衆国メイン州, アイルズボロ

審査官 田内 幸治

(56)参考文献 国際公開第９６／０２７１５５（WO, Ａ１）
特表平１０－５１２０７４（ＪＰ, Ａ）
国際公開第９８／００８３４４（WO, Ａ１）
特開平０８－０６３４３６（ＪＰ, Ａ）
特開平０８－２６３４４１（ＪＰ, Ａ）
米国特許第０５７３４８２３（ＵＳ, Ａ）
福永 勇二 Yuji Fukunaga, 電子メールのプライバシーを守る！, ｎｅｔ ＰＣ 第3巻 第４号, 日本, 株式会社アスキー, １９９８年 4月 1日, Ｐ. １６１－Ｐ. １６７

(58)調査した分野(Int.Cl., ＤＢ名)
G06Q 10/00-50/00
G06F 17/30
H04L 9/08
H04L 9/10