世界知的所有権機関
国際事務局
PCT
特許協力条約に基づいて公開された国際出願

RECEIVED 12 JAN 1996 REGISTRY OF TRADE MARKS & PATENTS SINGAPORE

(51) 国際特許分類6
G06F 9/06

A1

(11) 国際公開番号 WO95/29438

(43) 国際公開日 1995年11月2日 (02.11.95)

(21) 国際出願番号 PCT/JP95/00796
(22) 国際出願日 1995年4月21日(21.04.95)

(30) 優先権データ
特願平6/106316 1994年4月22日(22.04.94) JP

(71) 出願人（米国を除くすべての指定国について）
株式会社 アドバンス(KABUSHIKI KAISYA ADVANCE)[JP/JP]
〒103 東京都中央区日本橋小舟町5番7号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
大槻和則(OTSUKI, Kazunori)[JP/JP]
〒241 神奈川県横浜市旭区中希望が丘35-2 Kanagawa, (JP)
渡辺晋一郎(WATANABE, Shinichirou)[JP/JP]
〒174 東京都江戸川区小松川1-2-3
コーシャタワー小松川902 Tokyo, (JP)
(74) 代理人
弁理士 石田 敬, 外(ISHIDA, Takashi et al.)
〒105 東京都港区虎ノ門一丁目8番10号
静光虎ノ門ビル 青和特許法律事務所 Tokyo, (JP)

(81) 指定国
CA, CN, KR, SG, US, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類 国際調査報告書

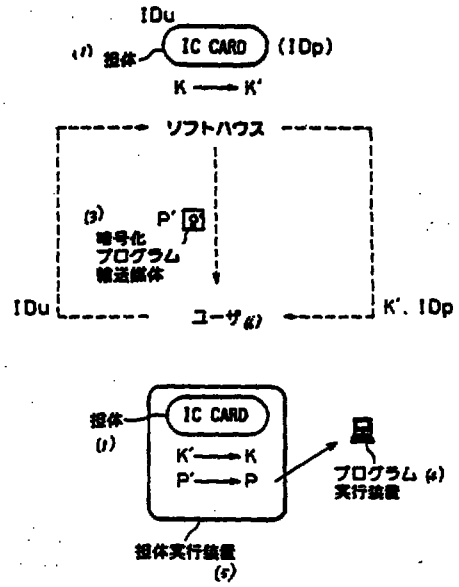
RTMP's copy

(54) Title : DATA PROTECTION SYSTEM

(54) 発明の名称 データプロテクト方式

(57) Abstract

A data protection system which enables a qualified user to use target data but inhibits other users to use the data, though enabling them to copy the data. The system has the following construction. A center generates a specific algorithm, that is, a center algorithm which only the center holds in secrecy. The center applies the center algorithm to open identifiers peculiar to data and users, which are used semi-fixedly, so as to generate secret algorithms for exclusive use for the data and users, and supplies them to user and data suppliers. Before a data transfer, the data supplier inputs the identifier of the user to the secret algorithm of the data to be supplied and thus generates the same and inherent cipher key between the data and the user. Then, the whole or part of the data is encrypted either directly or indirectly on the basis of this cipher key and is supplied to the user. The user inputs the identifier of the data supplied to his own secret algorithm at the time of use, generates the same and inherent cipher key between the supplied data and the user and decodes the encrypted data either directly or indirectly.



(1) ... support
(2) ... soft house
(3) ... encrypted program transportation medium
(4) ... program execution apparatus
(5) ... support execution apparatus
(6) ... user

（５７）要約

ターゲットとなるデータを、正当なユーザは、簡単な操作により使用ができるが、その他のユーザは、コピーはできても使用ができないデータプロテクト方式。

センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、データ並びにユーザのそれぞれに固有で公開され且つ半固定的に用いられる各データ並びにユーザの識別子にセンタアルゴリズムを施して各データ並びにユーザに専用な秘密アルゴリズムを作成し、ユーザ及びデータ供給体に供給するという準備を行った後、データ供給体とユーザとの間で、データの供給が生じた場合、データ供給体は、ユーザの識別子を供給対象となるデータの秘密アルゴリズムに入力することによって、供給対象となるデータとユーザとの間で同一且つ固有の暗号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるデータの一部又は全部を暗号化してユーザへ供給し、ユーザは、使用時、供給されたデータの識別子を自己の秘密アルゴリズムに入力することによって、供給されたデータとユーザとの間で同一且つ固有の暗号鍵を作成し暗号化データを直接的又は間接的に復号化する方式によりなる。

情報としての用途のみ
ＰＣＴに基づいて公開される国際出願をパンフレット第一頁にＰＣＴ加盟国を同定するために使用されるコード

AM	アルメニア	ES	エストニア	LK	スリランカ	RU	ロシア連邦
AT	オーストリア	FI	フィンランド	LR	リベリア	SD	スーダン
AU	オーストラリア	FR	フランス	LS	レソト	SE	スウェーデン
BB	バルバドス	GA	ガボン	LT	リトアニア	SG	シンガポール
BE	ベルギー	GB	英国	LU	ルクセンブルグ	SI	スロヴェニア
BF	ブルキナ・ファソ	GE	グルジア	LV	ラトヴィア	SK	スロヴァキア共和国
BG	ブルガリア	GN	ギニア	MC	モナコ	SN	セネガル
BJ	ベナン	GR	ギリシャ	MD	モルドバ	SZ	スワジランド
BR	ブラジル	HU	ハンガリー	MG	マダガスカル	TD	チャード
BY	ベラルーシ	IE	アイルランド	ML	マリ	TG	トーゴ
CA	カナダ	IL	イスラエル	MN	モンゴル	TJ	タジキスタン
CF	中央アフリカ共和国	IS	アイスランド	MR	モーリタニア	TM	トルクメニスタン
CG	コンゴー	IT	イタリー	MW	マラウイ	TT	トリニダード・トバゴ
CH	スイス	JP	日本	MX	メキシコ	UA	ウクライナ
CI	コート・ジボアール	KE	ケニア	NE	ニジェール	UG	ウガンダ
CM	カメルーン	KG	キルギスタン	NL	オランダ	US	米国
CN	中国	KP	朝鮮民主主義人民共和国	NO	ノルウェー	UZ	ウズベキスタン共和国
CS	チェッコ共和国	KR	大韓民国	NZ	ニュージーランド	VN	ヴィエトナム
CZ	チェッコ	KZ	カザフスタン	PL	ポーランド		
DE	ドイツ	LI	リヒテンシュタイン	PT	ポルトガル		
DK	デンマーク			RO	ルーマニア		