

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4486851号
(P4486851)

(45) 発行日 平成22年6月23日(2010.6.23)

(24) 登録日 平成22年4月2日(2010.4.2)

(51) Int.Cl.		F I			
HO4L	9/08	(2006.01)	HO4L	9/00	601A
GO6F	21/24	(2006.01)	GO6F	12/14	510F
GO9C	1/00	(2006.01)	GO6F	12/14	530P
			GO6F	12/14	540P
			GO9C	1/00	650Z

請求項の数 16 (全 40 頁)

(21) 出願番号	特願2004-169004 (P2004-169004)	(73) 特許権者	399035766
(22) 出願日	平成16年6月7日(2004.6.7)		エヌ・ティ・ティ・コミュニケーションズ
(65) 公開番号	特開2005-346659 (P2005-346659A)		株式会社
(43) 公開日	平成17年12月15日(2005.12.15)		東京都千代田区内幸町一丁目1番6号
審査請求日	平成19年6月6日(2007.6.6)	(74) 代理人	100083806
			弁理士 三好 秀和
		(74) 代理人	100095500
			弁理士 伊藤 正和
		(74) 代理人	100101247
			弁理士 高橋 俊一
		(74) 代理人	100098327
			弁理士 高松 俊雄

最終頁に続く

(54) 【発明の名称】 機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラム

(57) 【特許請求の範囲】

【請求項1】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

10

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、

所定の初期情報を生成する初期情報生成手段と、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情

20

報を、第2の記憶部に記憶させるデータ記憶手段と、

前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶手段と、

前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、

新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、

前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶手段と、

前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段と、

前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新手段と、
を有することを特徴とする機密情報管理システム。

【請求項2】

前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、

前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項1記載の機密情報管理システム。

【請求項3】

前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項1又は2記載の機密情報管理システム。

【請求項4】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項1乃至3のいずれか1項に記載の機密情報管理システム。

【請求項5】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項1乃至3のいずれか1項に記載の機密情報管理システム。

【請求項6】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理方法であって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり

10

20

30

40

50

、
前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

所定の初期情報を生成する初期情報生成ステップと、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶ステップと、

前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶ステップと、

前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、

新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、

前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶ステップと、

前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、

前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新ステップと、
を有することを特徴とする機密情報管理方法。

【請求項7】

利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

、
前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、

所定の初期情報を生成する初期情報生成ステップと、

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶ステップと、

前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶ステップと、

前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、

10

20

30

40

50

新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、

前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶ステップと、

前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、

10

前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新ステップと、を前記コンピュータに実行させることを特徴とする機密情報管理プログラム。

【請求項8】

前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、

前記乱数生成ステップは、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項7記載の機密情報管理プログラム。

【請求項9】

前記データ分割ステップの秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項7又は8記載の機密情報管理プログラム。

20

【請求項10】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項7乃至9のいずれか1項に記載の機密情報管理プログラム。

【請求項11】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項7乃至9のいずれか1項に記載の機密情報管理プログラム。

30

【請求項12】

利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムを利用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、

前記秘密分散法は、

前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

40

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記機密情報管理システムは、

前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、

所定の初期情報を生成する初期情報生成手段と、

50

前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶手段と、

前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶手段と、

前記利用者が前記機密情報を使用する場合には、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、

新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、

前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶手段と、を有し、

前記第1の記憶部に記憶された分割データ及び初期情報を第3の記憶部に記憶するステップと、

前記利用者が前記機密情報を使用するときは、前記機密情報管理システムから前記同期情報を受信するステップと、

前記初期情報及び前記同期情報に基づいて、前記機密情報管理システムで生成された新たな乱数と同じ乱数を生成する乱数生成ステップと、

新たに生成された乱数及び前記秘密分散法を用いて、前記第3の記憶部に記憶された分割データから、再分割データを生成するデータ再分割ステップと、

前記再分割データを前記機密情報管理システムに送信するステップと、

を前記端末に実行させ、前記機密情報管理システムは、送信された再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記同期情報を更新して前記第2の記憶部に記憶させることを特徴とする機密情報管理システム用端末プログラム。

【請求項13】

前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、

前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする請求項12記載の機密情報管理システム用端末プログラム。

【請求項14】

前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする請求項12又は13記載の機密情報管理システム用端末プログラム。

【請求項15】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項12乃至14のいずれか1項に記載の機密情報管理システム用端末プログラム。

【請求項16】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項12乃至14のいずれか1項に記載の機密情報管理システム用端末プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

10

20

30

40

50

本発明は、利用者の機密情報を管理する機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムに関する。

【背景技術】

【0002】

IT (Information Technology) 技術の発展に伴って、パスワード、クレジット番号などが入った携帯電話および携帯情報端末、並びにPKI秘密鍵が入ったICカードなどを用いて、所望のサービスの提供を受ける機会が増えている。例えば、ユーザのパスワードを使用してログインし、情報を閲覧したり、ユーザのクレジットカード番号を使用して物品購入したりするようなサービスが普及している。

【0003】

尚、この出願に関連する先行技術文献情報としては、次のものがある。

【非特許文献1】電子認証システム推進検討会、“企業間電子商取引システムにおける電子認証システムの仕様に関するガイドライン”、[Online]、[平成16年5月20日検索]、インターネット<URL: <http://www.ecom.or.jp/home/gl2.pdf>>

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、ユーザが上述したサービスを利用するときは、インターネット網などオープンなネットワークを介して機密情報(例えば、パスワード、クレジット番号およびPKI秘密鍵など)を送信することが多いので、第三者に機密情報が漏洩される可能性があるという課題がある。

【0005】

本発明は、上記の課題を解決するためになされたものであり、サービス利用時に仮にユーザの機密情報が第三者に漏洩したとしても、なりすましを確実に防止することができる機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

上記目的を達成するため、請求項1記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、所定の初期情報を生成する初期情報生成手段と、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶手段と、前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶手段と、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の

10

20

30

40

50

記憶部に記憶させるデータ再記憶手段と、前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元手段と、前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新手段と、を有することを特徴とする。

【0007】

請求項2記載の本発明は、請求項1記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

10

【0008】

請求項3記載の本発明は、請求項1又は2記載の発明において、前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【0009】

請求項4記載の本発明は、請求項1乃至3のいずれか1項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

20

【0010】

請求項5記載の本発明は、請求項1乃至3のいずれか1項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0011】

請求項6記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理方法であって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、所定の初期情報を生成する初期情報生成ステップと、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶ステップと、前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶ステップと、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、前記第2の記憶部に記憶された

30

40

50

各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶ステップと、前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新ステップと、を有することを特徴とする。

【0012】

請求項7記載の本発明は、利用者の機密情報を秘密分散法を用いて管理するためのコンピュータが読み取り可能な機密情報管理プログラムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割ステップと、所定の初期情報を生成する初期情報生成ステップと、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶ステップと、前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶ステップと、前記利用者が前記機密情報を使用する場合には、前記同期情報を前記利用者が備える端末に送信するとともに、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割ステップと、前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶ステップと、前記第1の記憶部に記憶された前記初期情報、及び前記端末に送信した前記同期情報から前記新たに発生させた乱数と同一の乱数を生成し、該乱数及び前記秘密分散法を用いて、前記第1の記憶部に記憶された分割データから、再分割データを生成する前記端末から送信された該再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元するデータ復元ステップと、前記同期情報を更新して前記第2の記憶部に記憶させる同期情報更新ステップと、を前記コンピュータに実行させることを特徴とする。

【0013】

請求項8記載の本発明は、請求項7記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成ステップは、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

【0014】

請求項9記載の本発明は、請求項7又は8記載の発明において、前記データ分割ステップの秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【0015】

請求項10記載の本発明は、請求項7乃至9のいずれか1項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0016】

請求項11記載の本発明は、請求項7乃至9のいずれか1項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

10

【0017】

請求項12記載の本発明は、利用者の機密情報を秘密分散法を用いて管理する機密情報管理システムを利用するための端末が読み取り可能な機密情報管理システム用端末プログラムであって、前記秘密分散法は、前記機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記機密情報管理システムは、前記機密情報を前記秘密分散法を用いて複数の分割データに分割するデータ分割手段と、所定の初期情報を生成する初期情報生成手段と、前記複数の分割データの一部及び前記初期情報を、前記利用者が保持するためのデータとして第1の記憶部に記憶させるとともに、前記複数の分割データの残り及び前記初期情報を、第2の記憶部に記憶させるデータ記憶手段と、前記第1の記憶部及び前記第2の記憶部に記憶された各分割データの同期をとるために設定された同期情報を前記第2の記憶部に記憶させる同期情報記憶手段と、前記利用者が前記機密情報を使用する場合には、前記同期情報及び前記初期情報に基づいて新たに乱数を生成する乱数生成手段と、新たに生成された乱数及び前記秘密分散法を用いて、前記第2の記憶部に記憶された各分割データから、再分割データを生成するデータ再分割手段と、前記第2の記憶部に記憶された各分割データを無効にして、前記再分割データを新たな分割データとして前記第2の記憶部に記憶させるデータ再記憶手段と、を有し、前記第1の記憶部に記憶された分割データ及び初期情報を第3の記憶部に記憶するステップと、前記利用者が前記機密情報を使用するときは、前記機密情報管理システムから前記同期情報を受信するステップと、前記初期情報及び前記同期情報に基づいて、前記機密情報管理システムで生成された新たな乱数と同じ乱数を生成する乱数生成ステップと、新たに生成された乱数及び前記秘密分散法を用いて、前記第3の記憶部に記憶された分割データから、再分割データを生成するデータ再分割ステップと、前記再分割データを前記機密情報管理システムに送信するステップと、を前記端末に実行させ、前記機密情報管理システムは、送信された再分割データ、及び前記第2の記憶部に記憶された再分割データのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記機密情報を復元し、前記同期情報を更新して前記第1の記憶部に記憶させることを特徴とする。

20

30

40

【0018】

請求項13記載の本発明は、請求項12記載の発明において、前記初期情報は、前記データ分割手段の秘密分散法で用いられた乱数のハッシュ関数値であり、前記乱数生成手段は、前記ハッシュ関数を前記同期情報の値に応じた回数分使用して、前記初期情報から生成された乱数種情報を基に、所定の疑似乱数生成アルゴリズムに従って新たな乱数を生成することを特徴とする。

50

【 0 0 1 9 】

請求項 1 4 記載の本発明は、請求項 1 2 又は 1 3 記載の発明において、前記データ分割手段の秘密分散法で用いられた乱数は、真性乱数であることを特徴とする。

【 0 0 2 0 】

請求項 1 5 記載の本発明は、請求項 1 2 乃至 1 4 のいずれか 1 項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データと該各乱数部分データに対応する新たな乱数部分データとの排他的論理和演算に置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【 0 0 2 1 】

請求項 1 6 記載の本発明は、請求項 1 2 乃至 1 4 のいずれか 1 項に記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【 発明の効果 】

【 0 0 2 2 】

本発明によれば、機密情報を秘密分散法を用いて複数に分割して、そのうちの一部をユーザに保持させるとともに、機密情報を使用するたびに、各分割データを同期をとって更新して再分割データを生成するので、仮にユーザが保持する機密情報の一部が第三者に漏洩したとしても、第三者のなりすましを確実に防止することができ、セキュリティが十分に確保された機密情報管理システム、機密情報管理方法、および機密情報管理プログラム、並びに機密情報管理システム用端末プログラムを提供することができる。

【 0 0 2 3 】

特に、本発明における秘密分散法は、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、機密情報を復元することなく、機密情報を再分割することができるので、ユーザの機密情報をよりセキュアに管理することができる。

【 発明を実施するための最良の形態 】

【 0 0 2 4 】

以下、本発明の実施の形態を図面を用いて説明する。

【 0 0 2 5 】

< システム構成 >

図 1 は、本発明の実施の形態に係る機密情報管理システム 1 が適用されるコンピュータシステム 1 0 全体の概略構成を示すブロック図である。

【 0 0 2 6 】

図 1 に示す機密情報管理システム 1 は、通信ネットワーク 4 を介してユーザが備えるクライアント端末 2 (以下、単に端末とよぶ) と接続されているとともに、通信ネットワーク 4 を介してユーザに所定のサービスを提供するサービス提供システム 5 と接続されている。また、機密情報管理システム 1 は、ハードウェア的に互いに独立した複数 (本実施の形態では 2 とする) のデータ保管用サーバコンピュータ (以下、単に保管サーバとよぶ) 3 a , 3 b と接続されている。

【 0 0 2 7 】

尚、本実施の形態における機密情報とは、ユーザがサービス提供システム 5 を利用する

10

20

30

40

50

ために必要なパスワード、クレジットカード番号、PKI秘密鍵などの個人情報をいう。

【0028】

上記構成のコンピュータシステム10においては、端末2がサービス提供システム5から所定のサービスを受けるには、まず、機密情報Sを機密情報管理システム1に送信（通信内容の漏洩を防止するため、オープンなネットワークではなく、セキュアな通信ネットワーク4a、例えば、LAN、IP-VPN、専用線、電話回線などによる）又は送付（例えば、郵便などの手段による）し、機密情報管理システム1において後述する独自の秘密分散アルゴリズムによる秘密分散法（以下、秘密分散法Aとよぶ）を用いて該機密情報Sを複数のデータに分割し、該分割データを保管サーバ3a、3bおよび端末2にそれぞれ送信（セキュアな通信ネットワーク4aによる）又は送付し、保管させるようになっている。この結果、機密情報Sが機密情報管理システム1に登録されたことになり、ユーザはサービス利用の準備が整ったことになる。尚、図1では、機密情報管理システム1は、端末2からの機密情報Sを3つの分割データD(1)、D(2)、D(3)に分割し、それぞれを複数の保管サーバ3a、3bおよび端末2に保管するようになっている。

10

【0029】

また、サービス利用時は、機密情報管理システム1及び端末2において、分割データD(1)、D(2)、D(3)をそれぞれ同期をとって更新した再分割データD'(1)、D'(2)、D'(3)を生成し、保管するので、端末2から機密情報管理システム1に対して、分割データD'(3)を送信（オープンな通信ネットワーク4b、例えば、インターネット網などによる）すると、機密情報管理システム1は、送信された分割データD'(3)および保管サーバ3a、3bの再分割データD'(1)、D'(2)のうち任意の2つから秘密分散法Aを用いてもとの機密情報Sを復元し、該機密情報Sをサービス提供システム5に送信するようになっている。これにより、ユーザは、サービス提供システム5から所定のサービスの提供を受けることができる。

20

【0030】

尚、本実施の形態においては、機密情報Sを3分割して保管する場合を例に説明するが、本発明は機密情報Sを3分割する場合に限定されるわけではなく、n分割（n=2以上の整数）の場合にも適用されるものである。また、端末2に送信される分割データは1つとは限らず複数であってもよいものである。さらに、本実施の形態においては、分割データD(1)、D(2)を保管サーバ3、分割データD(3)を利用端末2に割り当てたが、どの分割データをどの保管サーバ3および利用端末2に割り当ててもよいものである。

30

【0031】

機密情報管理システム1は、詳しくは、機密情報Sから秘密分散法Aを用いて複数の分割データD(1)、D(2)、D(3)に分割する分割データ生成部11、再分割データD'(1)、D'(2)を生成するために使用される乱数R'のシード（乱数生成の種となる情報） r_n を乱数種初期値 r_0 及びカウンタ値nを用いて生成する乱数種生成部12、機密情報Sから分割データD(1)、D(2)、D(3)を生成するために使用される真性乱数Rを生成するとともに、再分割データD'(1)、D'(2)を生成するために使用される乱数R'を上述したシード r_n 及び所定の疑似乱数アルゴリズムGに基づいて生成する乱数生成部13、ユーザがサービス提供システム5から所定のサービスを受ける際に、秘密分散法Aを用いて分割データD(1)、D(2)から再分割データD'(1)、D'(2)を生成する再分割データ生成部14、端末2と同期をとって再分割データD'(1)、D'(2)を生成するために必要なカウンタ値nを初期設定するとともに、機密情報Sをサービス提供システム5で使用するたびにカウンタ値nを減算して更新するカウンタ値管理部15、複数の再分割データD'(1)、D'(2)、D'(3)のいずれか2つから秘密分散法Aを用いて元データ（機密情報）Sを復元する元データ復元部16、並びに端末2、保管サーバ3a、3b、及びサービス提供システム5それぞれとデータの送受信を行う通信部17を具備する構成となっている。

40

【0032】

端末2は、詳しくは、ユーザがサービス提供システム5から所定のサービスを受ける際に、機密情報管理システム1から送信されたカウンタ値n及び乱数種初期値 r_0 を用いて

50

、再分割データD'(3)を生成するために使用される乱数R'のシード(乱数生成の種となる情報)r_nを生成する乱数種生成部22、再分割データD'(3)を生成するために使用される乱数R'を上述したシードr_n及び所定の疑似乱数アルゴリズムGに基づいて生成する乱数生成部22、上述した乱数R'及び機密情報管理システム1から送信された分割データD(3)から、秘密分散法Aを用いて再分割データD'(3)を生成する再分割データ生成部23、並びに、機密情報管理システム1及びサービス提供システム5それぞれとデータの送受信を行う通信部24を具備する構成となっている。

【0033】

尚、端末2は、ユーザが携行可能な携帯情報端末、携帯電話、ICカードなどの携帯記憶媒体などが想定されるが、他にモバイルを用途としないコンピュータ機器であってもよいものである。

10

【0034】

ここで、上述した機密情報管理システム1、端末2、保管サーバ3a、3bおよびサービス提供システム5は、それぞれ少なくとも演算機能および制御機能を備えた中央演算装置(CPU)、プログラムやデータを格納する機能を有するRAM等からなる主記憶装置(メモリ)を有する電子的な装置から構成されているものである。また、上記装置およびシステムは、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。尚、本実施の形態においては、保管サーバ3a、3b及びサービス提供システム5をそれぞれ、機密情報管理システム1と物理的に独立したサーバ装置とし、各装置がネットワーク接続された形態としているが、物理的に機密情報管理システム1と一体化されたサーバ装置としてもよいものである。

20

【0035】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0036】

<秘密分散法A>

ここで、本実施の形態における独自の秘密分散アルゴリズムによる秘密分散法Aについて説明する。

30

【0037】

本実施形態における元データ(機密情報Sに相当する)の分割および復元では、元データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するが、この場合の処理単位ビット長は任意の値に設定することができ、元データを処理単位ビット長毎に区分けして、この元部分データから分割部分データを分割数より1少ない数ずつ生成するので、元データのビット長が処理単位ビット長の(分割数-1)倍の整数倍に一致しない場合は、元データの末尾の部分に0を埋めるなどして元データのビット長を処理単位ビット長の(分割数-1)倍の整数倍に合わせるにより本実施形態を適用することができる。

40

【0038】

また、上述した乱数も(分割数-1)個の元部分データの各々に対応して処理単位ビット長のビット長を有する(分割数-1)個の乱数部分データとして乱数生成部13から生成される。すなわち、乱数は処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する(分割数-1)個の乱数部分データとして生成される。更に、元データは処理単位ビット長に基づいて所望の分割数の分割データに分割されるが、この分割データの各々も(分割数-1)個の元部分データの各々に対応して処理単位ビット長のビット長を有する(分割数-1)個の分割部分データとして生成される。すなわち、分割データの各々は、処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する(分割数-1)個の分割部分データとして生成される。

50

【 0 0 3 9 】

なお、以下の説明では、上述した元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれ S, R, D, n および b で表すとともに、また複数のデータや乱数などのうちの1つを表わす変数として $i(=1 \sim n)$ および $j(=1 \sim n-1)$ を用い、(分割数 $n-1$)個の元部分データ、(分割数 $n-1$)個の乱数部分データ、および分割数 n 個の分割データ D のそれぞれのうちの1つをそれぞれ $S(j), R(j)$ および $D(i)$ で表記し、更に各分割データ $D(i)$ を構成する複数 $(n-1)$ の分割部分データを $D(i, j)$ で表記するものとする。すなわち、 $S(j)$ は、元データ S の先頭から処理単位ビット長毎に区分けして1番から順に採番した時の j 番目の元部分データを表すものである。

【 0 0 4 0 】

この表記を用いると、元データ、乱数データ、分割データとこれらをそれぞれ構成する元部分データ、乱数部分データ、分割部分データは、次のように表記される。

【 0 0 4 1 】

元データ $S=(n-1)$ 個の元部分データ $S(j)$
 $=S(1), S(2), \dots, S(n-1)$

乱数 $R=(n-1)$ 個の乱数部分データ $R(j)$
 $=R(1), R(2), \dots, R(n-1)$

n 個の分割データ $D(i)=D(1), D(2), \dots, D(n)$

各分割部分データ $D(i, j)$
 $=D(1, 1), D(1, 2), \dots, D(1, n-1)$
 $D(2, 1), D(2, 2), \dots, D(2, n-1)$
 $\dots \quad \dots \quad \dots$
 $D(n, 1), D(n, 2), \dots, D(n, n-1)$
 $(i=1 \sim n), (j=1 \sim n-1)$

本実施形態は、上述したように処理単位ビット長毎に区分けされる複数の部分データに対して元部分データと乱数部分データの排他的論理和演算(XOR)を行って、詳しくは、元部分データと乱数部分データの排他的論理和演算(XOR)からなる定義式を用いて、元データの分割を行うことを特徴とするものであり、上述したデータ分割処理に多項式や剰余演算を用いる方法に比較して、コンピュータ処理に適したビット演算である排他的論理和(XOR)演算を用いることにより高速かつ高性能な演算処理能力を必要とせず、大容量のデータに対しても簡単な演算処理を繰り返して分割データを生成することができるとともに、また分割データの保管に必要な記憶容量も分割数に比例した倍数の容量よりも小さくすることができる。更に、任意に定めた一定の長さ毎にデータの先頭から順に演算処理を行うストリーム処理により分割データが生成される。

【 0 0 4 2 】

なお、本実施形態で使用する排他的論理和演算(XOR)は、以下の説明では、「 $*$ 」なる演算記号で表すことにするが、この排他的論理和演算のビット毎の演算規則での各演算結果は下記のとおりである。

【 0 0 4 3 】

$0 * 0$ の演算結果は 0

$0 * 1$ の演算結果は 1

$1 * 0$ の演算結果は 1

$1 * 1$ の演算結果は 0

また、XOR演算は交換法則、結合法則が成り立つ。すなわち、

$a * b = b * a$

$(a * b) * c = a * (b * c)$ が成り立つことが数学的に証明される。

【 0 0 4 4 】

また、 $a * a = 0, a * 0 = 0 * a = a$ が成り立つ。

【 0 0 4 5 】

ここで a, b, c は同じ長さのビット列を表し、 0 はこれらと同じ長さですべて「 0 」からなる

10

20

30

40

50

ビット列を表す。

【 0 0 4 6 】

次に、フローチャートなどの図面も参照して、本実施の形態における秘密分散法 A の作用について説明するが、この説明の前に図 2 乃至 6、図 8 および図 1 0 に示す記号の定義について説明する。

【 0 0 4 7 】

(1) $\prod_{i=1}^n A(i)$ は、 $A(1) * A(2) * \dots * A(n)$ を意味するものとする。

【 0 0 4 8 】

(2) $c(j, i, k)$ を $(n-1) \times (n-1)$ 行列である $U[n-1, n-1] \times (P[n-1, n-1])^{(j-1)}$ の i 行 k 列の値と定義する。

【 0 0 4 9 】

このとき $Q(j, i, k)$ を下記のように定義する。

【 0 0 5 0 】

$c(j, i, k) = 1$ のとき $Q(j, i, k) = R((n-1) \times m + k)$

$c(j, i, k) = 0$ のとき $Q(j, i, k) = 0$

ただし、 m は $m \geq 0$ の整数を表す。

【 0 0 5 1 】

(3) $U[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $u(i, j)$ で表すと、

$i + j \leq n + 1$ のとき $u(i, j) = 1$

$i + j > n + 1$ のとき $u(i, j) = 0$

である行列を意味するものとし、「上三角行列」ということとする。具体的には下記のような行列である。

【数 1】

$$U[3, 3] = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【 0 0 5 2 】

(4) $P[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $p(i, j)$ で表すと、

$j = i + 1$ のとき $p(i, j) = 1$

$i = n, j = 1$ のとき $p(i, j) = 1$

上記以外のとき $p(i, j) = 0$

である行列を意味するものとし、「回転行列」ということとする。具体的には下記のような行列であり、他の行列の右側からかけると当該他の行列の 1 列目を 2 列目へ、2 列目を 3 列目へ、...、 $n-1$ 列目を n 列目へ、 n 列目を 1 列目へ移動させる作用がある。つまり、行列 P を他の行列に右側から複数回かけると、その回数分だけ各列を右方向へ回転させるように移動させることができる。

【数 2】

$$P[3, 3] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

10

20

30

40

50

【 0 0 5 3 】

(5) A,Bを $n \times n$ 行列とすると、 $A \times B$ とは行列AとBの積を意味するものとする。行列の成分同士の計算規則は通常の数学で用いるものと同じである。

【 0 0 5 4 】

(6) Aを $n \times n$ 行列とし、 i を整数とすると、 A^i とは行列Aの i 個の積を意味するものとする。また、 A^0 とは単位行列Eを意味するものとする。

【 0 0 5 5 】

(7) 単位行列 $E[n,n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $e(i,j)$ で表すと、

$$i=j \quad \text{のとき} \quad e(i,j)=1$$

$$\text{上記以外のとき} \quad e(i,j)=0$$

である行列を意味するものとする。具体的には下記のような行列である。Aを任意の $n \times n$ 行列とすると

$$A \times E = E \times A = A$$

となる性質がある。

【 数 3 】

$$E[3,3] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad E[4,4] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

【 0 0 5 6 】

次に、図2に示すフローチャートおよび図3および図4に示す具体的データなどを参照して、まず元データSの分割処理について説明する。これは、機密情報管理システム1の分割データ生成部11の機能を説明するものである。

【 0 0 5 7 】

まず、元データSを機密情報管理システム1に与える(図2のステップS201)。なお、本例では、元データSは、16ビットの「10110010 00110111」とする。

【 0 0 5 8 】

次に、機密情報管理システム1は、分割数 n として3と指示する(ステップS203)。なお、この分割数 $n=3$ に従って機密情報管理システム1で生成される3個の分割データを $D(1)$ 、 $D(2)$ 、 $D(3)$ とする。この分割データ $D(1)$ 、 $D(2)$ 、 $D(3)$ は、すべて元データのビット長と同じ16ビット長のデータである。

【 0 0 5 9 】

それから、元データSを分割するために使用される処理単位ビット長 b を8ビットと決定する(ステップS205)。この処理単位ビット長 b は、利用者が端末2から機密情報管理システム1に対して指定してもよいし、または機密情報管理システム1において予め定められた値を用いてもよい。なお、処理単位ビット長 b は、任意のビット数でよいが、ここでは元データSを割り切ることができる8ビットとしている。従って、上記16ビットの「10110010 00110111」の元データSは、8ビットの処理単位ビット長で分けられた場合の2個の元分割データ $S(1)$ および $S(2)$ は、それぞれ「10110010」および「00110111」となる。

【 0 0 6 0 】

次のステップS207では、元データSのビット長が 8×2 の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を0で埋めて、 8×2 の整数倍に合わせる。なお、本例のように処理単位ビット長 b が8ビットおよび分割数 n が3に設定された場合における分割処理は、元データSのビット長として16ビットに限られるものでなく、処理単位ビット長 $b \times (分割数n-1) = 8 \times 2$ の整数倍の元データSに対して有効なものである。

【 0 0 6 1 】

次に、ステップS 2 0 9では、変数m、すなわち上述した整数倍を意味する変数mを0に設定する。本例のように、元データSが処理単位ビット長 $b \times (\text{分割数}n-1) = 8 \times 2 = 16$ ビットである場合には、変数mは0であるが、2倍の32ビットの場合には、変数mは1となり、3倍の48ビットの場合には、変数mは2となる。

【 0 0 6 2 】

次に、元データSの $8 \times 2 \times m + 1$ ビット目から 8×2 ビット分のデータが存在するか否かが判定される(ステップS 2 1 1)。これは、このステップS 2 1 1以降に示す分割処理を元データSの変数mで特定される処理単位ビット長 $b \times (\text{分割数}n-1) = 8 \times 2 = 16$ ビットに対して行った後、元データSとして次の16ビットがあるか否かを判定しているものである。本例のように元データSが16ビットである場合には、16ビットの元データSに対してステップS 2 1 1以降の分割処理を1回行うと、後述するステップS 2 1 9で変数mが+1されるが、本例の元データSでは変数mがm+1の場合に相当する17ビット以降のデータは存在しないので、ステップS 2 1 1からステップS 2 2 1に進むことになるが、今の場合は、変数mは0であるので、元データSの $8 \times 2 \times m + 1$ ビット目は、 $8 \times 2 \times 0 + 1 = 1$ となり、元データSの16ビットの1ビット目から 8×2 ビット分にデータが存在するため、ステップS 2 1 3に進む。

【 0 0 6 3 】

ステップS 2 1 3では、変数jを1から2(=分割数n-1)まで変えて、元データSの $8 \times (2 \times m + j - 1) + 1$ ビット目から8ビット分(=処理単位ビット長)のデータを元部分データS(2 × m + j)に設定し、これにより元データSを処理単位ビット長で分けした2(分割数n-1)個の元部分データS(1), S(2)を次のように生成する。

【 0 0 6 4 】

元データS=S(1), S(2)

第1の元部分データS(1)=「10110010」

第2の元部分データS(2)=「00110111」

次に、変数jを1から2(=分割数n-1)まで変えて、乱数部分データR(2 × m + j)に乱数生成部13から発生する8ビットの長さの乱数を設定し、これにより乱数Rを処理単位ビット長で分けした2(分割数n-1)個の乱数部分データR(1), R(2)を次のように生成する(ステップS 2 1 5)。

【 0 0 6 5 】

乱数R=R(1), R(2)

第1の乱数部分データR(1)=「10110001」

第2の乱数部分データR(2)=「00110101」

次に、ステップS 2 1 7において、変数iを1から3(=分割数n)まで変えるとともに、更に各変数iにおいて変数jを1から2(=分割数n-1)まで変えながら、ステップS 2 1 7に示す分割データを生成するための元部分データと乱数部分データの排他的論理和からなる定義式により複数の分割データD(i)の各々を構成する各分割部分データD(i, 2 × m + j)を生成する。この結果、次に示すような分割データDが生成される。

【 0 0 6 6 】

分割データD

= 3個の分割データD(i)=D(1), D(2), D(3)

第1の分割データD(1)

= 2個の分割部分データD(1, j)=D(1, 1), D(1, 2)

= 「00110110」, 「10110011」

第2の分割データD(2)

= 2個の分割部分データD(2, j)=D(2, 1), D(2, 2)

= 「00000011」, 「00000010」

第3の分割データD(3)

= 2個の分割部分データD(3, j)=D(3, 1), D(3, 2)

10

20

30

40

50

= 「10110001」, 「00110101」

なお、各分割部分データ (i, j) を生成するためのステップS 2 1 7に示す定義式は、本例のように分割数 $n=3$ の場合には、具体的には図4に示す表に記載されているものとなる。図4に示す表から、分割部分データ $D(1, 1)$ を生成するための定義式は $S(1)*R(1)*R(2)$ であり、 $D(1, 2)$ の定義式は $S(2)*R(1)*R(2)$ であり、 $D(2, 1)$ の定義式は $S(1)*R(1)$ であり、 $D(2, 2)$ の定義式は $S(2)*R(2)$ であり、 $D(3, 1)$ の定義式は $R(1)$ であり、 $D(3, 2)$ の定義式は $R(2)$ である。また、図4に示す表には $m>0$ の場合の任意の整数についての一般的な定義式も記載されている。

【0067】

このように整数倍を意味する変数 $m=0$ の場合について分割データ D を生成した後、次に変数 m を1増やし(ステップS 2 1 9)、ステップS 2 1 1に戻り、変数 $m+1$ に該当する元データ S の17ビット以降について同様の分割処理を行おうとするが、本例の元データ S は16ビットであり、17ビット以降のデータは存在しないので、ステップS 2 1 1からステップS 2 2 1に進み、上述したように生成した分割データ $D(1), D(2), D(3)$ を保管サーバ3及び端末2にそれぞれ保存して、分割処理を終了する。なお、このように保管された分割データ $D(1), D(2), D(3)$ はそれぞれ単独では元データが推測できない。

10

【0068】

ここで、上述した図2のフローチャートのステップS 2 1 7における定義式による分割データの生成処理、具体的には分割数 $n=3$ の場合の分割データの生成処理について詳しく説明する。

20

【0069】

まず、整数倍を意味する変数 $m=0$ の場合には、ステップS 2 1 7に示す定義式から各分割データ $D(i)=D(1) \sim D(3)$ の各々を構成する各分割部分データ $D(i, 2 \times m + j)=D(i, j)$ ($i=1 \sim 3, j=1 \sim 2$)は、次のようになる。

【0070】

$$D(1, 1)=S(1)*Q(1, 1, 1)*Q(1, 1, 2)$$

$$D(1, 2)=S(2)*Q(2, 1, 1)*Q(2, 1, 2)$$

$$D(2, 1)=S(1)*Q(1, 2, 1)*Q(1, 2, 2)$$

$$D(2, 2)=S(2)*Q(2, 2, 1)*Q(2, 2, 2)$$

$$D(3, 1)=R(1)$$

$$D(3, 2)=R(2)$$

30

上記の6つの式のうち上から4つの式に含まれる $Q(j, i, k)$ を具体的に求める。

【0071】

これは $c(j, i, k)$ を 2×2 行列である $U[2, 2] \times (P[2, 2])^{(j-1)}$ の i 行 k 列の値としたとき下記のように定義される。

【0072】

$$c(j, i, k)=1 \text{ のとき } Q(j, i, k)=R(k)$$

$$c(j, i, k)=0 \text{ のとき } Q(j, i, k)=0$$

ここで、

$j=1$ のときは

40

【数4】

$$\begin{aligned}
 U[2, 2] \times (P[2, 2])^{-(j-1)} &= U[2, 2] \times (P[2, 2])^{-0} \\
 &= U[2, 2] \times E[2, 2] \\
 &= U[2, 2] \\
 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}
 \end{aligned}$$

10

【0073】

j=2のときは

【数5】

$$\begin{aligned}
 U[2, 2] \times (P[2, 2])^{-(j-1)} &= U[2, 2] \times (P[2, 2])^{-1} \\
 &= U[2, 2] \times P[2, 2] \\
 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
 \end{aligned}$$

20

【0074】

これを用いると、各分割部分データD(i, j)は次のような定義式により生成される。

【0075】

$$\begin{aligned}
 D(1, 1) &= S(1) * Q(1, 1, 1) * Q(1, 1, 2) = S(1) * R(1) * R(2) \\
 D(1, 2) &= S(2) * Q(2, 1, 1) * Q(2, 1, 2) = S(2) * R(1) * R(2) \\
 D(2, 1) &= S(1) * Q(1, 2, 1) * Q(1, 2, 2) = S(1) * R(1) * 0 = S(1) * R(1) \\
 D(2, 2) &= S(2) * Q(2, 2, 1) * Q(2, 2, 2) = S(2) * 0 * R(2) = S(2) * R(2)
 \end{aligned}$$

30

上述した各分割部分データD(i, j)を生成するための定義式は、図3にも図示されている。

【0076】

図3は、上述したように16ビットの元データSを8ビットの処理単位ビット長に基づいて分割数n=3で3分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0077】

ここで、上述した定義式により分割データD(1), D(2), D(3)および各分割部分データD(1, 1), D(1, 2), D(2, 1), D(2, 2), D(3, 1), D(3, 2)を生成する過程と定義式の一般形について説明する。

40

【0078】

まず、第1の分割データD(1)に対しては、第1の分割部分データD(1, 1)は、上述した定義式S(1) * R(1) * R(2)で定義され、第2の分割部分データD(1, 2)は定義式S(2) * R(1) * R(2)で定義される。なお、この定義式の一般形は、D(1, j)に対してはS(j) * R(j) * R(j+1)であり、D(1, j+1)に対してS(j+1) * R(j) * R(j+1)である(jは奇数とする)。定義式に従って計算すると、D(1, 1)は00110110、D(1, 2)は10110011となるので、D(1)は00110110 10110011である。なお、定義式の一般形は、図4にまとめて示されている。

50

【 0 0 7 9 】

また、第 2 の分割データD(2)に対しては、D(2,1)はS(1)*R(1)で定義され、D(2,2)はS(2)*R(2)で定義される。この定義式の一般形は、D(2,j)に対してはS(j)*R(j)であり、D(2,j+1)に対してはS(j+1)*R(j+1)である(jは奇数とする)。定義式に従って計算すると、D(2,1)は00000011、D(2,2)は00000010となるので、D(2)は00000011 00000010である。

【 0 0 8 0 】

更に第 3 の分割データD(3)に対しては、D(3,1)はR(1)で定義され、D(3,2)はR(2)で定義される。この定義式の一般形は、D(3,j)に対してはR(j)であり、D(3,j+1)に対してはR(j+1)である(jは奇数とする)。定義式に従って計算すると、D(3,1)は10110001、D(3,2)は0110101となるので、D(3)は10110001 00110101である。

10

【 0 0 8 1 】

上記説明は、S,R,D(1),D(2),D(3)の長さを 16 ビットとしたが、データの先頭から上記分割処理を繰り返すことにより、どのような長さの元データSからでも分割データD(1),D(2),D(3)を生成することができる。また、処理単位ビット長bは任意にとることができ、元データSの先頭から順にb×2の長さ毎に上記分割処理を繰り返すことにより任意の長さの元データ、具体的には処理単位ビット長b×2の整数倍の長さの元データに対して適用することができる。なお、元データSの長さが処理単位ビット長b×2の整数倍でない場合は、例えば、データ末尾の部分を 0 で埋めるなどして元データSの長さを処理単位ビット長b×2の整数倍に合わせるにより上述した本実施形態の分割処理を適用することができる。

20

【 0 0 8 2 】

次に、図 3 の右側に示す表を参照して、分割データから元データを復元する処理について説明する。尚、機密情報管理システム 1 の元データ復元部 16 は、この処理を行うのではなく、後述する再分割データから元データを復元するものであるが、以下、分割データD(1),D(2),D(3)から元データSを復元できることを示す。

【 0 0 8 3 】

まず、分割部分データD(2,1),D(3,1)から第 1 の元部分データS(1)を次のように生成することができる。

【 0 0 8 4 】

$$\begin{aligned} D(2,1)*D(3,1) &= (S(1)*R(1))*R(1) \\ &= S(1)*(R(1)*R(1)) \\ &= S(1)*0 \\ &= S(1) \end{aligned}$$

30

具体的に計算すると、D(2,1)は00000011、D(3,1)は10110001なので、S(1)は10110010となる。

【 0 0 8 5 】

また、別の分割部分データから次のように第 2 の元部分データS(2)を生成することができる。

【 0 0 8 6 】

$$\begin{aligned} D(2,2)*D(3,2) &= (S(2)*R(2))*R(2) \\ &= S(2)*(R(2)*R(2)) \\ &= S(2)*0 \\ &= S(2) \end{aligned}$$

40

具体的に計算すると、D(2,2)は00000010、D(3,2)は00110101なので、S(2)は00110111となる。

【 0 0 8 7 】

一般に、jを奇数として、

$$\begin{aligned} D(2,j)*D(3,j) &= (S(j)*R(j))*R(j) \\ &= S(j)*(R(j)*R(j)) \\ &= S(j)*0 \end{aligned}$$

50

$$=S(j)$$

であるから、 $D(2, j) * D(3, j)$ を計算すれば、 $S(j)$ が求まる。

【 0 0 8 8 】

また、一般に、 j を奇数として、

$$\begin{aligned} D(2, j+1) * D(3, j+1) &= (S(j+1) * R(j+1)) * R(j+1) \\ &= S(j+1) * (R(j+1) * R(j+1)) \\ &= S(j+1) * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D(2, j+1) * D(3, j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【 0 0 8 9 】

次に、 $D(1), D(3)$ を取得して S を復元する場合には、次のようになる。

【 0 0 9 0 】

$$\begin{aligned} D(1, 1) * D(3, 1) * D(3, 2) &= (S(1) * R(1) * R(2)) * R(1) * R(2) = S(1) * (R(1) * R(1)) * (R(2) * R(2)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

であるから、 $D(1, 1) * D(3, 1) * D(3, 2)$ を計算すれば、 $S(1)$ が求まる。具体的に計算すると、 $D(1, 1)$ は00110110、 $D(3, 1)$ は10110001、 $D(3, 2)$ は00110101なので、 $S(1)$ は10110010となる。

【 0 0 9 1 】

また同様に、

$$\begin{aligned} D(1, 2) * D(3, 1) * D(3, 2) &= (S(2) * R(1) * R(2)) * R(1) * R(2) \\ &= S(2) * (R(1) * R(1)) * (R(2) * R(2)) \\ &= S(2) * 0 * 0 \\ &= S(2) \end{aligned}$$

であるから、 $D(1, 2) * D(3, 1) * D(3, 2)$ を計算すれば、 $S(2)$ が求まる。具体的に計算すると、 $D(1, 2)$ は10110011、 $D(3, 1)$ は10110001、 $D(3, 2)$ は00110101なので、 $S(2)$ は00110111となる。

【 0 0 9 2 】

一般に、 j を奇数として、

$$\begin{aligned} D(1, j) * D(3, j) * D(3, j+1) &= (S(j) * R(j) * R(j+1)) * R(j) * R(j+1) \\ &= S(j) * (R(j) * R(j)) * (R(j+1) * R(j+1)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

であるから、 $D(1, j) * D(3, j) * D(3, j+1)$ を計算すれば、 $S(j)$ が求まる。

【 0 0 9 3 】

また、一般に、 j を奇数として、

$$\begin{aligned} D(1, j+1) * D(3, j) * D(3, j+1) &= (S(j+1) * R(j) * R(j+1)) * R(j) * R(j+1) \\ &= S(j+1) * (R(j) * R(j)) * (R(j+1) * R(j+1)) \\ &= S(j+1) * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D(1, j+1) * D(3, j) * D(3, j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【 0 0 9 4 】

次に、 $D(1), D(2)$ を取得して S を復元する場合には、次のようになる。

【 0 0 9 5 】

$$\begin{aligned} D(1, 1) * D(2, 1) &= (S(1) * R(1) * R(2)) * (S(1) * R(1)) \\ &= (S(1) * S(1)) * (R(1) * R(1)) * R(2) \\ &= 0 * 0 * R(2) \\ &= R(2) \end{aligned}$$

であるから、 $D(1, 1) * D(2, 1)$ を計算すれば、 $R(2)$ が求まる。具体的に計算すると、 $D(1, 1)$ は00110110、 $D(2, 1)$ は00000011なので、 $R(2)$ は00110101となる。

10

20

30

40

50

【 0 0 9 6 】

また同様に、

$$\begin{aligned} D(1,2)*D(2,2) &= (S(2)*R(1)*R(2))*(S(2)*R(2)) \\ &= (S(2)*S(2))*R(1)*(R(2)*R(2)) \\ &= 0*R(1)*0 \\ &= R(1) \end{aligned}$$

であるから、 $D(1,2)*D(2,2)$ を計算すれば、 $R(1)$ が求まる。具体的に計算すると、 $D(1,2)$ は10110011, $D(2,2)$ は00000010なので、 $R(1)$ は10110001となる。

【 0 0 9 7 】

この $R(1), R(2)$ を使用して $S(1), S(2)$ を求める。

10

【 0 0 9 8 】

$$\begin{aligned} D(2,1)*R(1) &= (S(1)*R(1))*R(1) \\ &= S(1)*(R(1)*R(1)) \\ &= S(1)*0 \\ &= S(1) \end{aligned}$$

であるから、 $D(2,1)*R(1)$ を計算すれば、 $S(1)$ が求まる。具体的に計算すると、 $D(2,1)$ は0000011, $R(1)$ は10110001なので、 $S(1)$ は10110010となる。

【 0 0 9 9 】

また同様に、

$$\begin{aligned} D(2,2)*R(2) &= (S(2)*R(2))*R(2) \\ &= S(2)*(R(2)*R(2)) \\ &= S(2)*0 \\ &= S(2) \end{aligned}$$

20

であるから $D(2,2)*R(2)$ を計算すれば $S(2)$ が求まる。具体的に計算すると $D(2,2)$ は00000010, $R(2)$ は00110101なので、 $S(2)$ は00110111となる。

【 0 1 0 0 】

一般に、 j を奇数として、

$$\begin{aligned} D(1,j)*D(2,j) &= (S(j)*R(j)*R(j+1))*(S(j)*R(j)) \\ &= (S(j)*S(j))*(R(j)*R(j))*R(j+1) \\ &= 0*0*R(j+1) \\ &= R(j+1) \end{aligned}$$

30

であるから $D(1,j)*D(2,j)$ を計算すれば $R(j+1)$ が求まる。

【 0 1 0 1 】

また同様に、

$$\begin{aligned} D(1,j+1)*D(2,j+1) &= (S(j+1)*R(j)*R(j+1))*(S(j+1)*R(j+1)) \\ &= (S(j+1)*S(j+1))*R(j)*(R(j+1)*R(j+1)) \\ &= 0*R(j)*0 \\ &= R(j) \end{aligned}$$

であるから $D(1,j+1)*D(2,j+1)$ を計算すれば $R(j)$ が求まる。

【 0 1 0 2 】

この $R(j), R(j+1)$ を使用して $S(j), S(j+1)$ を求める。

40

【 0 1 0 3 】

$$\begin{aligned} D(2,j)*R(j) &= (S(j)*R(j))*R(j) \\ &= S(j)*(R(j)*R(j)) \\ &= S(j)*0 \\ &= S(j) \end{aligned}$$

であるから $D(2,j)*R(j)$ を計算すれば $S(j)$ が求まる。

【 0 1 0 4 】

また同様に、

$$D(2,j+1)*R(j+1) = (S(j+1)*R(j+1))*R(j+1)$$

50

$$\begin{aligned}
 &=S(j+1)*(R(j+1)*R(j+1)) \\
 &=S(j+1)*0 \\
 &=S(j+1)
 \end{aligned}$$

であるから $D(2, j+1)*R(j+1)$ を計算すれば $S(j+1)$ が求まる。

【 0 1 0 5 】

上述したように、元データの先頭から処理単位ビット長 b に基づいて分割処理を繰り返して行って、分割データを生成した場合には、3つの分割データ $D(1), D(2), D(3)$ のすべてを用いなくても、3つの分割データのうち、2つの分割データを用いて上述したように元データを復元することができる。

【 0 1 0 6 】

尚、本実施の形態に係る機密情報管理システム1においては、3つの分割データ $D(1), D(2), D(3)$ を生成するようになっていたので、分割数が3の場合について説明したが、秘密分散法Aは、分割数が n の場合にも適用できるものである。

【 0 1 0 7 】

次に、図5に示すフローチャートを参照して、分割数が n で、処理単位ビット長が b である場合の一般的な分割処理について説明する。

【 0 1 0 8 】

まず、元データ S を機密情報管理システム1に与える(ステップS401)。また、機密情報管理システム1に、分割数 n ($n \geq 3$ である任意の整数)を指示する(ステップS403)。処理単位ビット長 b を決定する(ステップS405)。なお、 b は0より大きい任意の整数である。次に、元データ S のビット長が $b \times (n-1)$ の整数倍であるか否かを判定し、整数倍でない場合には、元データ S の末尾を0で埋める(ステップS407)。また、整数倍を意味する変数 m を0に設定する(ステップS409)。

【 0 1 0 9 】

次に、元データ S の $b \times (n-1) \times m+1$ ビット目から $b \times (n-1)$ ビット分のデータが存在するかが判定される(ステップS411)。この判定の結果、データが存在しない場合は、ステップS421に進むことになるが、今の場合は、ステップS409で変数 m は0に設定された場合であるので、データが存在するため、ステップS413に進む。

【 0 1 1 0 】

ステップS413では、変数 j を1から $n-1$ まで変えて、元データ S の $b \times ((n-1) \times m+j-1) + 1$ ビット目から b ビット分のデータを元部分データ $S((n-1) \times m+j)$ に設定する処理を繰り返し、これにより元データ S を処理単位ビット長 b で区分けした $(n-1)$ 個の元部分データ $S(1), S(2), \dots, S(n-1)$ が生成される。

【 0 1 1 1 】

次に、変数 j を1から $n-1$ まで変えて、乱数部分データ $R((n-1) \times m+j)$ に乱数生成部13から発生する処理単位ビット長 b の乱数を設定し、これにより乱数 R を処理単位ビット長 b で区分けした $n-1$ 個の乱数部分データ $R(1), R(2), \dots, R(n-1)$ が生成される(ステップS415)。

【 0 1 1 2 】

次に、ステップS417において、変数 i を1から n まで変えるとともに、更に各変数 i において変数 j を1から $n-1$ まで変えながら、ステップS417に示す分割データを生成するための定義式により複数の分割データ $D(i)$ の各々を構成する各分割部分データ $D(i, (n-1) \times m+j)$ を生成する。この結果、次に示すような分割データ D が生成される。

【 0 1 1 3 】

分割データ D

$$=n\text{個の分割データ } D(i)=D(1), D(2), \dots, D(n)$$

第1の分割データ $D(1)$

$$=n-1\text{個の分割部分データ } D(1, j)=D(1, 1), D(1, 2), \dots, D(1, n-1)$$

第2の分割データ $D(2)$

$$=n-1\text{個の分割部分データ } D(2, j)=D(2, 1), D(2, 2), \dots, D(2, n-1)$$

10

20

30

40

50

$$\begin{aligned}
 &=S(j)*S(j+1)*(R(j)*R(j))*R(j+1)) \\
 &=S(j)*S(j+1)*0*R(j+1) \\
 &=S(j)*S(j+1)*R(j+1)
 \end{aligned}$$

$$D(3, j)*D(3, j+1)=R(j)*R(j+1)$$

となるからである。

【 0 1 2 0 】

また、この場合、3つの分割データのうち2つから、元データを復元することができるという特性は失われていない。これは、D(1)、D(2)を取得してSを復元する場合には、図6におけるD(1)、D(2)は、図4におけるD(1)、D(2)を構成する分割部分データを入れ替えたものにすぎないので、明らかにこれらから元データを復元することができ、また、D(1)とD(3)またはD(2)とD(3)を取得してSを復元する場合には、D(3)は乱数のみからなる分割データであるので、D(1)またはD(2)の分割部分データ毎に必要な個数の乱数との排他的論理和演算を行うことにより、乱数部分を消去して元データを復元することができるからである。

10

【 0 1 2 1 】

次に、一旦分割された分割データにさらに乱数を与えて新たな分割データ（再分割データ）を生成する再分割処理について説明する。これは、ユーザが機密情報Sを使って所定のサービスを受ける場合の機密情報管理システム1の再分割データ生成部14、及び端末2の再分割データ生成部23の機能を説明するものであるが、これに関しても、分割数が3の場合を例に説明する。尚、本実施の形態における再分割処理は、2つの方法があるので、以下、それぞれについて説明する。

20

【 0 1 2 2 】

（乱数追加注入方式）

図7は、乱数追加注入方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データD(1)、D(2)、D(3)を取得し（ステップS501）、次に、再分割の際に用いる乱数R'を発生させる（ステップS503）。尚、乱数R'に関しては、後述する機密情報管理システム1の動作において、詳しく説明する。

【 0 1 2 3 】

次に、分割データD(1)、D(2)、D(3)それぞれに乱数R'を所定のルールで注入する（ステップS505）。これは、後述するようなルールにより分割データD(1)、D(2)、D(3)の分割部分データと乱数R'の乱数部分データの排他的論理和をとり、新たな分割データD'(1)、D'(2)、D'(3)を生成するものである（ステップS507）。

30

【 0 1 2 4 】

図8は、元データSを、元データの半分の長さの処理単位ビット長bに基づいて分割数n=3で3分割する場合の分割部分データの定義式、乱数の再注入後の分割部分データの定義式、および各分割部分データから元データを復元する場合の計算式などを示す表である。

【 0 1 2 5 】

ここで、分割部分データD(i, j)の定義式について説明する。

【 0 1 2 6 】

まず、第1の分割データD(1)に対しては、図6に示すように、第1の分割部分データD(1, 1)は、定義式S(1)*R(1)*R(2)で定義され、第2の分割部分データD(1, 2)は定義式S(2)*R(2)で定義される。なお、この定義式の一般形は、D(1, j)に対してはS(j)*R(j)*R(j+1)であり、D(1, j+1)に対してS(j+1)*R(j+1)である（jは奇数とする）。

40

【 0 1 2 7 】

また、第2の分割データD(2)に対しては、図6に示すように、D(2, 1)はS(1)*R(1)で定義され、D(2, 2)はS(2)*R(1)*R(2)で定義される。この定義式の一般形は、D(2, j)に対してはS(j)*R(j)であり、D(2, j+1)に対してはS(j+1)*R(j)*R(j+1)である（jは奇数とする）。

【 0 1 2 8 】

更に第3の分割データD(3)に対しては、図6に示すように、D(3, 1)はR(1)で定義され、D(3, 2)はR(2)で定義される。この定義式の一般形は、D(3, j)に対してはR(j)であり、D(3,

50

$j+1$)に対しては $R(j+1)$ である (j は奇数とする)。

【0129】

次に、新たな乱数 R' 注入後の分割部分データ $D'(i, j)$ の定義式について説明する。

【0130】

まず、第1の分割データ $D'(1)$ に対しては、図8に示すように、第1の分割部分データ $D'(1, 1)$ は、定義式 $D(1, 1) * R'(1) * R'(2)$ 、即ち、 $S(1) * R(1) * R(2) * R'(1) * R'(2)$ で定義され、第2の分割部分データ $D'(1, 2)$ は、定義式 $D(1, 2) * R'(2)$ 、即ち、 $S(2) * R(2) * R'(2)$ で定義される。なお、この定義式の一般形は、 $D'(1, j)$ に対しては $D(1, j) * R'(j) * R'(j+1)$ であり、 $D'(1, j+1)$ に対して $D(1, j+1) * R'(j+1)$ である (j は奇数とする)。

【0131】

また、第2の分割データ $D'(2)$ に対しては、図8に示すように、 $D'(2, 1)$ は $D(2, 1) * R'(1)$ 、即ち、 $S(1) * R(1) * R'(1)$ で定義され、 $D'(2, 2)$ は $D(2, 2) * R'(1) * R'(2)$ 、即ち、 $S(2) * R(1) * R(2) * R'(1) * R'(2)$ で定義される。この定義式の一般形は、 $D'(2, j)$ に対しては $D(2, j) * R'(j)$ であり、 $D'(2, j+1)$ に対しては $D(2, j+1) * R'(j) * R'(j+1)$ である (j は奇数とする)。

【0132】

また、第3の分割データ $D'(3)$ に対しては、図8に示すように、 $D'(3, 1)$ は $D(3, 1) * R'(1)$ 、即ち、 $R(1) * R'(1)$ で定義され、 $D'(3, 2)$ は $D(3, 2) * R'(2)$ 、即ち、 $R(2) * R'(2)$ で定義される。この定義式の一般形は、 $D'(3, j)$ に対しては $D(3, j) * R'(j)$ であり、 $D'(3, j+1)$ に対しては $D(3, j+1) * R'(j+1)$ である (j は奇数とする)。

【0133】

このように、再分割部分データ $D'(i, j)$ はそれぞれ、分割部分データ $D(i, j)$ に、分割部分データ $D(i, j)$ の定義式で注入されていた乱数部分データ $R(j)$ に対応する乱数部分データ $R'(j)$ を注入して排他的論理和を計算して求めるものである。

【0134】

次に、図8の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、機密情報管理システム1の元データ復元部16の機能を説明するものである。

【0135】

まず、分割部分データ $D'(2, 1)$ 、 $D'(3, 1)$ から第1の元部分データ $S(1)$ を次のように生成することができる。

【0136】

$$\begin{aligned} D'(2, 1) * D'(3, 1) &= (S(1) * R(1) * R'(1)) * (R(1) * R'(1)) \\ &= S(1) * (R(1) * R(1)) * (R'(1) * R'(1)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

また、別の分割部分データから次のように第2の元部分データ $S(2)$ を生成することができる。

【0137】

$$\begin{aligned} D'(2, 2) * D'(3, 1) * D'(3, 2) &= (S(2) * R(1) * R(2) * R'(1) * R'(2)) * \\ &\quad (R(1) * R'(1)) * (R(2) * R'(2)) \\ &= S(2) * (R(1) * R(1)) * (R(2) * R(2)) * \\ &\quad (R'(1) * R'(1)) * (R'(2) * R'(2)) \\ &= S(2) * 0 * 0 * 0 * 0 \\ &= S(2) \end{aligned}$$

一般に、 j を奇数として、

$$\begin{aligned} D'(2, j) * D'(3, j) &= (S(j) * R(j) * R'(j)) * (R(j) * R'(j)) \\ &= S(j) * (R(j) * R(j)) * (R'(j) * R'(j)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

10

20

30

40

50

であるから、 $D'(2,j) \cdot D'(3,j)$ を計算すれば、 $S(j)$ が求まる。

【0138】

また、一般に、 j を奇数として、

$$\begin{aligned} D'(2,j+1) \cdot D'(3,j) \cdot D'(3,j+1) &= (S(j+1) \cdot R(j) \cdot R(j+1) \cdot R'(j) \cdot R'(j+1)) \cdot \\ &\quad (R(j) \cdot R'(j)) \cdot (R(j+1) \cdot R'(j+1)) \\ &= S(j+1) \cdot ((R(j) \cdot R(j)) \cdot (R(j+1) \cdot R(j+1))) \cdot \\ &\quad \cdot (R'(j) \cdot R'(j)) \cdot (R'(j+1) \cdot R'(j+1)) \\ &= S(j+1) \cdot 0 \cdot 0 \cdot 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D'(2,j+1) \cdot D'(3,j) \cdot D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

10

【0139】

次に、 $D'(1), D'(3)$ を取得して S を復元する場合には、次のようになる。

【0140】

$$\begin{aligned} D'(1,1) \cdot D'(3,1) \cdot D'(3,2) &= (S(1) \cdot R(1) \cdot R(2) \cdot R'(1) \cdot R'(2)) \cdot \\ &\quad (R(1) \cdot R'(1)) \cdot (R(2) \cdot R'(2)) \\ &= S(1) \cdot (R(1) \cdot R(1)) \cdot (R(2) \cdot R(2)) \cdot \\ &\quad (R'(1) \cdot R'(1)) \cdot (R'(2) \cdot R'(2)) \\ &= S(1) \cdot 0 \cdot 0 \cdot 0 \\ &= S(1) \end{aligned}$$

であるから、 $D'(1,1) \cdot D'(3,1) \cdot D'(3,2)$ を計算すれば、 $S(1)$ が求まる。

20

【0141】

また同様に、

$$\begin{aligned} D'(1,2) \cdot D'(3,2) &= (S(2) \cdot R(2) \cdot R'(2)) \cdot (R(2) \cdot R'(2)) \\ &= S(2) \cdot (R(2) \cdot R(2)) \cdot (R'(2) \cdot R'(2)) \\ &= S(2) \cdot 0 \cdot 0 \\ &= S(2) \end{aligned}$$

であるから、 $D'(1,2) \cdot D'(3,2)$ を計算すれば、 $S(2)$ が求まる。

【0142】

一般に、 j を奇数として、

$$\begin{aligned} D'(1,j) \cdot D'(3,j) \cdot D'(3,j+1) &= (S(j) \cdot R(j) \cdot R(j+1) \cdot R'(j) \cdot R'(j+1)) \cdot \\ &\quad (R(j) \cdot R'(j)) \cdot (R(j+1) \cdot R'(j+1)) \\ &= S(j) \cdot (R(j) \cdot R(j)) \cdot (R(j+1) \cdot R(j+1)) \cdot \\ &\quad (R'(j) \cdot R'(j)) \cdot (R'(j+1) \cdot R'(j+1)) \\ &= S(j) \cdot 0 \cdot 0 \cdot 0 \\ &= S(j) \end{aligned}$$

30

であるから、 $D'(1,j) \cdot D'(3,j) \cdot D'(3,j+1)$ を計算すれば、 $S(j)$ が求まる。

【0143】

また、一般に、 j を奇数として、

$$\begin{aligned} D'(1,j+1) \cdot D'(3,j+1) &= (S(j+1) \cdot R(j+1) \cdot R'(j+1)) \cdot (R(j+1) \cdot R'(j+1)) \\ &= S(j+1) \cdot (R(j+1) \cdot R(j+1)) \cdot (R'(j+1) \cdot R'(j+1)) \\ &= S(j+1) \cdot 0 \cdot 0 \\ &= S(j+1) \end{aligned}$$

40

であるから、 $D'(1,j+1) \cdot D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0144】

次に、 $D'(1), D'(2)$ を取得して S を復元する場合には、次のようになる。

【0145】

$$\begin{aligned} D'(1,1) \cdot D'(2,1) &= (S(1) \cdot R(1) \cdot R(2) \cdot R'(1) \cdot R'(2)) \cdot (S(1) \cdot R(1) \cdot R'(1)) \\ &= (S(1) \cdot S(1)) \cdot (R(1) \cdot R(1)) \cdot (R'(1) \cdot R'(1)) \cdot R(2) \cdot R'(2) \\ &= 0 \cdot 0 \cdot 0 \cdot R(2) \cdot R'(2) \\ &= R(2) \cdot R'(2) \end{aligned}$$

50

であるから、 $D'(1,1) \cdot D'(2,1)$ を計算すれば、 $R(2) \cdot R'(2)$ が求まる。

【0146】

また同様に、

$$\begin{aligned} D'(1,2) \cdot D'(2,2) &= (S(2) \cdot R(2) \cdot R'(2)) \cdot (S(2) \cdot R(1) \cdot R(2) \cdot R'(1) \cdot R'(2)) \\ &= (S(2) \cdot S(2)) \cdot R(1) \cdot R'(1) \cdot (R(2) \cdot R(2)) \cdot (R'(2) \cdot R'(2)) \\ &= 0 \cdot R(1) \cdot R'(1) \cdot 0 \cdot 0 \\ &= R(1) \cdot R'(1) \end{aligned}$$

であるから、 $D'(1,2) \cdot D'(2,2)$ を計算すれば、 $R(1) \cdot R'(1)$ が求まる。

【0147】

この $R(1) \cdot R'(1)$ 、 $R(2) \cdot R'(2)$ を使用して $S(1)$ 、 $S(2)$ を求める。

10

【0148】

$$\begin{aligned} D'(2,1) \cdot R(1) \cdot R'(1) &= (S(1) \cdot R(1) \cdot R'(1)) \cdot R(1) \cdot R'(1) \\ &= S(1) \cdot (R(1) \cdot R(1)) \cdot (R'(1) \cdot R'(1)) \\ &= S(1) \cdot 0 \cdot 0 \\ &= S(1) \end{aligned}$$

であるから、 $D'(2,1) \cdot R(1) \cdot R'(1)$ を計算すれば、 $S(1)$ が求まる。

【0149】

また同様に、

$$\begin{aligned} D'(1,2) \cdot R(2) \cdot R'(2) &= (S(2) \cdot R(2) \cdot R'(2)) \cdot R(2) \cdot R'(2) \\ &= S(2) \cdot (R(2) \cdot R(2)) \cdot (R'(2) \cdot R'(2)) \\ &= S(2) \cdot 0 \cdot 0 \\ &= S(2) \end{aligned}$$

20

であるから $D'(2,2) \cdot R(2) \cdot R'(2)$ を計算すれば $S(2)$ が求まる。

【0150】

一般に、 j を奇数として、

$$\begin{aligned} D'(1,j) \cdot D'(2,j) &= (S(j) \cdot R(j) \cdot R(j+1) \cdot R'(j) \cdot R'(j+1)) \cdot (S(j) \cdot R(j) \cdot R'(j)) \\ &= (S(j) \cdot S(j)) \cdot (R(j) \cdot R(j)) \cdot (R'(j) \cdot R'(j)) \cdot R(j+1) \cdot R'(j+1) \\ &= 0 \cdot 0 \cdot 0 \cdot R(j+1) \cdot R'(j+1) \\ &= R(j+1) \cdot R'(j+1) \end{aligned}$$

であるから $D'(1,j) \cdot D'(2,j)$ を計算すれば $R(j+1) \cdot R'(j+1)$ が求まる。

30

【0151】

また同様に、

$$\begin{aligned} D'(1,j+1) \cdot D'(2,j+1) &= (S(j+1) \cdot R(j+1) \cdot R'(j+1)) \cdot \\ &\quad (S(j+1) \cdot R(j) \cdot R(j+1) \cdot R'(j) \cdot R'(j+1)) \\ &= (S(j+1) \cdot S(j+1)) \cdot R(j) \cdot R'(j) \cdot \\ &\quad (R(j+1) \cdot R(j+1)) \cdot (R'(j+1) \cdot R'(j+1)) \\ &= 0 \cdot R(j) \cdot R'(j) \cdot 0 \cdot 0 \\ &= R(j) \cdot R'(j) \end{aligned}$$

であるから $D'(1,j+1) \cdot D'(2,j+1)$ を計算すれば $R(j) \cdot R'(j)$ が求まる。

【0152】

この $R(j) \cdot R'(j)$ 、 $R(j+1) \cdot R'(j+1)$ を使用して $S(j)$ 、 $S(j+1)$ を求める。

40

【0153】

$$\begin{aligned} D'(2,j) \cdot R(j) \cdot R'(j) &= (S(j) \cdot R(j) \cdot R'(j)) \cdot R(j) \cdot R'(j) \\ &= S(j) \cdot (R(j) \cdot R(j)) \cdot (R'(j) \cdot R'(j)) \\ &= S(j) \cdot 0 \cdot 0 \\ &= S(j) \end{aligned}$$

であるから $D'(2,j) \cdot R(j) \cdot R'(j)$ を計算すれば $S(j)$ が求まる。

【0154】

また同様に、

$$D'(1,j+1) \cdot R(j+1) \cdot R'(j+1) = (S(j+1) \cdot R(j+1) \cdot R'(j+1)) \cdot R(j+1) \cdot R'(j+1)$$

50

$$\begin{aligned}
 &=S(j+1)*(R(j+1)*R(j+1))* (R'(j+1)*R'(j+1)) \\
 &=S(j+1)*0*0 \\
 &=S(j+1)
 \end{aligned}$$

であるから $D'(1, j+1)*R(j+1)*R'(j+1)$ を計算すれば $S(j+1)$ が求まる。

【0155】

以上、乱数追加注入方式により再分割データを生成した場合には、3つの再分割データ $D'(1), D'(2), D'(3)$ のすべてを用いなくても、3つの再分割データのうち、2つの再分割データを用いて上述したように元データを復元することができる。

【0156】

また、乱数追加注入方式においては、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0157】

（乱数書き換え方式）

図9は、乱数書き換え方式におけるデータ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データ $D(1), D(2), D(3)$ を取得し（ステップS601）、次に、再分割の際に用いる乱数 R' を発生させる（ステップS603）。

【0158】

次に、分割データ $D(1), D(2), D(3)$ それぞれに乱数 R' を上述した乱数追加注入方式により注入する（ステップS605）。次に、乱数 R' を注入された分割データから旧乱数である R を消去して、新たな再分割データ $D'(1), D'(2), D'(3)$ を生成する（ステップS607, S609）。

【0159】

図10は、元データ S を、元データの半分の長さの処理単位ビット長 b に基づいて分割数 $n=3$ で3分割する場合の分割部分データの定義式、乱数 R' の再注入後の分割部分データの定義式、さらに乱数 R を消去後の分割部分データの定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0160】

本方式においては、ステップS605までは、上述した乱数追加注入方式と同様であるため、説明は省略し、古い乱数 R を消去した分割部分データの定義式について説明する。

【0161】

まず、第1の分割データ $D'(1)$ に対しては、図10に示すように、第1の分割部分データ $D'(1,1)$ は、定義式 $(S(1)*R(1)*R(2)*R'(1)*R'(2))*(R(1)*R(2))$ 、即ち、 $S(1)*R'(1)*R'(2)$ で定義され、第2の分割部分データ $D'(1,2)$ は、定義式 $(S(2)*R(2)*R'(2))*R(2)$ 、即ち、 $S(2)*R'(2)$ で定義される。なお、この定義式の一般形は、 $D'(1, j)$ に対しては $S(j)*R'(j)*R'(j+1)$ であり、 $D'(1, j+1)$ に対して $S(j+1)*R'(j+1)$ である（ j は奇数とする）。

【0162】

また、第2の分割データ $D'(2)$ に対しては、図10に示すように、 $D'(2,1)$ は $(S(1)*R(1)*R'(1))*R(1)$ 、即ち、 $S(1)*R'(1)$ で定義され、 $D'(2,2)$ は $(S(2)*R(1)*R(2)*R'(1)*R'(2))*R(1)*R(2)$ 、即ち、 $S(2)*R'(1)*R'(2)$ で定義される。この定義式の一般形は、 $D'(2, j)$ に対しては $S(j)*R'(j)*R'(j+1)$ であり、 $D(2, j+1)$ に対しては $S(j+1)*R'(j)*R'(j+1)$ である（ j は奇数とする）。

【0163】

また、第3の分割データ $D'(3)$ に対しては、図10に示すように、 $D'(3,1)$ は $(R(1)*R'(1))*R(1)$ 、即ち、 $R'(1)$ で定義され、 $D'(3,2)$ は $(R(2)*R'(2))*R(2)$ 、即ち、 $R'(2)$ で定義される。この定義式の一般形は、 $D'(3, j)$ に対しては $R'(j)*R'(j+1)$ であり、 $D(3, j+1)$ に対しては $R'(j+1)$ である（ j は奇数とする）。

【0164】

このように、再分割部分データ $D'(i, j)$ はそれぞれ、分割部分データ $D(i, j)$ に、分割

10

20

30

40

50

部分データD (i, j)の定義式で注入されていた乱数部分データR(j)に対応する乱数部分データR'(j)を注入した後、さらに乱数部分データR(j)を消去するように乱数部分データR(j)を注入して排他的論理和を計算し、求めるものである。

【0165】

その結果、もとの分割部分データD (i, j)の定義式において、乱数部分データR(j)を乱数部分データR'(j)に置換したものが、再分割部分データD'(i, j)の定義式となる。

【0166】

次に、図10の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、機密情報管理システム1の元データ復元部16の機能を説明するものである。

10

【0167】

まず、分割部分データD'(2,1), D'(3,1)から第1の元部分データS(1)を次のように生成することができる。

【0168】

$$\begin{aligned} D'(2,1) * D'(3,1) &= (S(1) * R'(1)) * R'(1) \\ &= S(1) * (R'(1) * R'(1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

また、別の分割部分データから次のように第2の元部分データS(2)を生成することができる。

20

【0169】

$$\begin{aligned} D'(2,2) * D'(3,1) * D'(3,2) &= (S(2) * R'(1) * R'(2)) * R'(1) * R'(2) \\ &= S(2) * (R'(1) * R'(1)) * (R'(2) * R'(2)) \\ &= S(2) * 0 * 0 \\ &= S(2) \end{aligned}$$

一般に、jを奇数として、

$$\begin{aligned} D'(2,j) * D'(3,j) &= (S(j) * R'(j)) * R'(j) \\ &= S(j) * (R'(j) * R'(j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

30

であるから、D'(2,j) * D'(3,j)を計算すれば、S(j)が求まる。

【0170】

また、一般に、jを奇数として、

$$\begin{aligned} D'(2,j+1) * D'(3,j) * D'(3,j+1) &= (S(j+1) * R'(j) * R'(j+1)) * R'(j) * R'(j+1) \\ &= S(j+1) * (R'(j) * R'(j)) * (R'(j+1) * R'(j+1)) \\ &= S(j+1) * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから、D'(2,j+1) * D'(3,j) * D'(3,j+1)を計算すれば、S(j+1)が求まる。

【0171】

次に、D'(1), D'(3)を取得してSを復元する場合には、次のようになる。

40

【0172】

$$\begin{aligned} D'(1,1) * D'(3,1) * D'(3,2) &= (S(1) * R'(1) * R'(2)) * R'(1) * R'(2) \\ &= S(1) * (R'(1) * R'(1)) * (R'(2) * R'(2)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

であるから、D'(1,1) * D'(3,1) * D'(3,2)を計算すれば、S(1)が求まる。

【0173】

また同様に、

$$\begin{aligned} D'(1,2) * D'(3,2) &= (S(2) * R'(2)) * R'(2) \\ &= S(2) * (R'(2) * R'(2)) \end{aligned}$$

50

$$=S(2)*0$$

$$=S(2)$$

であるから、 $D'(1,2)*D'(3,2)$ を計算すれば、 $S(2)$ が求まる。

【0174】

一般に、 j を奇数として、

$$D'(1,j)*D'(3,j)*D'(3,j+1)=(S(j)*R'(j)*R'(j+1))*R'(j)*R'(j+1)$$

$$=S(j)*(R'(j)*R'(j))*(R'(j+1)*R'(j+1))$$

$$=S(j)*0*0$$

$$=S(j)$$

であるから、 $D'(1,j)*D'(3,j)*D'(3,j+1)$ を計算すれば、 $S(j)$ が求まる。

10

【0175】

また、一般に、 j を奇数として、

$$D'(1,j+1)*D'(3,j+1)=(S(j+1)*R'(j+1))*R'(j+1)$$

$$=S(j+1)*(R'(j+1)*R'(j+1))$$

$$=S(j+1)*0$$

$$=S(j+1)$$

であるから、 $D'(1,j+1)*D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0176】

次に、 $D'(1),D'(2)$ を取得して S を復元する場合には、次のようになる。

【0177】

$$D'(1,1)*D'(2,1)=(S(1)*R'(1)*R'(2))*(S(1)*R'(1))$$

$$=(S(1)*S(1))*(R'(1)*R'(1))*R'(2)$$

$$=0*0*R'(2)$$

$$=R'(2)$$

であるから、 $D'(1,1)*D'(2,1)$ を計算すれば、 $R'(2)$ が求まる。

【0178】

また同様に、

$$D'(1,2)*D'(2,2)=(S(2)*R'(2))*(S(2)*R'(1)*R'(2))$$

$$=(S(2)*S(2))*(R'(2)*R'(2))*R'(1)$$

$$=0*0*R'(1)$$

$$=R'(1)$$

であるから、 $D'(1,2)*D'(2,2)$ を計算すれば、 $R'(1)$ が求まる。

【0179】

この $R'(1),R'(2)$ を使用して $S(1),S(2)$ を求める。

【0180】

$$D'(2,1)*R'(1)=(S(1)*R'(1))*R'(1)$$

$$=S(1)*(R'(1)*R'(1))$$

$$=S(1)*0$$

$$=S(1)$$

であるから、 $D'(2,1)*R'(1)$ を計算すれば、 $S(1)$ が求まる。

40

【0181】

また同様に、

$$D'(1,2)*R'(2)=(S(2)*R'(2))*R'(2)$$

$$=S(2)*(R'(2)*R'(2))$$

$$=S(2)*0$$

$$=S(2)$$

であるから $D'(1,2)*R'(2)$ を計算すれば $S(2)$ が求まる。

【0182】

一般に、 j を奇数として、

$$D'(1,j)*D'(2,j)=(S(j)*R'(j)*R'(j+1))*(S(j)*R'(j))$$

50

$$\begin{aligned}
 &= (S(j) * S(j)) * (R'(j) * R'(j)) * R'(j+1) \\
 &= 0 * 0 * R'(j+1) \\
 &= R'(j+1)
 \end{aligned}$$

であるから $D'(1, j) * D'(2, j)$ を計算すれば $R'(j+1)$ が求まる。

【0183】

また同様に、

$$\begin{aligned}
 D'(1, j+1) * D'(2, j+1) &= (S(j+1) * R'(j+1)) * (S(j+1) * R'(j) * R'(j+1)) \\
 &= (S(j+1) * S(j+1)) * (R'(j+1) * R'(j+1)) * R'(j) \\
 &= 0 * 0 * R'(j) \\
 &= R'(j)
 \end{aligned}$$

10

であるから $D'(1, j+1) * D'(2, j+1)$ を計算すれば $R'(j)$ が求まる。

【0184】

この $R'(j)$, $R'(j+1)$ を使用して $S(j)$, $S(j+1)$ を求める。

【0185】

$$\begin{aligned}
 D'(2, j) * R'(j) &= (S(j) * R'(j)) * R'(j) \\
 &= S(j) * (R'(j) * R'(j)) \\
 &= S(j) * 0 \\
 &= S(j)
 \end{aligned}$$

であるから $D'(2, j) * R'(j)$ を計算すれば $S(j)$ が求まる。

【0186】

20

また同様に、

$$\begin{aligned}
 D'(1, j+1) * R'(j+1) &= (S(j+1) * R'(j+1)) * R'(j+1) \\
 &= S(j+1) * (R'(j+1) * R'(j+1)) \\
 &= S(j+1) * 0 \\
 &= S(j+1)
 \end{aligned}$$

であるから $D'(1, j+1) * R'(j+1)$ を計算すれば $S(j+1)$ が求まる。

【0187】

以上、乱数書き換え方式により再分割データを生成した場合には、3つの再分割データ $D'(1)$, $D'(2)$, $D'(3)$ のすべてを用いなくても、3つの再分割データのうち、2つの再分割データを用いて上述したように元データを復元することができる。

30

【0188】

また、乱数書き換え方式においても、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0189】

<動作>

次に、本実施の形態に係る機密情報管理システム1が適用されるコンピュータシステム10全体の動作について説明する。ここで、図11は、ユーザが機密情報Sを機密情報管理システム1に登録する動作を説明するシーケンス図であり、図12は、ユーザがサービスを利用する時の機密情報管理システム1及び端末2の動作を説明するシーケンス図である。

40

【0190】

(1) 機密情報登録処理

まず、ユーザが端末2から機密情報管理システム1に機密情報Sを送信（又は送付）する（ステップS10）。機密情報システム1は、機密情報Sと同じ長さの真性乱数Rを生成し、該真性乱数R及び機密情報Sから、上述した秘密分散法Aを用いて3つのデータ（分割データ） $D(1)$, $D(2)$, $D(3)$ を生成する（ステップS20, S30）。例えば、具体的には、

$$\begin{aligned}
 D(1) &= (S(1) * R(1) * R(2)) \quad (S(2) * R(2)) \\
 D(2) &= (S(1) * R(1)) \quad (S(2) * R(1) * R(2))
 \end{aligned}$$

50

$D(3) = R(1) \ R(2)$

が生成される。ただし、 \oplus は、ビット列とビット列との結合を意味する。

【0191】

次に、機密情報管理システム1は、 $r_0 = h(D(3))$ を初期情報(乱数種初期値)として生成する(ステップS40)。尚、 h はハッシュ関数を表し、具体的には、SHA-1、SHA-256、SHA-512などであり、任意の長さのデータから、それぞれ128ビット、256ビット、及び512ビットのハッシュ値を生成するようになっている。また、本実施の形態におけるハッシュ値 $h(D(3))$ のデータの長さは、後述する疑似乱数アルゴリズムGのシードの長さ以上であればよい。

【0192】

次に、機密情報管理システム1は、このようにして生成された分割データD(1)及びD(2)をそれぞれ保管サーバ3a及び3bに送信し、分割データD(3)及び初期情報 r_0 を端末2に送信(又は送付)する(ステップS50)。

【0193】

これにより、端末2は、送信されてきた分割データD(3)及び初期情報 r_0 をハードディスク等の記憶装置に記憶するとともに(ステップS60)、保管サーバ3a及び3bは、それぞれ送信されてきた分割データD(1)、D(2)をハードディスク等の記憶装置に記憶する(ステップS70)。また、機密情報管理システム1は、初期情報 r_0 をハードディスク等の記憶装置に記憶する(ステップS80)。

【0194】

最後に、機密情報管理システム1は、真性乱数Rを消去し、カウンタ値nを十分に大きい値、例えば、 $n = 100$ と設定して、記憶装置に記憶する(ステップS100, S110)。

【0195】

(2) サービス利用処理

ユーザがサービス提供システム5を利用する場合には、まず、ユーザは機密情報Sの使用を機密情報管理システム1に対して要求する(ステップS210)。これは、端末2から機密情報Sの使用を要求する旨をオープンな通信ネットワーク4bを介して機密情報管理システム1に送信するものである。

【0196】

機密情報管理システム1は、端末2から機密情報Sの使用要求を受け取ると、カウンタ値nを記憶装置から取得して、端末2に送信する(ステップS220)。これにより、機密情報管理システム1及び端末2においては、上述した秘密分散法Sを用いて同期がとられた再分割データを生成する。

【0197】

機密情報管理システム1においては、カウンタ値n及び乱数種初期値 r_0 を用いて乱数種情報 $r_n = h^n(r_0)$ を生成する(ステップS230)。尚、 $r_n = h(r_{n-1})$ であり、例えば、 $r_1 = h(r_0)$ 、 $r_2 = h(h(r_0))$ 、 $r_3 = h(h(h(r_0)))$...であり、 $n = 100$ のときには、 r_0 に対してハッシュ値を100回求めることになる。

【0198】

次に、所定の疑似乱数生成アルゴリズムGを用いて、乱数種情報 r_n から、機密情報Sと同じ長さの疑似乱数 $R' (= G(r_n))$ を生成する(ステップS240)。尚、乱数種情報 r_n のデータの長さが、疑似乱数アルゴリズムGの乱数生成に用いられるシードの長さより長い場合には、例えば、ハッシュ値の先頭からシードの長さ分だけ取り出すなど、データ長の調節を行う。

【0199】

次に、保管サーバ3a及び3bから取得した分割データD(1)及びD(2)、並びに疑似乱数 R' から上述した秘密分散法Aを用いて再分割データD'(1)及びD'(2)を生成する(ステップS250, S260)。尚、データ再分割の方法は、乱数追加注入方式及び乱数書き

10

20

30

40

50

換え方式のいずれでもよいが、乱数追加注入方式の場合には、例えば、具体的には、

$$D'(1) = (D(1,1) * R'(1) * R'(2)) \quad (D(1,2) * R'(2))$$

$$D'(2) = (D(2,1) * R'(1)) \quad (D(2,2) * R'(1) * R'(2))$$

が生成される。

【0200】

次に、機密情報管理システム1は、分割データD(1)及びD(2)に代えて、保管サーバ3a及び3bに再分割データD'(1)及びD'(2)をそれぞれ記憶させる(ステップS270)。

【0201】

一方、端末2においても、機密情報管理システム1から送信されたカウンタ値n及び乱数種初期値 r_0 を用いて、機密情報管理システム1と同様に、乱数種情報 $r_n = h^n (r_0)$ を生成する(ステップS280)。

10

【0202】

次に、所定の疑似乱数生成アルゴリズムGを用いて、機密情報管理システム1と同様に、乱数種情報 r_n から、機密情報Sと同じ長さの疑似乱数 $R' (= G(r_n))$ を生成する(ステップS290)。尚、乱数種情報 r_n のデータの長さが、疑似乱数アルゴリズムGの乱数生成に用いられるシードの長さより長い場合には、例えば、ハッシュ値の先頭からシードの長さ分だけ取り出すなど、データ長の調節を行う。

【0203】

次に、分割データD(3)及び疑似乱数 R' から上述した秘密分散法Aを用いて再分割データD'(3)を生成する(ステップS300)。尚、乱数追加注入方式の場合には、例えば、

20

$$D'(3) = (D(3,1) * R'(1)) \quad (D(3,2) * R'(2))$$

が生成される。

【0204】

次に、端末2は、分割データD(3)に代えて、記憶装置に再分割データD'(3)を記憶させるとともに、再分割データD'(3)を機密情報管理システム1にオープンな通信ネットワーク4bを介して送信する(ステップS310, S320)。

【0205】

これにより、機密情報管理システム1は、同期がとられた再分割データD'(1), D'(2), D'(3)を取得するので、再分割データD'(1), D'(2), D'(3)のいずれか2つから秘密分散法Aを用いて機密情報Sを復元する(ステップS330)。そして、復元した機密情報Sをセキュアな通信ネットワーク4aを介してサービス提供システム5に送信する(ステップS340)。

30

【0206】

サービス提供システム5は、機密情報管理システム1から機密情報Sを受け取ると、該機密情報Sの正当性を判断して、端末2に通信ネットワーク4を介してサービス提供を行う(ステップS350, S360)。これにより、ユーザは所望のサービスの提供を受けることができる。

【0207】

最後に、機密情報管理システム1は、カウンタ値nを1減算し(例えば、 $n = 100$ の場合には、 $n = 99$ になる)、更新されたカウンタ値を記憶装置に記憶させる(ステップS370, S380)。

40

【0208】

従って、ユーザが次回、機密情報Sを使ってサービス提供システム5を利用する場合には、1減算されたカウンタ値をもとに再分割データD'(1), D'(2), D'(3)が生成されることになる。尚、カウンタ値nが0となったときは、再度、機密情報登録処理のステップS20~S110の処理を実行した後、上記サービス利用処理を実行するものである。

【0209】

次に、サービス利用時に端末2から送信される再分割データD'(3)が、仮に第三者に盗聴されたとしても、なりすましが不可能であることを以下に示す。

50

【 0 2 1 0 】

定義より、 $D'(3) = (D(3,1) * R'(1)) \quad (D(3,2) * R'(2))$

ここで、 $D'(3)$ の前半部と後半部とを別々に排他的論理和 (XOR) を計算するのも、前半部と後半部を接続したものに排他的論理和 (XOR) を計算するのも結果は同じであるため、

$$\begin{aligned} D'(3) &= (D(3,1) \quad D(3,2)) * (R'(1) \quad R'(2)) \\ &= R * R' \\ &= R * G(r_n) \\ &= R * G(h^n(r_0)) \end{aligned}$$

この結果から、第3者が $D'(3)$ を盗聴して、仮に $D'(3)$ から R 、 r_0 を算出し、疑似乱数アルゴリズム G を把握できれば、上述したサービス利用処理のステップ $S210 \sim S310$ を実行することで、送信すべき再分割データ $D'(3)$ を求めることはできるが、実際には、 R は真性乱数であり数式等に基づく規則性がないため、 $D'(3)$ を盗聴しても、 $G(h^n(r_0))$ を特定することができない。これは、パーナム暗号(データと同じ長さの乱数列を用意し、暗号化に際してはデータの n ビット目と乱数列の n ビット目の排他的論理和 (XOR) を計算し、復号化に際しては暗号化されたデータの n ビット目と乱数列の n ビット目の排他的論理和 (XOR) を計算する暗号)は、いくら計算リソースがあっても鍵となる乱数列がなければデータを得ることができないことに起因する。また、 R が真性乱数でなく(上記実施の形態においては好適な形態として真性乱数を用いたが、疑似乱数を用いた場合)、仮に、 $G(h^n(r_0))$ が特定でき、さらに疑似乱数アルゴリズム G のシード $h^n(r_0)$ が逆算できたとしても、ハッシュ関数は一方向性関数であるため、 r_0 を計算することはできず、結局のところ、第3者のなりすましは不可能である。

【 0 2 1 1 】

従って、本実施の形態によれば、機密情報を秘密分散法 A を用いて複数に分割して、そのうちの一部をユーザに保持させるとともに、機密情報を使用するたびに、各分割データを同期をとって更新して再分割データを生成するので、仮にユーザが保持する機密情報の一部が第3者に漏洩したとしても、第3者のなりすましを確実に防止することができ、セキュリティを十分に確保することができる。

【 0 2 1 2 】

特に、本発明における秘密分散法 A は、機密情報を所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、機密情報を処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、機密情報のビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、機密情報を復元することなく、機密情報を再分割することができるので、ユーザの機密情報をよりセキュアに管理することができる。所定のサービスを受ける際に必要とされる機密情報 S を秘密分散法 A を用いて複数に分割して、そのうちの一部をユーザに保持させるので、ユーザが保持する分割データの紛失があったとしても、残りの分割データから機密情報 S を復元できるとともに、秘密分散法 A を用いて新たに再分割データを生成し、該再分割データの一部を新たにユーザに保持させるので、機密情報 S の変更は不要である。

【 0 2 1 3 】

尚、本実施の形態における秘密分散法 A は、多項式演算・剰余演算などを含む多倍長整数の演算処理を必要としないので、大容量データを多数処理する場合においても簡単かつ迅速にデータの分割および復元を行うことができるという効果を得ることができる。

【 0 2 1 4 】

10

20

30

40

50

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、機密情報管理システム1が端末2にカウンタ値nを送信することにより、機密情報管理システム1と端末2の同期をとっていたが、本発明において同期をとる方法はこれに限定されず、減少する同期値を用いるのであれば、他の方法であってもよい。例えば、機密情報管理システム1及び端末2それぞれの時計を同じ時刻に合わせるとともに、nを所定の時期（例えば、具体的には、2004年12月31日）までの残りの秒数として同期をとるようにしてもよい。

【0215】

また、本実施の形態においては、乱数種初期値 r_0 を $r_0 = h(D(3))$ とし、分割データD(3)に依存するように設定したが、乱数種初期値 r_0 を分割データに依存させず、独立に所定の値を与えてもよいものである。

【図面の簡単な説明】

【0216】

【図1】本発明の実施の形態に係る機密情報管理システムが適用されるコンピュータシステム全体の概略構成を示すブロック図である。

【図2】本発明の実施の形態に係る機密情報管理システムの分割数 $n=3$ の場合の分割処理を示すフローチャートである。

【図3】16ビットの元データSを8ビットの処理単位ビット長に基づいて分割数 $n=3$ で3分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図4】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成する定義式を示す表である。

【図5】本発明の実施の形態に係る機密情報管理システムの分割数が n で処理単位ビット長が b である場合の一般的な分割処理を示すフローチャートである。

【図6】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成する定義式の別の例を示す表である。

【図7】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理（乱数追加注入方式）を示すフローチャートである。

【図8】乱数追加注入方式により元データSを元データSの半分の長さの処理単位ビット長に基づいて分割数 $n=3$ で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図9】本発明の実施の形態に係る機密情報管理システムにおけるデータ再分割処理（乱数書き換え方式）を示すフローチャートである。

【図10】乱数書き換え方式により元データSを元データSの半分の長さの処理単位ビット長に基づいて分割数 $n=3$ で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図11】本発明の実施の形態に係る機密情報管理システムにおいて機密情報を登録する処理を説明するシーケンス図である。

【図12】本発明の実施の形態に係る機密情報管理システムにおいてサービス利用時の処理を説明するシーケンス図である。

【符号の説明】

【0217】

- 1 ... 機密情報管理システム
- 2 ... 端末
- 3 a, 3 b ... 保管サーバ
- 4 ... 通信ネットワーク
- 5 ... サービス提供システム
- 10 ... コンピュータシステム
- 11 ... 分割データ生成部

10

20

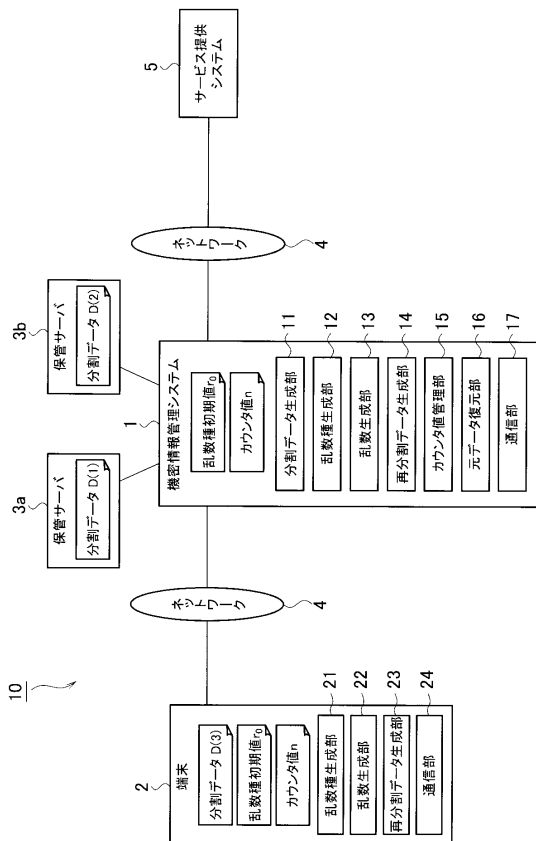
30

40

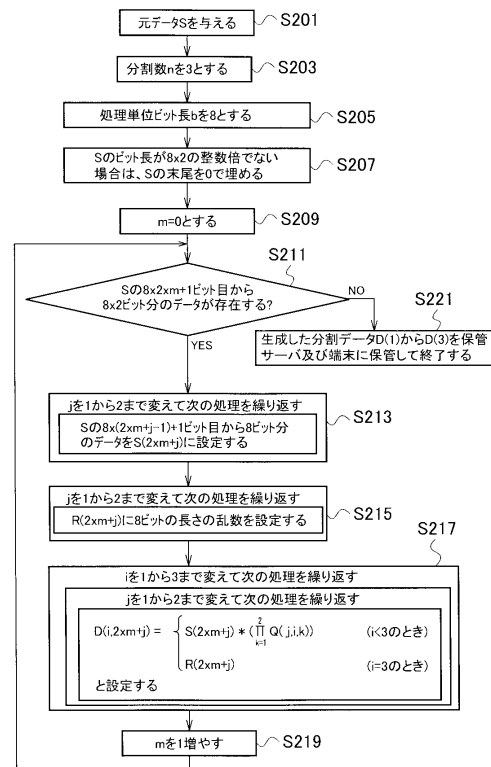
50

- 1 2 ... 乱数種生成部
- 1 3 ... 乱数生成部
- 1 4 ... 再分割データ生成部
- 1 5 ... カウンタ値管理部
- 1 6 ... 元データ復元部
- 1 7 ... 通信部
- 2 1 ... 乱数種生成部
- 2 2 ... 乱数生成部
- 2 3 ... 再分割データ生成部
- 2 4 ... 通信部

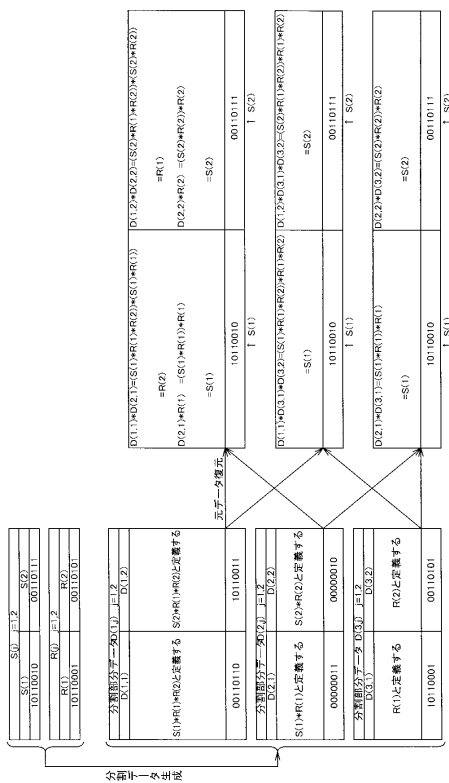
【図1】



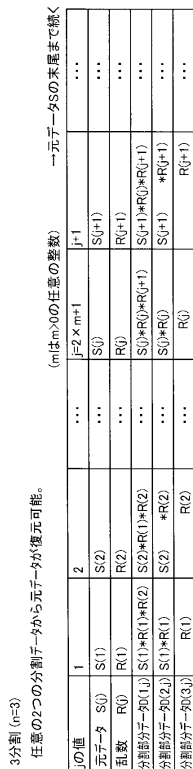
【図2】



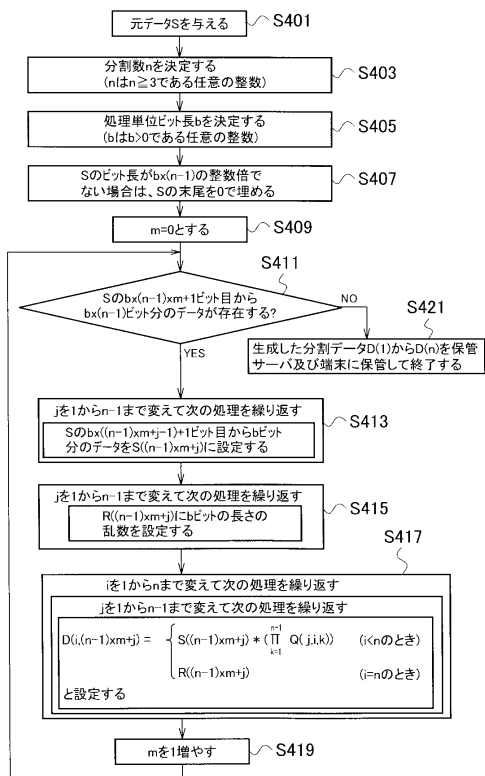
【図3】



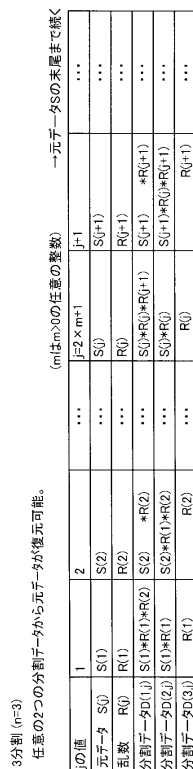
【図4】



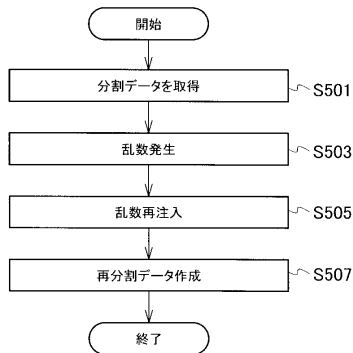
【図5】



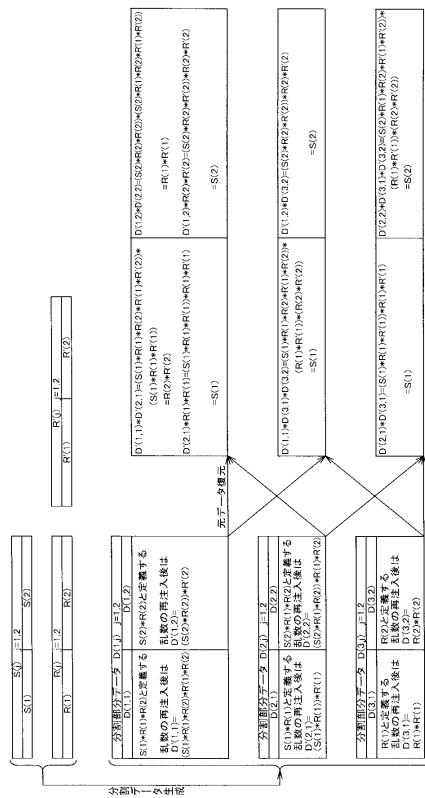
【図6】



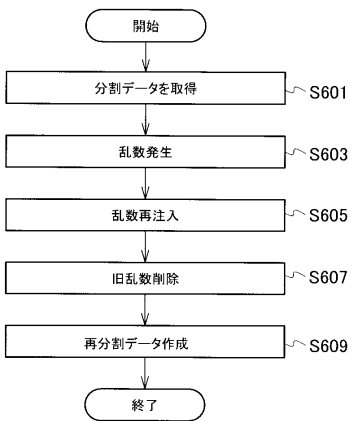
【図7】



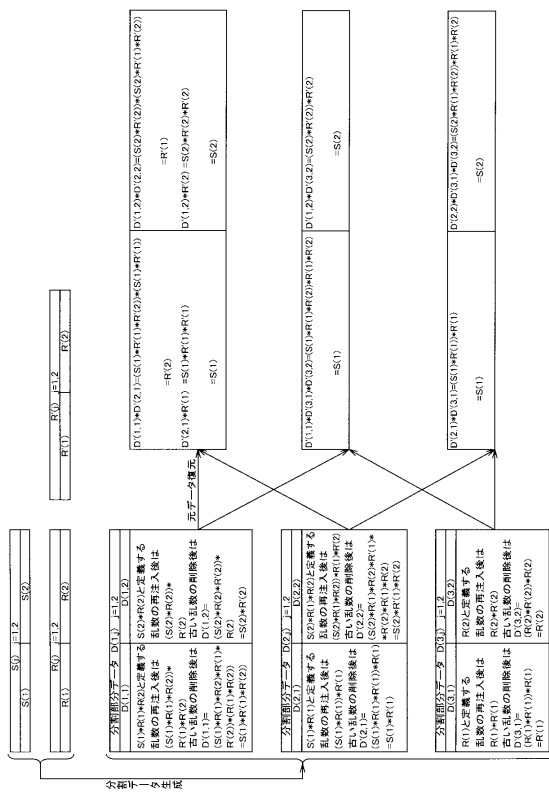
【図8】



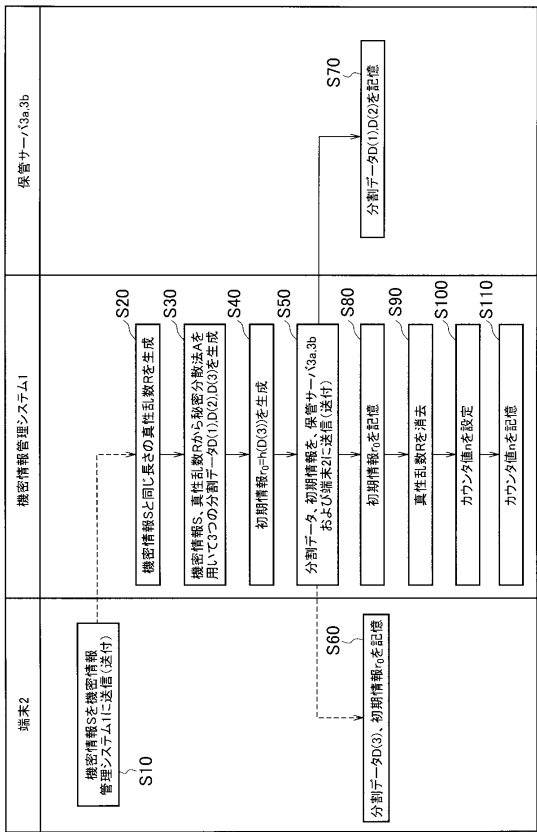
【図9】



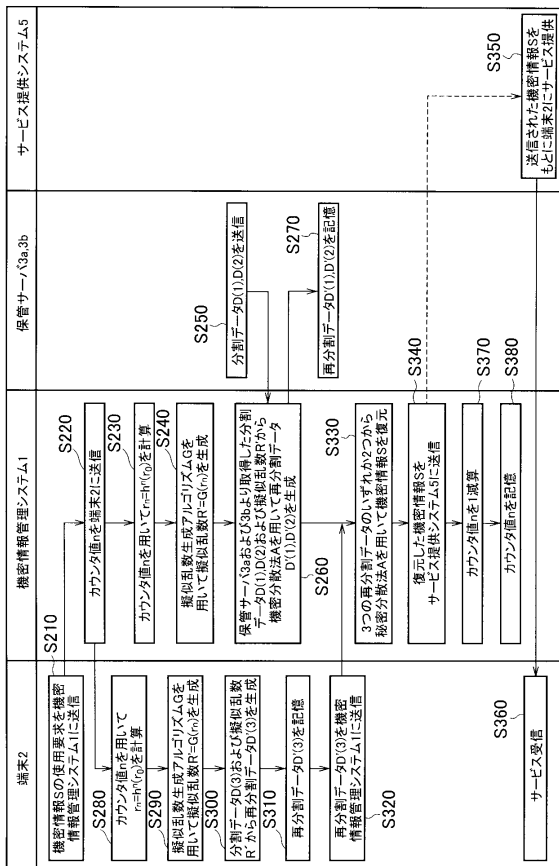
【図10】



【 図 1 1 】



【 図 1 2 】



フロントページの続き

- (72)発明者 荻原 利彦
東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
- (72)発明者 加賀谷 誠
東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内
- (72)発明者 野村 進
東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内

審査官 鳥居 稔

- (56)参考文献 特開2004-053969(JP,A)
特開平11-317734(JP,A)
特開2003-132229(JP,A)
特開2004-147218(JP,A)
廣田啓一、北原亮、ランプ型閾値秘密分散法における部分情報の復元制御、信学技報、社団法人
電子情報通信学会、2003年11月6日
秘密分散システムの暗号システムへの応用について、1991年電子情報通信学会春季全国大会講演
論文集、1991年3月15日
尾形わかば 黒沢馨、秘密分散共有法とその応用、電子情報通信学会誌、1999年12月25
日、Vol.82 No.12 pp.1228 1236

(58)調査した分野(Int.Cl., DB名)

H04L 9/08
G06F 21/24
G09C 1/00