(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4664008号
(P4664008)
(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月14日(2011.1.14)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　G09C 1/00 610Z
H04L 9/20 (2006.01)　G09C 1/00 650Z
H04L 9/32 (2006.01)　H04L 9/00 653
　　H04L 9/00 675Z

請求項の数 11　(全 37 頁)

(21)出願番号　特願2004-169001 (P2004-169001)
(22)出願日　平成16年6月7日 (2004.6.7)
(65)公開番号　特開2005-346006 (P2005-346006A)
(43)公開日　平成17年12月15日 (2005.12.15)
審査請求日　平成19年6月6日 (2007.6.6)

(73)特許権者　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(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】アクセス権管理システム、アクセス権管理装置、アクセス権管理方法、端末用プログラム、及びアクセス権管理プログラム

(57)【特許請求の範囲】
【請求項１】
データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムであって、
前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成する手段と、
前記第１の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信する手段と、
前記譲受側端末において、前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成する手段と、
前記第２の暗号データを前記譲受側端末から前記譲渡側端末に送信する手段と、
前記譲渡側端末において、前記譲渡側端末の前記第１の暗号鍵で前記第２の暗号データを暗号化し、第３の暗号データを生成する手段と、
前記第３の暗号データを前記譲渡側端末から前記譲受側端末に送信する手段と、
前記譲受側端末において、前記第３の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶する手段と、
を有することを特徴とするアクセス権管理システム。
【請求項２】
前記譲受側端末において、前記記憶部に記憶された前記第３の暗号データを前記第２の暗号鍵で復号し、前記データを生成する手段を有することを特徴とする請求項１記載のア

クセス権管理システム。
【請求項３】
複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、
前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成する手段と、
前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、
前記第１の暗号鍵を前記譲渡側端末に送信する手段と、
前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第１の暗号鍵を受信する手段と、
前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成する手段と、
前記第２の暗号データを前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、
前記第２の暗号鍵を前記譲受側端末に送信する手段と、
を有することを特徴とするアクセス権管理装置。
【請求項４】
前記データが使用されるときは、前記譲受側端末から前記第２の暗号鍵を受信する手段と、
前記記憶部に記憶された第２の暗号データを、受信した第２の暗号鍵で復号化し、前記データを生成する手段と、
を有することを特徴とする請求項３記載のアクセス権管理装置。
【請求項５】
データをバーナム暗号を用いて暗号化する端末を複数備えたアクセス権管理システムの該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理方法であって、
前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、
前記第１の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、
前記譲受側端末において、前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成するステップと、
前記第２の暗号データを前記譲受側端末から前記譲渡側端末に送信するステップと、
前記譲渡側端末において、前記譲渡側端末の前記第１の暗号鍵で前記第２の暗号データを暗号化し、第３の暗号データを生成するステップと、
前記第３の暗号データを前記譲渡側端末から前記譲受側端末に送信するステップと、
前記譲受側端末において、前記第３の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、
を有することを特徴とするアクセス権管理方法。
【請求項６】
複数の端末と相互に通信可能なアクセス権管理装置が、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、
前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、
前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、
前記第１の暗号鍵を前記譲渡側端末に送信するステップと、
前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第１の暗号鍵を

受信するステップと、
前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成するステップと、
前記第２の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、
前記第２の暗号鍵を前記譲受側端末に送信するステップと、
を有することを特徴とするアクセス権管理方法。
【請求項７】
データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、
前記データのアクセス権限を有する譲渡側端末に、
該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、
前記第１の暗号データを前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、
前記譲受側端末から、前記譲受側端末の第２の暗号鍵で暗号化して、生成された第２の暗号データを受信するステップと、
前記第１の暗号鍵で前記第２の暗号データを暗号し、第３の暗号データを生成するステップと、
前記第３の暗号データを、アクセス権譲渡のデータとして前記譲受側端末に送信するステップと、
を実行させることを特徴とする端末用プログラム。
【請求項８】
データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、
前記データのアクセス権限を譲り受ける譲受側端末に、
前記データのアクセス権限を有する譲渡側端末から、該譲渡側端末の第１の暗号鍵で前記データを暗号化して、生成された第１の暗号データを受信するステップと、
前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成するステップと、
前記第２の暗号データを前記譲受側端末に送信するステップと、
前記譲渡側端末から、前記第１の暗号鍵で前記第２の暗号データを暗号化して、生成された第３の暗号データを受信するステップと、
前記第３の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、
を実行させることを特徴とする端末用プログラム。
【請求項９】
前記記憶部に記憶された前記第３の暗号データを前記第２の暗号鍵で復号し、前記データを生成するステップを前記譲受側端末に実行させることを特徴とする請求項８記載の端末用プログラム。
【請求項１０】
複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、
前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、
前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータ

として記憶するステップと、
前記第１の暗号鍵を前記譲渡側端末に送信するステップと、
前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第１の暗号鍵を受信するステップと、
前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成するステップと、
前記第２の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、
前記第２の暗号鍵を前記譲渡側端末に送信するステップと、
を前記コンピュータに実行させることを特徴とするアクセス権管理プログラム。
【請求項１１】
前記データが使用されるときは、前記譲受側端末から前記第２の暗号鍵を受信するステップと、
前記記憶部に記憶された第２の暗号データを、受信した第２の暗号鍵で復号化し、前記データを生成するステップと、
を前記コンピュータに実行させることを特徴とする請求項１０記載のアクセス権管理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化されたデータを他人に譲渡する、又は暗号化されたデータのアクセス権を他人に譲渡する場合のセキュリティ技術に関する。
【背景技術】
【０００２】
従来、自己が保有するデータへのアクセスを制限する方法の１つとして、暗号化してデータへのアクセスを制限するという方法がある。例えば、自己の秘匿したいデータ、重要な機密データなどに対して、他人からのアクセスを防ぐには、データを暗号化して保管するというものである。このような場合、暗号化されたデータは、暗号鍵の所有者以外には誰も復号できない。
【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】電子商取引実証推進協議会セキュリティＷＧ、“暗号利用技術ハンドブック（第２版）”、[Online]、［平成１６年５月２０日検索］、インターネット＜ＵＲＬ：http://www.ecom.jp/qecom/seika/naiyou/11report/e11-sec3.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、このような暗号化されたデータのアクセス権限を他人に譲渡したい場合（暗号化されたデータ自体を他人に譲渡したい場合も含む。以下、同じ。）には、自己の暗号鍵を他人に譲渡する場合を除けば、一旦、暗号化されたデータを自己の暗号鍵で復号化し、さらに、譲渡後、他人が自己の暗号鍵でデータを暗号化する必要がある。この場合には、暗号化されたデータが一旦、復号化され、暗号化されていない状態で譲渡されるので、この状態でデータが漏洩した場合、セキュリティが十分確保されないという問題がある。
【０００５】
本発明は、上記の事情に鑑みてなされたものであり、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、データ復号化によるデータ漏洩の危険性を回避して、セキュリティを十分に確保し得るアクセス権管理システム、アクセス権管理装置、アクセス権管理方法、端末用プログラム、及びアクセス権管理プログラム

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、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムであって、前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成する手段と、前記第１の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信する手段と、前記譲受側端末において、前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成する手段と、前記第２の暗号データを前記譲受側端末から前記譲渡側端末に送信する手段と、前記譲渡側端末において、前記譲渡側端末の前記第１の暗号鍵で前記第２の暗号データを暗号化し、第３の暗号データを生成する手段と、前記第３の暗号データを前記譲渡側端末から前記譲受側端末に送信する手段と、前記譲受側端末において、前記第３の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶する手段と、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、前記譲受側端末において、前記記憶部に記憶された前記第３の暗号データを前記第２の暗号鍵で復号し、前記データを生成する手段を有することを特徴とする。
【０００８】
請求項３記載の本発明は、複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成する手段と、前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、前記第１の暗号鍵を前記譲渡側端末に送信する手段と、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第１の暗号鍵を受信する手段と、前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成する手段と、前記第２の暗号データを前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、前記第２の暗号鍵を前記譲受側端末に送信する手段と、を有することを特徴とする。
【０００９】
請求項４記載の本発明は、請求項３記載の発明において、前記データが使用されるときは、前記譲受側端末から前記第２の暗号鍵を受信する手段と、前記記憶部に記憶された第２の暗号データを、受信した第２の暗号鍵で復号化し、前記データを生成する手段と、を有することを特徴とする。
【００１３】
請求項５記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えたアクセス権管理システムの該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理方法であって、前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、前記第１の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、前記譲受側端末において、前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成するステップと、前記第２の暗号データを前記譲受側端末から前記譲渡側端末に送信するステップと、前記譲渡側端末において、前記譲渡側端末の前記第１の暗号鍵で前記第２の暗号データを暗号化し、第３の暗号データを生成するステップと、前記第３の暗号データを前記譲渡側端末から前記譲受側端末に送信するステップと、前記譲受側端末において、前記第３の暗号デ

ータを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、を有することを特徴とする。

【００１４】

請求項６記載の本発明は、複数の端末と相互に通信可能なアクセス権管理装置が、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、前記第１の暗号鍵を前記譲渡側端末に送信するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第１の暗号鍵を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成するステップと、前記第２の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、前記第２の暗号鍵を前記譲受側端末に送信するステップと、を有することを特徴とする。

【００１６】

請求項７記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、前記データのアクセス権限を有する譲渡側端末に、該譲渡側端末の第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、前記第１の暗号データを前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、前記譲受側端末から、前記譲受側端末の第２の暗号鍵で暗号化して、生成された第２の暗号データを受信するステップと、前記第１の暗号鍵で前記第２の暗号データを暗号し、第３の暗号データを生成するステップと、前記第３の暗号データを、アクセス権譲渡のデータとして前記譲受側端末に送信するステップと、を実行させることを特徴とする。

【００１７】

請求項８記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、前記データのアクセス権限を譲り受ける譲受側端末に、前記データのアクセス権限を有する譲渡側端末から、該譲渡側端末の第１の暗号鍵で前記データを暗号化して、生成された第１の暗号データを受信するステップと、前記譲受側端末の第２の暗号鍵で前記第１の暗号データを暗号化し、第２の暗号データを生成するステップと、前記第２の暗号データを前記譲受側端末に送信するステップと、前記譲渡側端末から、前記第１の暗号鍵で前記第２の暗号データを暗号化して、生成された第３の暗号データを受信するステップと、前記第３の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、を実行させることを特徴とする。

【００１８】

請求項９記載の本発明は、請求項８記載の発明において、前記記憶部に記憶された前記第３の暗号データを前記第２の暗号鍵で復号し、前記データを生成するステップを前記譲受側端末に実行させることを特徴とする。

【００１９】

請求項１０記載の本発明は、複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、前記データのアクセス権限を有する譲渡側端末の第１の暗号鍵を生成し、該第１の暗号鍵で前記データを暗号化し、第１の暗号データを生成するステップと、前記第１の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、前記第１の暗号鍵を前記譲渡側端末に送信するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から

前記第１の暗号鍵を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第２の暗号鍵を生成し、前記記憶部に記憶された第１の暗号データを、受信した第１の暗号鍵及び生成した第２の暗号鍵で暗号化し、第２の暗号データを生成するステップと、前記第２の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、前記第２の暗号鍵を前記譲渡側端末に送信するステップと、を前記コンピュータに実行させることを特徴とする。

【００２０】

請求項１１記載の本発明は、請求項１０記載の発明において、前記データが使用されるときは、前記譲受側端末から前記第２の暗号鍵を受信するステップと、前記記憶部に記憶された第２の暗号データを、受信した第２の暗号鍵で復号化し、前記データを生成するステップと、を前記コンピュータに実行させることを特徴とする。

【発明の効果】

【００２４】

本発明によれば、バーナム暗号を用いて暗号化する端末を複数備え、データのアクセス権限を譲渡する譲渡側端末において第１の暗号鍵で暗号化した第１の暗号データを譲受側端末において第２の暗号鍵で暗号化して第２の暗号データとし、さらに、譲渡側端末において第２の暗号データを第１の暗号鍵で暗号化した第３の暗号データを生成し、該第３の暗号データを譲受側端末に譲渡するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【００２５】

また、本発明によれば、バーナム暗号を用いて暗号化するアクセス権管理装置及び複数の端末を備え、アクセス権管理装置は、譲渡側端末のための第１の暗号鍵でデータを暗号化して、第１の暗号データを管理し、第１の暗号鍵は譲渡側端末で管理する。そして、データのアクセス権限が譲渡された場合には、アクセス権管理装置は、譲渡側端末のための第１の暗号鍵及び譲受側端末のための第２の暗号鍵を用いて第１の暗号データをさらに暗号化し、第２の暗号データを管理し、第２の暗号鍵は譲受側端末で管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【発明を実施するための最良の形態】

【００２８】

以下、本発明の実施の形態を図面を用いて説明する。

【００２９】

＜第１の実施の形態＞

図１は、本発明の第１の実施の形態に係るアクセス権管理システム１０の概略構成を示す図である。

【００３０】

図１に示すように、アクセス権管理システム１０は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）１ｉ（ｉ＝ａ，ｂ）をインターネット等の通信ネットワーク２を介して接続しており、各端末１ｉが相互に通信可能となっている。尚、本実施の形態においては、１対の端末のうち、端末１ａのユーザを甲（データ譲渡側）、端末１ｂのユーザを乙（データ譲受側）として、以下、説明する。

【００３１】

各端末１ｉは、バーナム暗号を利用してデータの暗号及び復号を行う装置であり、記憶部１１、データ暗号部１２、データ復号部１３、及び通信部１４を備えている。

【００３２】

ここで、バーナム暗号は、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演算（XOR）をし、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演算（XOR）をする暗号方式をいう。以下、排他的論理和演算（XOR）は、「＊」なる演算記号で表すこ

とにするが、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。

【００３３】

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。

【００３４】

また、a*a=0,a*0=0*a=aが成り立つ。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」からなるビット列を表す。

【００３５】

記憶部１１には、ユーザがアクセスを制限したいデータＳ、データＳを暗号するための暗号鍵（復号鍵）Ｒ、暗号化されたデータなどを記憶するようになっている。尚、図１においては、甲の暗号鍵をＲ、乙の暗号鍵をＲ’と表記して、両者を区別している。また、データＳと暗号鍵Ｒ及び暗号鍵Ｒ’のデータ長は同一である。

【００３６】

データ暗号部１２は、データＳを暗号鍵Ｒで暗号化し、暗号データＡを生成するようになっており、データ復号部１３は、暗号データＡを暗号鍵Ｒで復号し、データＳを生成するようになっている。即ち、暗号化に際しては、Ａ＝Ｓ*Ｒ、復号化に際しては、Ｓ＝Ａ*Ｒであり、データＳと暗号鍵Ｒとの排他的論理和演算により生成された暗号データＡを、さらに、暗号鍵Ｒと排他的論理和演算を行うことにより、データＳが復元されるものである。

【００３７】

また、データ暗号部１２は、後述するように、データＳを暗号化するだけでなく、他の端末１ｉから送られた暗号データＡ’に関しても、自己の暗号鍵Ｒでさらに暗号化するようになっている。また、データ復号部１３は、後述するように、他の端末１ｉから送られた暗号データＡ’に関しても、自己の暗号鍵Ｒで復号できるようになっており、これにより、アクセス制限されたデータの譲渡が可能となっている。

【００３８】

通信部１４は、端末１ｉ間における暗号データの送受信を行うようになっている。

【００３９】

ここで、上述した端末１ｉは、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。

【００４０】

このうち、データ暗号部１２、データ復号部１３、及び通信部１４は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、記憶部１１は、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【００４１】

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。

【００４２】

次に、本実施の形態に係るアクセス権管理システム１０の動作を図２を用いて説明する

。ここで、図２は、甲が暗号化したデータのデータ権限を乙に譲渡するときの端末１ａ及び端末１ｂ間のデータのやりとりを示すシーケンス図である。

【００４３】

まず、端末１ａにおいて、甲の暗号鍵Ｒを用いてデータＳを暗号化した暗号化データＡを生成し、記憶部１１に保管する（ステップＳ１０，Ｓ２０）。ここで、Ａ＝Ｓ*Ｒである。

【００４４】

次に、データＳのアクセス権限を譲渡するときは、譲渡端末１ａから端末１ｂに暗号データＡを送信する（ステップＳ３０）。

【００４５】

端末１ｂにおいては、暗号データＡを受信すると、さらに、乙の暗号鍵Ｒ’を用いて暗号データＡを暗号化し、暗号データＡ’を生成する（ステップＳ４０）。即ち、Ａ’＝Ａ*Ｒ’である。

【００４６】

次に、端末１ｂから端末１ａに暗号データＡ’を送信する（ステップＳ５０）。

【００４７】

端末１ａにおいては、暗号データＡ’を受信すると、さらに、甲の暗号鍵Ｒを用いて暗号データＡ’を暗号化し、暗号データＡ”を生成する（ステップＳ６０）。即ち、Ａ”＝Ａ’*Ｒである。

【００４８】

次に、端末１ａから端末１ｂに暗号データＡ”を、アクセス権限が譲渡されたデータとして送信する（ステップＳ７０）。

【００４９】

端末１ｂにおいては、受信した暗号データＡ”を記憶部１１にアクセス権限が譲渡されたデータとして記憶する（ステップＳ８０）。

【００５０】

次に、端末１ｂで暗号データＡ”を復号するときは、乙の暗号鍵Ｒ’を用いて、復号されたデータＳを生成する（ステップＳ９０）。これは、

Ａ”＝Ａ’*Ｒ
＝（Ａ*Ｒ’）*Ｒ
＝（（Ｓ*Ｒ）*Ｒ’）*Ｒ
＝Ｓ*Ｒ*Ｒ’*Ｒ
＝Ｓ*（Ｒ*Ｒ）*Ｒ’
＝Ｓ*０*Ｒ’
＝Ｓ*Ｒ’

であるから、受信した暗号データＡ”と暗号鍵Ｒ’の排他的論理和により、

Ａ”*Ｒ’＝（Ｓ*Ｒ’）*Ｒ’＝Ｓ

となることによる。尚、Ａ”＝Ｓ*Ｒ’より、暗号データＡ”は、甲の暗号鍵Ｒでは復号することができない。

【００５１】

従って、本実施の形態に係るアクセス権管理システム１０によれば、バーナム暗号を用いて暗号化する端末１ａ及び１ｂを備え、データのアクセス権限を譲渡する譲渡側の端末１ａにおいて暗号鍵Ｒで暗号化した暗号データＡを譲受側の端末１ｂにおいて暗号鍵Ｒ’で暗号化して暗号化データＡ’とし、さらに、端末１ａにおいて暗号化データＡ’を暗号鍵Ｒで暗号化された暗号データＡ”を生成し、該暗号データＡ”を端末１ｂに譲渡するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【００５２】

＜第２の実施の形態＞

図３は、本発明の第２の実施の形態に係るアクセス権管理システム２０の概略構成を示す図である。

【００５３】

図３に示すように、アクセス権管理システム２０は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）３ｉ（ｉ＝ａ，ｂ）と、アクセス権管理サーバ４を通信ネットワーク２を介して接続しており、各端末３ｉ及びアクセス権管理サーバ４が相互に通信可能となっている。尚、本実施の形態においては、１対の端末のうち、端末３ａのユーザを甲（データ権限譲渡側）、端末３ｂのユーザを乙（データ権限譲受側）として、以下、説明する。

【００５４】

各端末３ｉは、アクセスを制限したいデータＳを保持する端末であり、記憶部３１、及び通信部３２を備えている。

【００５５】

記憶部３１には、アクセスを制限したいデータＳ、アクセス権管理サーバ４から送信される暗号鍵Ｒ（データ権限を有するユーザのデータ暗号化の際に用いられた暗号鍵）などを記憶するようになっている。尚、図１においては、甲の暗号鍵をＲ、乙の暗号鍵をＲ’と表記して、両者を区別している。また、データＳと暗号鍵Ｒ及び暗号鍵Ｒ’のデータ長は同一である。

【００５６】

通信部３２は、端末３ｉとアクセス権管理サーバ４間のデータの送受信を行うようになっている。

【００５７】

アクセス権管理サーバ４は、バーナム暗号を利用してデータの暗号及び復号を行う装置であり、暗号データ記憶部４１、鍵生成部４２、データ暗号部４３、データ復号部４４、及び通信部４５を備えている。

【００５８】

暗号データ記憶部４１は、データ暗号部４３で暗号化された暗号データＡ（データＳのアクセス権限を甲が有する場合の甲の暗号データ），Ａ”（ データＳのアクセス権限を乙が有する場合の乙の暗号データ）を記憶するようになっている。

【００５９】

鍵生成部４２は、データ暗号部４３で暗号化に用いる暗号鍵（復号鍵）Ｒ，Ｒ’を生成するようになっている。

【００６０】

データ暗号部４３は、端末３ａから送信（送付）されたデータＳを、甲の暗号鍵Ｒを用いて暗号化し、暗号データＡを生成するようになっている。また、データＳの権限を甲から乙に譲渡したときは、甲の暗号鍵Ｒ及び乙の暗号鍵Ｒ’を用いて、暗号データＡをさらに暗号化し、暗号化データＡ”を生成するようになっている。尚、暗号化に用いた暗号鍵Ｒ及びＲ’は、それぞれ端末３ａ及び３ｂに通信部４５を介して送信される。

【００６１】

データ復号部４４は、データ権限を譲渡されたユーザ、即ち、乙から暗号鍵Ｒ’が送信されると、該暗号鍵Ｒ’を用いて暗号化データＡ”を復号し、データＳを通信部４５を介して、端末３ｂに送信（送付）するようになっている。

【００６２】

通信部４５は、端末１ｉとアクセス権管理サーバ４間のデータの送受信を行うようになっている。

【００６３】

ここで、上述した端末３ｉ及びアクセス権管理サーバ４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。

【００６４】

このうち、端末３ｉの通信部３２、アクセス権管理サーバ４の鍵生成部４２、データ暗号部４３、データ復号部４４、及び通信部４５は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、端末３ｉの記憶部３１、及びアクセス権管理サーバ４の暗号データ記憶部４１は、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【００６５】

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。

【００６６】

次に、本実施の形態に係るアクセス権管理システム２０の動作を図４を用いて説明する。ここで、図４は、データＳのデータ権限を甲から乙に譲渡するときの端末３ａ，端末３ｂとアクセス権管理サーバ４間のデータのやりとりを示すシーケンス図である。

【００６７】

まず、甲がデータＳのアクセス権限を有する場合には、データＳを甲の端末３ａからアクセス管理サーバ４に送信する（ステップＳ１１０）。尚、データＳの送信に際しては、通信内容の漏洩を防止するセキュアな通信ネットワーク２ａ（例えば、インターネット網などのオープンな通信ネットワーク２ｂではなく、ＬＡＮ、ＩＰ－ＶＰＮ、専用線、電話回線など）を用いる、また、通信ネットワーク２ａを介した通信ではなく、例えば、郵便などの送付手段を用いてもよい。

【００６８】

アクセス権管理サーバ４は、端末３ａからデータＳを受け取ると、甲の暗号鍵Ｒを生成し、暗号鍵Ｒを用いて暗号データＡ＝Ｓ*Ｒを生成する（ステップＳ１２０，Ｓ１３０）。そして、暗号データＡを暗号データ記憶部４１に記憶させるとともに、暗号鍵Ｒを通信ネットワーク２を介して甲の端末３ａに送信する（ステップＳ１４０，Ｓ１５０）。

【００６９】

端末３ａは、アクセス権管理サーバ４から暗号鍵Ｒを受け取ると、暗号鍵Ｒを記憶部３１に記憶させる（ステップＳ１６０）。

【００７０】

以上の動作により、甲のデータＳに対するアクセス権限は、アクセス権管理サーバ４で管理されることになる。

【００７１】

次に、甲がデータＳのアクセス権限を乙に譲渡する場合には、甲から乙へのデータのアクセス権譲渡の要求、及び暗号鍵Ｒを、甲の端末３ａから通信ネットワーク２を介してアクセス権管理サーバ４に送信する（ステップＳ２１０）。

【００７２】

アクセス権管理サーバ４は、端末３ａから甲から乙へのアクセス権譲渡要求、及び暗号鍵Ｒを受け取ると、乙の暗号鍵Ｒ’を生成し、暗号データ記憶部４１に記憶された暗号データＡから暗号鍵Ｒ及びＲ’を用いて暗号データＡ”＝Ａ*Ｒ*Ｒ”を生成する（ステップＳ２２０，Ｓ２３０）。そして、暗号データＡ”を暗号データ記憶部４１に記憶させるとともに、暗号鍵Ｒ’を通信ネットワーク２を介して乙の端末３ｂに送信する（ステップＳ２４０，Ｓ２５０）。

【００７３】

端末３ｂは、アクセス権管理サーバ４から暗号鍵Ｒ’を受け取ると、暗号鍵Ｒ’を記憶部３１に記憶させる（ステップＳ２６０）。

【００７４】

以上の動作により、データＳに対するアクセス権限は、甲から乙に譲渡されたことになる。

【００７５】

次に、乙がデータＳを使用する場合には、データＳの使用要求、及び暗号鍵Ｒ’を端末３ｂから通信ネットワーク２を介してアクセス管理サーバ４に送信する（ステップＳ３１０）。

【００７６】

アクセス権管理サーバ４は、端末３ｂから甲データＳの使用要求、及び暗号鍵Ｒ’を受け取ると、暗号データ記憶部４１に記憶された暗号データＡ”を暗号鍵Ｒ’を用いて復号し、データＳを生成する（ステップＳ３２０）。これは、

Ａ”＝Ａ*Ｒ*Ｒ’
　＝（Ｓ*Ｒ）*Ｒ*Ｒ’
　＝Ｓ*Ｒ*Ｒ*Ｒ’
　＝Ｓ*（Ｒ*Ｒ）*Ｒ’
　＝Ｓ*０*Ｒ’
　＝Ｓ*Ｒ’

であるから、

Ａ”*Ｒ’＝（Ｓ*Ｒ’）*Ｒ’
　　＝Ｓ*Ｒ’*Ｒ’
　　＝Ｓ

となり、データＳが得られるものである。そして、復号されたデータＳをセキュアな通信ネットワーク２ａ又は送付手段を介して乙の端末３ｂに送信する（ステップＳ３３０）。

【００７７】

端末３ｂは、アクセス管理サーバ４からデータＳを受け取ると、データＳを記憶部３１に記憶させる（ステップＳ３４０）。これにより、乙はデータＳを端末３ｂで使用することができる。

【００７８】

従って、本実施の形態に係るアクセス権管理システム２０によれば、バーナム暗号を用いて暗号化するアクセス権管理サーバ４、並びに端末３ａ及び３ｂを備え、アクセス権管理サーバ４は、データのアクセス権限を譲渡する譲渡側の端末３ａのユーザ甲のデータＳを甲の暗号鍵Ｒで暗号化し、暗号データＡを管理し、甲の暗号鍵は端末３ａが管理する。そして、甲から譲受側の端末３ｂのユーザ乙にデータＳのアクセス権限が譲渡された場合には、アクセス権管理サーバ４は、甲の暗号鍵Ｒ及び乙の暗号鍵Ｒ’を用いて暗号データＡをさらに暗号化し、暗号データＡ”を管理し、乙の暗号鍵は端末３ｂが管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【００７９】

＜第３の実施の形態＞

（システム構成）

図５は、本発明の第３の実施の形態に係るアクセス権管理システム３０の概略構成を示す図である。

【００８０】

図５に示すように、アクセス権管理システム３０は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）３ｉ（ｉ＝ａ，ｂ）と、アクセス権管理サーバ５を通信ネットワーク２を介して接続しており、各端末３ｉ及びアクセス権管理サーバ５が相互に通信可能となっている。また、アクセス権管理サーバ５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）６ａ，６ｂと接続されている。尚、本実施の形態においては、１対の端末のうち、端末３ａのユーザを甲（データ権限譲渡側）、端末３ｂのユーザを乙（データ権限譲受側）として、以下、説明する。

【００８１】
各端末３ｉは、アクセスを制限したいデータＳを保持する端末であり、記憶部３１、及び通信部３２を備えている。
【００８２】
記憶部３１には、アクセスを制限したいデータＳ、アクセス権管理サーバ５から送信される分割データD(3)などを記憶するようになっている。即ち、第２の実施の形態では暗号鍵Ｒが送信されたが、本実施の形態においては、分割データD(3)が送信される点が異なっている。尚、図１においては、甲の分割データをD(3)、乙の甲の分割データをD’(3)をと表記して、両者を区別している。
【００８３】
通信部３２は、端末３ｉとアクセス権管理サーバ５間のデータの送受信を行うようになっている。
【００８４】
アクセス権管理サーバ５は、甲が権限を有するデータＳを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）を用いて複数のデータに分割し、該分割データを保管サーバ６ａ，６ｂおよび端末３ａにそれぞれ保管させるようになっている。尚、図１では、アクセス権管理サーバ５は、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６ａ，６ｂおよび端末３ａに保管するようになっている。
【００８５】
また、アクセス権管理サーバ５は、データＳのデータ権限を甲から乙に譲渡する場合には、上述した秘密分散法Ａを用いて、分割データD(1)，D(2)，D(3)から再分割データD’(1)，D’(2)，D’(3)を生成し、それぞれを複数の保管サーバ６ａ，６ｂおよび端末３ｂに保管するようになっている。
【００８６】
尚、本実施の形態においては、データＳを３分割して保管する場合を例に説明するが、本発明はデータ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３ｉで保管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。また、本実施の形態においては、分割データD(1),D(2)（再分割データD’(1),D’(2)）を保管サーバ６、分割データD(3)（再分割データD’(3)）を端末３ｉに割り当てたが、どの分割データをどの保管サーバ６および端末３ｉに割り当て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（再分割データ）の一部を保管サーバ６ａ，６ｂで保管するようにしているが、アクセス権管理サーバ５内で管理してもよいものである。
【００８７】
アクセス管理サーバ５は、詳しくは、データＳから複数の分割データＤを生成するために使用される乱数Ｒおよび再分割データＤ’を生成するために使用される乱数Ｒ’を発生させる乱数生成部５１、データＳから秘密分散法Ａを用いて複数の分割データＤに分割する分割データ生成部５２、データ権限を甲から乙に譲渡するときに、秘密分散法Ａを用いて複数の分割データＤから複数の再分割データＤ’を生成する再分割データ生成部５３、複数の再分割データＤ’から秘密分散法Ａを用いてデータＳを復元するデータ復元部５４、並びに端末３ｉ、及び保管サーバ６ａ,６ｂとそれぞれデータの送受信を行う通信部５５を具備する構成となっている。
【００８８】
ここで、上述した端末３ｉ、アクセス権管理サーバ５及び保管サーバ６ａ，６ｂ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。
【００８９】

このうち、端末３ｉの通信部３２、アクセス権管理サーバ５の乱数生成部５１、分割データ生成部５２、再分割データ生成部５３、データ復元部５４、及び通信部５５は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、端末３ｉの記憶部３１、及び保管サーバ６ａ，６ｂは、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【００９０】

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。

【００９１】

（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。

【００９２】

本実施形態における元データ（データ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ことにより本実施形態を適用することができる。

【００９３】

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５１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。

【００９４】

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～n)およびj(=1～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。

【００９５】

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。

【００９６】

元データS=(n-1)個の元部分データS(j)

=S(1),S(2),…,S(n-1)

乱数R=(n-1)個の乱数部分データR(j)

=R(1),R(2),…,R(n-1)

n個の分割データD(i)=D(1),D(2),…,D(n)
各分割部分データD(i,j)
=D(1,1),D(1,2),…,D(1,n-1)
D(2,1),D(2,2),…,D(2,n-1)
… … …
D(n,1),D(n,2),…,D(n,n-1)
(i=1～n), (j=1～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となる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。

【００９７】

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６乃至１０、および図１２に示す記号の定義について説明する。

【００９８】

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

【００９９】

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

【０１００】

このときQ(j,i,k)を下記のように定義する。

【０１０１】

c(j,i,k)=1 のとき Q(j,i,k)=R((n-1)×m+k)
c(j,i,k)=0 のとき Q(j,i,k)=0

ただし、mはm≧0の整数を表す。

【０１０２】

（３）U[n,n]とは、n×n行列であって、i行j列の値をu(i,j)で表すと、
i+j<=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】

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

【０１０３】

（４）P[n,n]とは、n×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】

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

【０１０４】
（５）A,Bをn×n行列とすると、A×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。
【０１０５】
（６）Aをn×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。
【０１０６】
（７）単位行列E[n,n]とは、n×n行列であって、i行j列の値をe(i,j)で表すと、
i=j　　のとき e(i,j)=1
上記以外のとき 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×n行列とすると
A×E=E×A=A
となる性質がある。
【数３】

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

【０１０７】
次に、図６に示すフローチャートおよび図７および図８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、アクセス権管理サーバ５の分割データ生成部５２の機能を説明するものである。
【０１０８】
まず、元データSをアクセス権管理サーバ５に与える（図６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。
【０１０９】
次に、アクセス権管理サーバ５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に従ってアクセス権管理サーバ５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。

【０１１０】

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３からアクセス権管理サーバ５に対して指定してもよいし、またはアクセス権管理サーバ５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を割り切れることができる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区分けされた場合の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。

【０１１１】

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×(分割数n-1)=8×2の整数倍の元データSに対して有効なものである。

【０１１２】

次に、ステップＳ２０９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×(分割数n-1)=8×2=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。

【０１１３】

次に、元データSの8×2×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Ｓ２１１）。これは、このステップＳ２１１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×(分割数n-1)=8×2=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Ｓ２１１以降の分割処理を１回行うと、後述するステップＳ２１９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Ｓ２１１からステップＳ２２１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8×2×m+1ビット目は、8×2×0+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Ｓ２１３に進む。

【０１１４】

ステップＳ２１３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×(2×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区分けした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。

【０１１５】

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５１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区分けした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Ｓ２１５）。

【０１１６】

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Ｓ２１７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Ｓ２１７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。

【０１１７】

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)
=「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Ｓ２１７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８に示す表に記載されているものとなる。図８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８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。

【０１１８】

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Ｓ２１９）、ステップＳ２１１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Ｓ２１１からステップＳ２２１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６及び端末３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。

【０１１９】

ここで、上述した図６のフローチャートのステップＳ２１７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。

【０１２０】

まず、整数倍を意味する変数m=0の場合には、ステップＳ２１７に示す定義式から各分割データD(i)=D(1)～D(3)の各々を構成する各分割部分データD(i,2×m+j)=D(i,j)(i=1～3,j=1～2)は、次のようになる。

【０１２１】

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)

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。

【０１２２】

これはc(j,i,k)を2×2行列であるU[2,2]×(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。

【０１２３】

c(j,i,k)=1 のとき Q(j,i,k)=R(k)

c(j,i,k)=0 のとき Q(j,i,k)=0

ここで、

j=1のときは

【数４】

$$U[2,2]\times(P[2,2])^{(j-1)} = U[2,2]\times(P[2,2])^{0}$$

$$= U[2,2]\times E[2,2]$$

$$= U[2,2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

【０１２４】

j=2のときは

【数５】

$$U[2,2]\times(P[2,2])^{(j-1)} = U[2,2]\times(P[2,2])^{1}$$

$$= U[2,2]\times P[2,2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

【０１２５】

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。

【０１２６】

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)

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７にも図示されている。

【０１２７】

図７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。

【０１２８】

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。

【０１２９】

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８にまとめて示されている。

【０１３０】

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。

【０１３１】

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00110101となるので、D(3)は10110001 00110101である。

【０１３２】

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こと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。

【０１３３】

次に、図７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。これは、分割データから元データを復元できることを示すものである。

【０１３４】

まず、アクセス権管理サーバ５に元データSの復元を要求する。アクセス権管理サーバ５は、保管サーバ６および端末３から分割データD(1),D(2),D(3)を取得し、この取得した分割データD(1),D(2),D(3)から次に示すように元データSを復元する。

【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】

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

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。

【０１３７】

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。

【０１３８】

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

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。

【０１３９】

一般に、jを奇数として、

D(2,j)*D(3,j)=(S(j)*R(j))*R(j)
=S(j)*(R(j)*R(j))
=S(j)*0
=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。

【０１４０】

また、一般に、jを奇数として、

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)

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。

【０１４１】

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。

【０１４２】

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)

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。

【０１４３】

また同様に、

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)

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。

【０１４４】

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。

【０１４５】

また、一般に、jを奇数として、

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)

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。

【０１４６】

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。

【０１４７】

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。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。

【０１４８】

また同様に、

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)

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。

【０１４９】

このR(1),R(2)を使用してS(1),S(2)を求める。

【０１５０】

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

【０１５１】

また同様に、

D(2,2)*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(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。

【０１５２】

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

であるからD(1,j)*D(2,j)を計算すればR(j+1)が求まる。

【０１５３】

また同様に、

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)

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。

【０１５４】

このR(j),R(j+1)を使用してS(j),S(j+1)を求める。

【０１５５】

D(2,j)*R(j)=(S(j)*R(j))*R(j)

=S(j)*(R(j)*R(j))
=S(j)*0
=S(j)

であるからD(2,j)*R(j)を計算すればS(j)が求まる。

【０１５６】

また同様に、

D(2,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)

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。

【０１５７】

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。即ち、端末３において、仮に分割データを紛失したとしても、保管サーバ６に保管された他の分割データから元データを復元ですることができる。

【０１５８】

尚、本実施の形態に係るアクセス権管理サーバ５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。

【０１５９】

次に、図９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。

【０１６０】

まず、元データSをアクセス権管理サーバ５に与える（ステップＳ４０１）。また、アクセス権管理サーバ５に、分割数n(n≧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×(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）。

【０１６１】

次に、元データSのb×(n-1)×m+1ビット目からb×(n-1)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。

【０１６２】

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×((n-1)×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)×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),…S(n-1)が生成される。

【０１６３】

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)×m+j)に乱数生成部５１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),…R(n-1)が生成される（ステップＳ４１５）。

【０１６４】

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

)×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。

【０１６５】

分割データD
=n個の分割データD(i)=D(1),D(2),…D(n)
第１の分割データD(1)
=n-1個の分割部分データD(1,j)=D(1,1),D(1,2),…D(1,n-1)
第２の分割データD(2)
=n-1個の分割部分データD(2,j)=D(2,1),D(2,2),…D(2,n-1)
… … …
… … …
第nの分割データD(n)
=n-1個の分割部分データD(n,j)=D(n,1),D(n,2),…D(n,n-1)

このように変数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Ｓ４１９）、ステップＳ４１１に戻り、変数m=1に該当する元データSのb×(n-1)ビット以降について同様の分割処理を行う。最後にステップＳ４１１の判定の結果、元データSにデータがなくなった場合、ステップＳ４１１からステップＳ４２１に進み、上述したように生成した分割データD(1), …,D(n)を保管サーバ６および端末３にそれぞれ保存して、分割処理を終了する。

【０１６６】

さて、上述した実施形態においては、ここの分割データのみから、それを構成する部分データ間の演算を行うことによって乱数成分が失われる場合がある。即ち、例えば３分割の場合、各分割部分データは次のように定義される。

【０１６７】

D(1,1)=S(1)*R(1)*R(2), D(1,2)=S(2)*R(1)*R(2), …
D(2,1)=S(1)*R(1), D(2,2)=S(2)*R(2), …
D(3,1)=R(1), D(3,2)=R(2), …

D(1)について見ると、例えば、D(1,1)、D(1,2)が取得できると、

D(1,1)*D(1,2)=(S(1)*R(1)*R(2))*(S(2)*R(1)*R(2))
=S(1)*S(2)*((R(1)*R(1))*((R(2)*R(2))
=S(1)*S(2)*0*0
=S(1)*S(2)

となる。一般にはD(1,j)*D(1,j+1)=S(j)*S(j+1)である。ここでｊはｊ＝２×ｍ＋１、ｍはｍ≧０の任意の整数である。

【０１６８】

D(1,1)、D(1,2)は、上記の定義より、元データと乱数の演算により生成されたものであり、D(1,1)、D(1,2)それぞれを見ても元データの内容は分からないが、D(1,1)＊D(1,2)の演算を行うことによりS(1)*S(2)が算出される。これは元データそのものではないが、乱数成分を含んでいない。

【０１６９】

このように乱数成分が失われると、個々の元部分データについて、例えばS(2)の一部が既知である場合にはS(1)の一部が復元可能となるので、安全ではないと考えられる。例えば、元データが標準化されたデータフォーマットに従ったデータであって、S(2)がそのデータフォーマット中のヘッダ情報やパディング（例えば、データ領域の一部を０で埋めたもの）などを含む部分であった場合には、これらのデータフォーマット固有のキーワードや固定文字列などを含むため、その内容は予測され得る。また、S(2)のうち既知の部分とS(1)*S(2)の値から、S(1)の一部が復元可能である。

【０１７０】

この問題を解決する方法は以下の通りである。図１０におけるD(1,j+1)とD(2,j+1)は、図８におけるD(1,j+1)とD(2,j+1)を入れ替えたものである。ここでｊはｊ＝２×ｍ＋１、ｍはｍ≧０の任意の整数である。

【０１７１】
この場合、個々の分割データのみでは、それを構成する分割部分データ間で演算を行っても乱数成分が失われない。これは、図１０より

D(1,j)*D(1,j+1)=(S(j)*R(j)*R(j+1))*(S(j+1)*R(j+1))
=S(j)*S(j+1)*R(j)*((R(j+1)*R(j+1))
=S(j)*S(j+1)*R(j)*0
=S(j)*S(j+1)*R(j)
D(2,j)*D(2,j+1)=(S(j)*R(j))*(S(j+1)*R(j)*R(j+1))
=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)
D(3,j)*D(3,j+1)=R(j)*R(j+1)

となるからである。
【０１７２】
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１０におけるD(1)、D(2)は、図８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。
【０１７３】
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、アクセス権管理サーバ５の再分割データ生成部５３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。
【０１７４】
図１１は、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、乱数生成部５１で再分割の際に用いる乱数R’を発生させる（ステップＳ６０３）。
【０１７５】
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Ｓ６０５）。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、分割データから旧乱数であるRを消去して、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Ｓ６０７，Ｓ６０９）。
【０１７６】
図１２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。
【０１７７】
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。
【０１７８】
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)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）。
【０１７９】

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)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）。

【０１８０】

更に第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)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）。

【０１８１】

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。

【０１８２】

まず、第１の分割データD’(1)に対しては、図１２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）。

【０１８３】

また、第２の分割データD’(2)に対しては、図１２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）。

【０１８４】

また、第３の分割データD’(3)に対しては、図１２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）。

【０１８５】

次に、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。

【０１８６】

まず、上述の第１の分割データD’(1)に対しては、図１２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）。

【０１８７】

また、上述の第２の分割データD’(2)に対しては、図１２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)*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）。

【０１８８】

また、上述の第３の分割データD’(3)に対しては、図１２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)*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）。

【０１８９】

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。

【０１９０】

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。

【０１９１】

次に、図１２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、アクセス権管理サーバ５の元データ復元部５４の機能を説明するものである。

【０１９２】

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。

【０１９３】

D’(2,1)*D’(3,1)=(S(1)*R’(1))*R’(1)
=S(1)*(R’(1)*R’(1))
=S(1)*0
=S(1)

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。

【０１９４】

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)

一般に、jを奇数として、

D’(2,j)*D’(3,j)=(S(j)*R’(j))* R’(j)
=S(j)*(R’(j)*R’(j))
=S(j)*0
=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。

【０１９５】

また、一般に、jを奇数として、

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)

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。

【０１９６】

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。

【０１９７】

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)

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。

【０１９８】

また同様に、

D’(1,2)* D’(3,2)=(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)* D’(3,2)を計算すれば、S(2)が求まる。
【０１９９】
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。
【０２００】
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。
【０２０１】
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。
【０２０２】
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。
【０２０３】
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。
【０２０４】
このR’(1), R’(2)を使用してS(1),S(2)を求める。
【０２０５】
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。
【０２０６】
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。
【０２０７】
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))
=(S(j)*S(j))*(R’(j)*R’(j)) *R’(j+1)

=0*0*R’(j+1)
= R’(j+1)
であるからD’(1,j)*D’(2,j)を計算すればR’(j+1)が求まる。
【０２０８】
また同様に、
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)
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。
【０２０９】
このR’(j), R’(j+1)を使用してS(j),S(j+1)を求める。
【０２１０】
D’(2,j)*R’(j)=(S(j)* R’(j))* R’(j)
=S(j)*(R’(j)*R’(j))
=S(j)*0
=S(j)
であるからD’(2,j)*R’(j)を計算すればS(j)が求まる。
【０２１１】
また同様に、
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)
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。
【０２１２】
以上、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。
【０２１３】
また、このデータ再分割方法においては、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。
【０２１４】
（動作）
次に、本実施の形態に係るアクセス権管理システム３０の動作を図１３を用いて説明する。ここで、図１３は、データＳのデータ権限を甲から乙に譲渡するときの端末３ａ，端末３ｂとアクセス権管理サーバ５間のデータのやりとりを示すシーケンス図である。
【０２１５】
まず、甲がデータＳのアクセス権限を有する場合には、データＳを甲の端末３ａからアクセス管理サーバ５に送信する（ステップＳ４１０）。尚、データＳの送信に際しては、通信内容の漏洩を防止するセキュアな通信ネットワーク２ａ（例えば、インターネット網などのオープンな通信ネットワーク２ｂではなく、ＬＡＮ、ＩＰ－ＶＰＮ、専用線、電話回線など）を用いる、また、通信ネットワーク２ａを介した通信ではなく、例えば、郵便などの送付手段を用いてもよい。
【０２１６】
アクセス権管理サーバ５は、端末３ａからデータＳを受け取ると、甲の乱数Ｒを生成し、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Ｓ４２０，Ｓ４３０）。例えば、具体的には、
D(1)＝（S(1)*R(1)*R(2)） ‖ （S(2)*R(2)）

D(2)＝（S(1)*R(1)）‖（S(2)* R(1)*R(2)）
D(3)＝　R(1)‖R(2)
ただし、‖は、ビット列とビット列との結合を意味する。
【０２１７】
次に、アクセス権管理サーバ５は、分割データD(1),D(2)を保管サーバ６ａ，６ｂにそれぞれ保管するとともに、分割データD(3)を通信ネットワーク２を介して甲の端末３ａに送信する（ステップＳ４４０，Ｓ４５０）。尚、分割データD(3)は、上述したように、D(3)＝R(1)‖R(2)であるため、分割データD(3)の送信は、乱数Ｒの送信と同じことである。
【０２１８】
端末３ａは、アクセス権管理サーバ５から分割データD(3)を受け取ると、分割データD(3)を記憶部３１に記憶させる（ステップＳ４６０）。
【０２１９】
以上の動作により、甲のデータＳに対するアクセス権限は、アクセス権管理サーバ５で管理されることになる。
【０２２０】
次に、甲がデータＳのアクセス権限を乙に譲渡する場合には、甲から乙へのデータのアクセス権譲渡の要求、及び分割データD(3)を、甲の端末３ａから通信ネットワーク２を介してアクセス権管理サーバ５に送信する（ステップＳ５１０）。
【０２２１】
アクセス権管理サーバ５は、端末３ａから甲から乙へのアクセス権譲渡要求、及び分割データD(3)を受け取ると、乙の乱数Ｒ’を生成し、分割データD(1),D(2),D(3)から秘密分散法Ａを用いて、新たに３つのデータ（再分割データ）D’(1),D’(2),D’(3)を生成する（ステップＳ５２０，Ｓ５３０）。例えば、具体的には、
D’(1)＝（S(1)*R’(1)*R’(2)）‖（S(2)*R’(2)）
D’(2)＝（S(1)*R’(1)）‖（S(2)* R’(1)*R’(2)）
D’(3)＝　R’(1)‖R’(2)
次に、アクセス権管理サーバ５は、再分割データD’(1),D’(2)を保管サーバ６ａ，６ｂにそれぞれ保管するとともに、再分割データD’(3)を通信ネットワーク２を介して乙の端末３ｂに送信する（ステップＳ５４０，Ｓ５５０）。尚、再分割データD’(3)は、上述したように、D’(3)＝R’(1)‖R’(2)であるため、分割データD’(3)の送信は、乱数Ｒ’の送信と同じことである。
【０２２２】
端末３ｂは、アクセス権管理サーバ５から再分割データD’(3)を受け取ると、再分割データD’(3)を記憶部３１に記憶させる（ステップＳ５６０）。
【０２２３】
以上の動作により、データＳに対するアクセス権限は、甲から乙に譲渡されたことになる。
【０２２４】
次に、乙がデータＳを使用する場合には、データＳの使用要求、及び再分割データD’(3)を端末３ｂから通信ネットワーク２を介してアクセス管理サーバ５に送信する（ステップＳ６１０）。
【０２２５】
アクセス権管理サーバ５は、端末３ｂからデータＳの使用要求、及び再分割データD’(3)を受け取ると、保管サーバ６ａ，６ｂに保管された再分割データD’(1)，D’(2)を取得し、これら再分割データD’(1)，D’(2)，D’(3)のうち、任意の２つから秘密分散法Ａを用いて、データＳを復号する（ステップＳ６２０）。
【０２２６】
次に、アクセス権管理サーバ５は、復号されたデータＳをセキュアな通信ネットワーク２ａ又は送付手段を介して乙の端末３ｂに送信する（ステップＳ６３０）。
【０２２７】

端末３ｂは、アクセス管理サーバ５からデータＳを受け取ると、データＳを記憶部３１に記憶させる（ステップＳ６４０）。これにより、乙はデータＳを端末３ｂで使用することができる。

【０２２８】

従って、本実施の形態に係るアクセス権管理システム３０によれば、秘密分散法Ａを用いて暗号化するアクセス権管理サーバ５、並びに端末３ａ及び３ｂを備え、アクセス権管理サーバ５は、データのアクセス権限を譲渡する譲渡側の端末３ａのユーザ甲のデータＳを甲の乱数Ｒを用いて秘密分散法Ａにより、分割データを生成し、該分割データの一部を端末３ａ、残りをアクセス権管理サーバ５で管理する。そして、甲から譲受側の端末３ｂのユーザ乙にデータＳのアクセス権限が譲渡された場合には、アクセス権管理サーバ５は、乙の乱数Ｒ’を用いて分割データから秘密分散法Ａにより再分割データを生成し、該再分割データの一部を端末３ｂ、残りをアクセス権管理サーバ５で管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【０２２９】

特に、本発明における秘密分散法Ａは、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データ分割方法であり、データ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、データ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、生成した分割データのうちの所定の個数の分割データからデータが復元することができ、また、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とともに、生成した再分割データのうちの所定の個数の再分割データからデータが復元することができるので、データを復元することなく、データを再分割することができる。

【０２３０】

これにより、ユーザのデータをよりセキュアに管理することができる。

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。

【図面の簡単な説明】

【０２３１】

【図１】本発明の第１の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

【図２】本発明の第１の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。

【図３】本発明の第２の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

【図４】本発明の第２の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。

【図５】本発明の第３の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

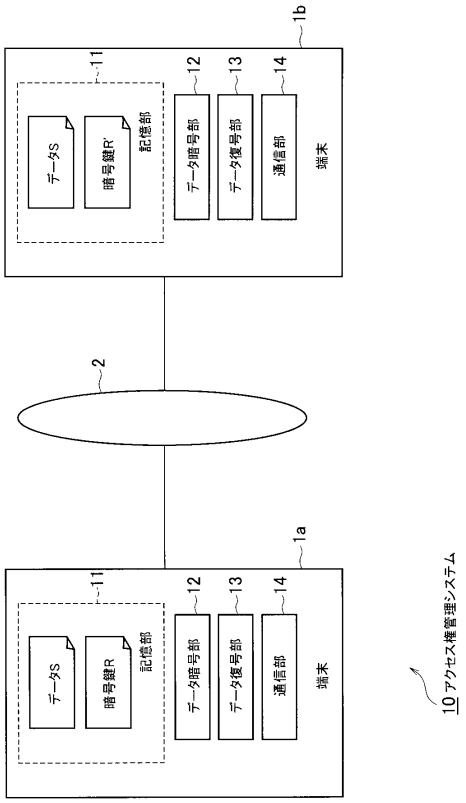
【図６】秘密分散法Ａの分割数ｎ＝３の場合の分割処理を示すフローチャートである。

【図７】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。

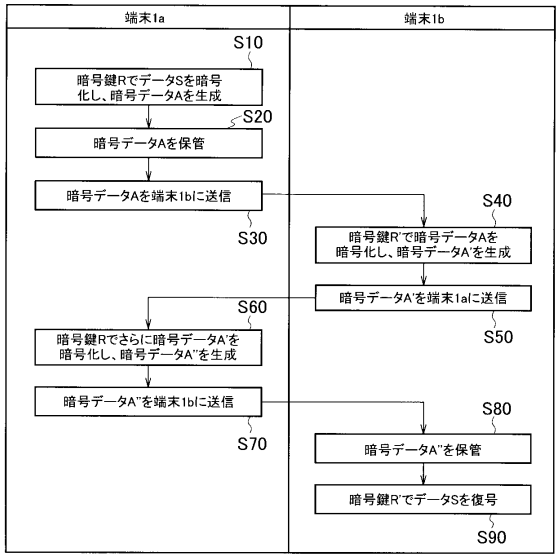
【図８】分割数n=3の場合の分割データ、分割部分データ、各分割部分データを生成する

定義式を示す表である。
【図９】秘密分散法Ａ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１０】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１１】秘密分散法Ａのデータ再分割処理を示すフローチャートである。
【図１２】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１３】本発明の第３の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。
【符号の説明】
【０２３２】
１ａ，１ｂ，３ａ，３ｂ…端末
２…通信ネットワーク
４，５…アクセス権管理サーバ
６ａ，６ｂ…保管サーバ
１０，２０，３０…アクセス権管理システム
１１，３１…記憶部
１２…データ暗号部
１３…データ復号部
１４，３２…通信部
４１…暗号データ記憶部
４２…鍵生成部
４３…データ暗号部
４４…データ復号部
４５…通信部

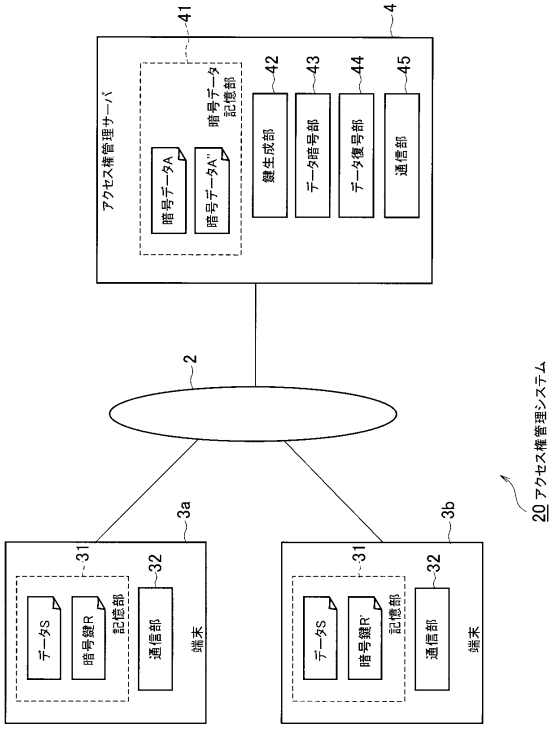
【図１】


1b
11
記憶部
データS
暗号鍵R'
12
データ暗号部
13
データ復号部
14
通信部
端末
2
1a
11
記憶部
データS
暗号鍵R
12
データ暗号部
13
データ復号部
14
通信部
端末
10 アクセス権管理システム

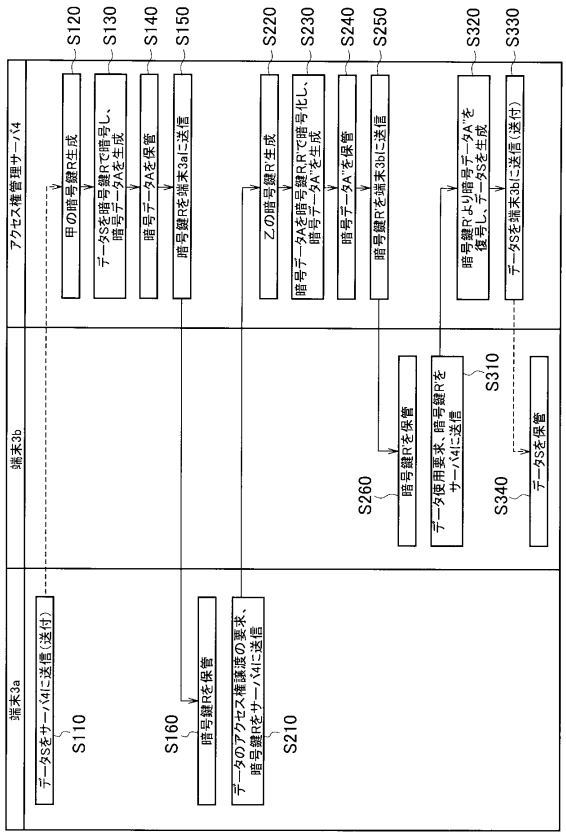
【図２】


端末1a
端末1b
S10
暗号鍵Rでデータsを暗号化し、暗号データAを生成
S20
暗号データAを保管
暗号データAを端末1blに送信
S30
S40
暗号鍵R'で暗号データAを暗号化し、暗号データA'を生成
暗号データA'を端末1alに送信
S50
S60
暗号鍵Rでさらに暗号データA'を暗号化し、暗号データA"を生成
暗号データA"を端末1blに送信
S70
S80
暗号データA"を保管
暗号鍵R'でデータSを復号
S90

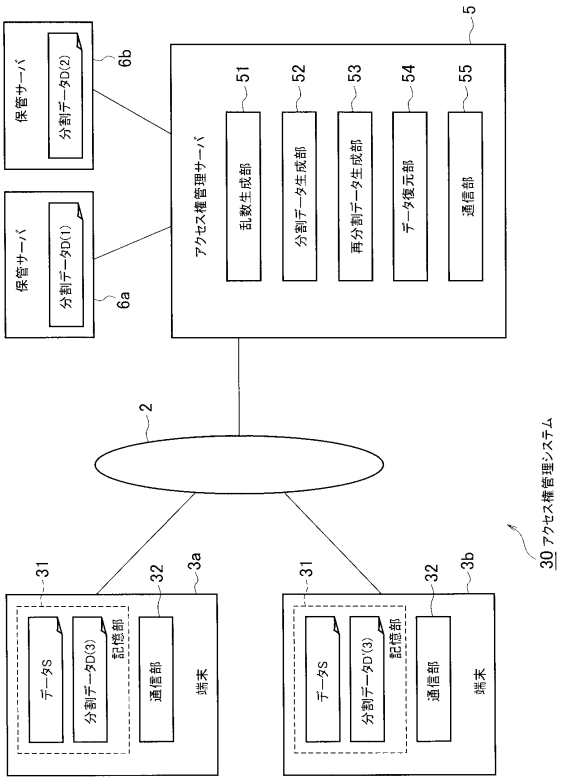
【図３】


41
アクセス権管理サーバ
暗号データ記憶部
暗号データA
暗号データA"
42
鍵生成部
43
データ暗号部
44
データ復号部
45
通信部
4
2
3a
31
記憶部
データS
暗号鍵R
32
通信部
端末
3b
31
記憶部
データS
暗号鍵R'
32
通信部
端末
20 アクセス権管理システム

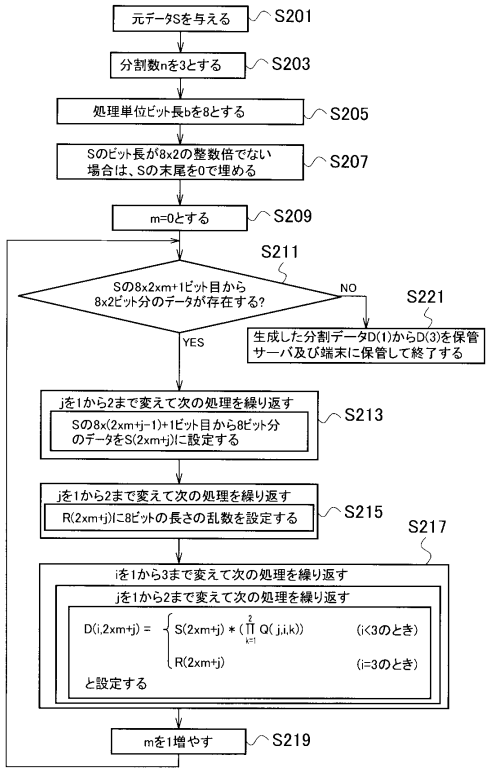
【図４】


アクセス権管理サーバ4
端末3b
端末3a
S120
甲の暗号鍵R生成
S130
データSを暗号鍵R'で暗号し、暗号データAを生成
S140
暗号データAを保管
S150
暗号鍵Rを端末3alに送信
S220
乙の暗号鍵R'生成
S230
暗号データAを暗号鍵R'R"で暗号化し、暗号データA'を生成
S240
暗号データA'を保管
S250
暗号鍵Rを端末3blに送信
S320
暗号鍵R'により暗号データA'を復号し、データSを生成
S330
データSを端末3blに送信(送付)
S260
暗号鍵Rを保管
S310
データ使用要求、暗号鍵R'をサーバ4に送信
S340
データSを保管
データSをサーバ4に送信(送付)
S110
S160
暗号鍵Rを保管
データのアクセス権限度の要求、暗号鍵Rをサーバ4に送信
S210

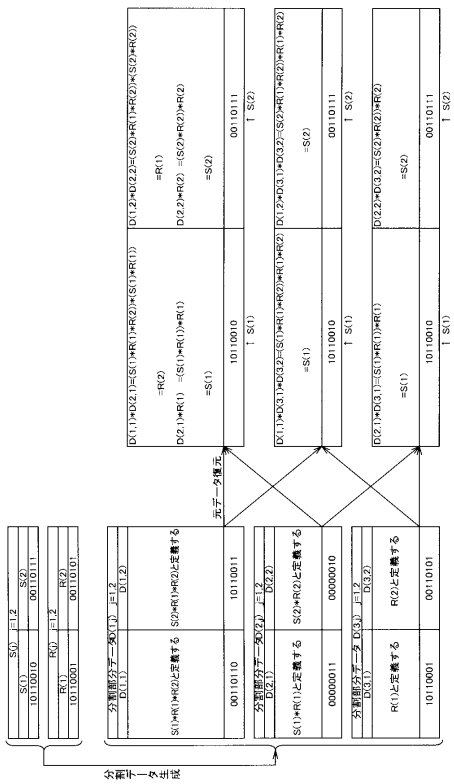
【図５】



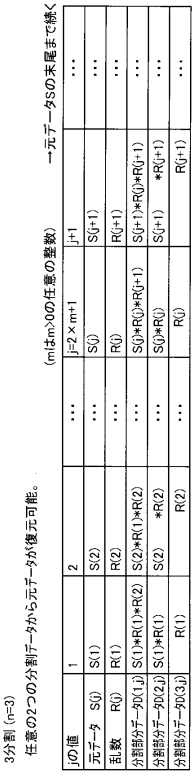
【図６】



【図７】

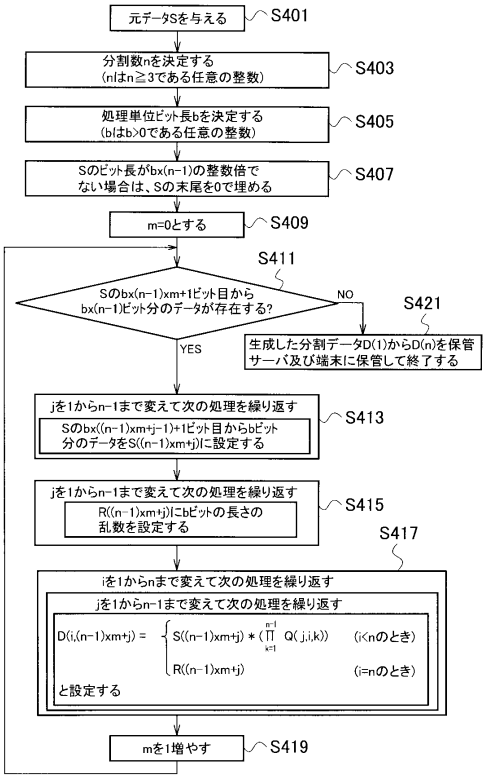


【図８】

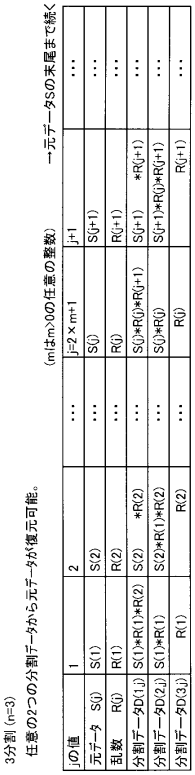


jの値	1	2	…	j=2×m+1	j+1	…
元データ S()	S(1)	S(2)	…	S(j)	S(j+1)	…
乱数 R()	R(1)	R(2)	…	R(j)	R(j+1)	…
分割部分データD(1,j)	S(1)*R(1)+R(2)	S(2)*R(1)+R(2)	…	S(j)*R()+R(j+1)	S(j+1)*R(j)+R(j+1)	…
分割部分データD(2,j)	S(1)*R(1)+R(2)	S(2)*R(1)+R(2)	…	S(j)*R()	S(j+1) *R(j+1)	…
分割部分データD(3,j)	R(1)	R(2)	…	R()	R(j+1)	…

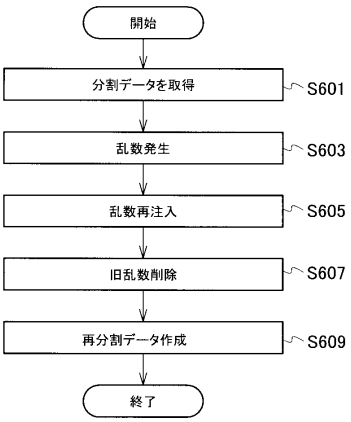
【図９】



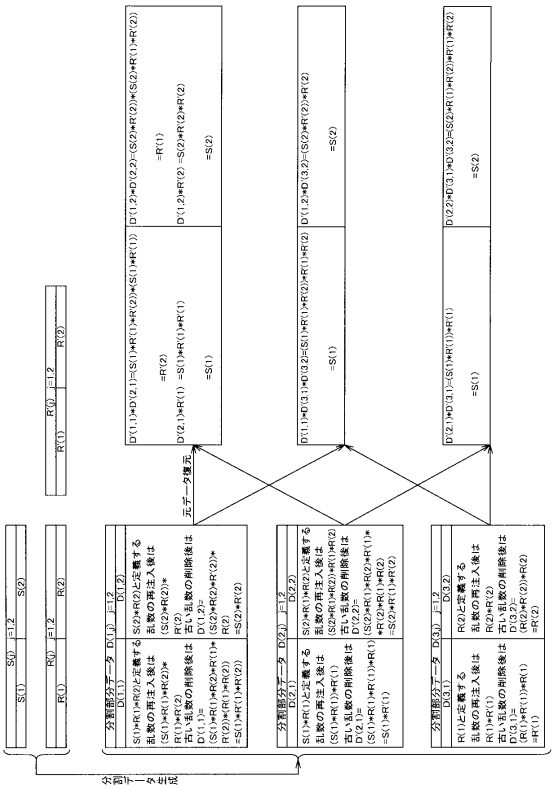
【図１０】



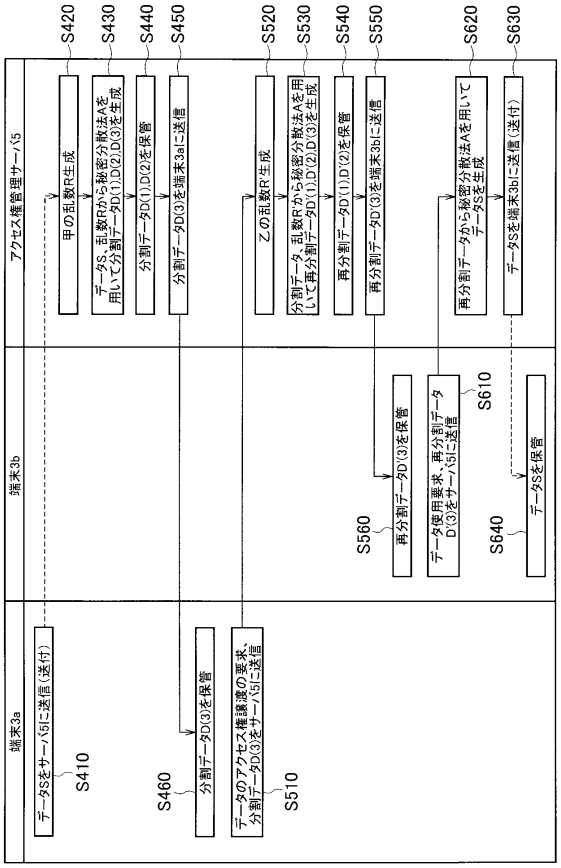
【図１１】



【図１２】



【図１３】


アクセス権管理サーバ5
端末3b
端末3a
甲の乱数R生成
データS、乱数Rから秘密分散法Aを用いて分割データD(1),D(2),D(3)を生成
分割データD(1),D(2)を保管
分割データD(3)を端末3aに送信
乙の乱数R生成
分割データ、乱数Rから秘密分散法Aを用いて再分割データD'(1),D'(2),D'(3)を生成
再分割データD'(1),D'(2)を保管
再分割データD'(3)を端末3bに送信
再分割データから秘密分散法Aを用いてデータSを生成
データSを端末3bに送信(送付)
データSをサーバ5に送信(送付)
分割データD(3)を保管
データのアクセス権譲渡の要求、分割データD(3)をサーバ5に送信
再分割データD'(3)を保管
データ使用要求、再分割データD'(3)をサーバ5に送信
データSを保管
S410
S420
S430
S440
S450
S460
S510
S520
S530
S540
S550
S560
S610
S620
S630
S640

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　松平　英

(56)参考文献　特開平０７－０３６９３２（ＪＰ，Ａ）
特開平１０－３２０４７８（ＪＰ，Ａ）
特開２００２－１６３２３５（ＪＰ，Ａ）
特開２００２－０７７１３９（ＪＰ，Ａ）
特開２００３－０４４３８８（ＪＰ，Ａ）
特開２００５－２３６４０３（ＪＰ，Ａ）
特開２００５－３４６００５（ＪＰ，Ａ）
特開２００５－３４６６５９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／００
Ｇ０６Ｇ　１２／１４