秘密分散法とその応用

Secret Sharing Scheme and Its Applications

保坂　範和　■ HOSAKA Norikazu
多田　美奈子　■ TADA Minako
加藤　岳久　■ KATO Takehisa

日本版SOX法（金融商品取引法の一部規定）(注1)や個人情報保護法などの法制度によって，機密情報や個人情報などの厳密な管理が，企業に求められている。しかし，厳密な管理を進めるがあまり，業務効率を落としてしまいがちである。これらの課題を同時に解決する技術として，秘密分散法が注目を集めている。

東芝ソリューション（株）では，従来よりも高速に処理できる秘密分散アルゴリズムを開発し，文書管理システムやコンテンツ配信システムに適用している。また，そのほかの様々なシステムへの応用も検討している。

With the enactment of the Financial Products Exchange Law and the Personal Information Protection Law, enterprises are required to strictly manage confidential information and personal information. On the other hand, operational efficiency tends to slow down when information has to be strictly managed. Secret sharing schemes are therefore attracting attention as a technology that can solve this problem.

Toshiba Solutions Corporation has developed a new secret sharing algorithm that is faster than previous algorithms. It is applicable to a broad range of systems, and has already been applied to a document management system and a content delivery system of Toshiba Solutions Corporation.

1　まえがき

個人情報だけでなく，組織の機密情報の漏えいに関する事件が社会問題となっている。これらの情報漏えい原因の約70 %が，紛失や管理ミス，誤操作などの内部要因という報告がある(1)。漏えい原因の多くは，情報を持ち出すことによる紛失や盗難である。そのため，情報資産の厳密な管理が，企業に求められている。

情報資産を厳密に管理するために，電子データを暗号化することが一般的であるが，この暗号化に用いた暗号鍵又は暗号化されたデータを紛失してしまうと，元データを復号できなくなってしまい可用性の損失を生ずる。この対策として，電子データのコピーを作成することが有効であるが，この場合，盗難のリスクが高くなってしまい機密性の損失を生ずる。

この可用性と機密性を両立させる技術として，秘密分散法が注目されている。秘密分散法の概念は，1979年にBlakleyとShamirによって，それぞれ独自に発表された(2), (3)。秘密分散法とは，秘密情報を複数に分散し，分散された情報からあらかじめ定められた個数が集まれば元の秘密情報に戻せるというものである。

ここでは，まず，秘密分散法の説明として，秘密分散法の一つである（k，n）しきい値秘密分散法（以下，（k，n）しきい値法と呼ぶ）のモデルと実現方法について概説し，その安全性について述べる。次に，東芝ソリューション（株）が提案する高速な秘密分散法のアルゴリズムと性能について述べ，最後に，秘密分散法を応用したシステムについて述べる。

（注1）　会計不祥事やコンプライアンス（法令遵守）の欠如などを防止するため，2006年6月に成立した法規制。同法で上場企業に対し“財務報告にかかわる”内部統制の評価と外部監査を義務付けた部分に焦点を当て，日本版SOX法と呼ぶ。

2　秘密分散法

2.1　概念

秘密分散法の一つである（k，n）しきい値法は，秘密情報をn個の分散情報に分散し，この分散情報から任意のk個を集めると，元の秘密情報が復元できる。一方，任意のk-1個の分散情報を集めても，元の秘密情報はまったくわからないという特長を持つ。

秘密分散法は，その特長を生かして，暗号鍵など重要な情報の管理に使われている(4), (5)。暗号鍵を秘密分散して管理することで，一部の分散情報が紛失しても，暗号鍵は漏えいしないので機密性の確保ができ，また，残っている分散された情報から元に戻せるので可用性の確保ができる。

更に，暗号鍵の管理だけでなく，データの保護にも適用が広まりつつある。内閣官房情報セキュリティセンターが出している「情報取扱手順書　雛(ひな)形」(6)によれば，「強化遵守事項」(注2)である要機密情報が格納された記憶媒体を移送する場合には，秘密分散を使って移送することとしている。

（注2）　特に重要な情報とこれを取り扱う情報システムにおいて，各府省庁でその事項の必要性の有無を検討し，必要と認められるときに選択して実施する必要がある対策事項のこと。

このため，大容量データも処理できる高速な秘密分散法が求められている。

2.2 モデル

(k, n) しきい値法は，秘密情報Sの保有者D（ディーラー）と，n人の分散情報を保管する管理者P1, …, Pnの間で実行される分散フェーズと復元フェーズとから構成される。

分散フェーズでは，Sの保有者DがSからn個の分散情報W1, …, Wnを生成し，分散情報を保管するn人の管理者P1, …, Pnにそれぞれ配布する。

復元フェーズでは，それぞれの管理者のなかから任意のk人以上の管理者が集まり，各自が保持する分散情報Wiを集めてSを復元する。モデルの例として，(3, 5) しきい値法の例を**図1**に示す。

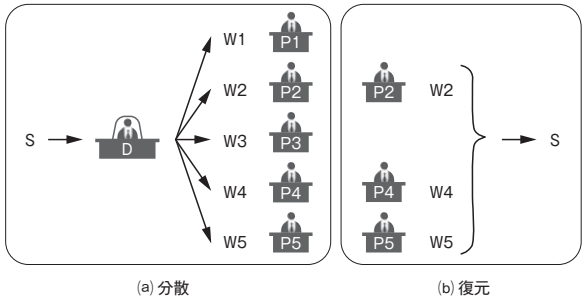

図1. (3, 5) しきい値法の例 — 秘密情報を五つの分散情報に秘密分散し，そのうちの任意の三つの分散情報を集めると，元の秘密情報を復元できる。

Example of (3, 5)-threshold secret sharing scheme

この場合，DはSから五つの分散情報W1, …, W5を生成し管理者P1, …, P5へそれぞれ配布する。任意の3人以上の管理者（例えばP2, P4, P5）が集まると，各自が保持する分散情報からSを復元できるが，管理者が3人未満の場合はSに関する情報はまったくわからない。

2.3 実現方法

(k, n) しきい値法の実現方法について，ここでは，一般的なk-1次の多項式を利用した方式[3]で述べる。以下に具体例として (2, 3) しきい値法の実現方法を示す（**図2**[7]）。

まず分散処理について述べる。Dは，y切片を秘密情報の値Sとし，傾きαをランダムに選択することで，一次式$y=\alpha x+S$を決定する。そして，一次式の直線上にある三つの点W1, W2, W3を分散情報として管理者P1, P2, P3にそれぞれ配布する（図2 (a)）。

次に復元処理について述べる。例えば，管理者P2とP3が集まると，点W2, W3が得られるため，一次式$y=\alpha x+S$に関する連立方程式を解くことで，Sを求めることができる。しかし，管理者1人では，直線上の1点しかわからないらないため，一次式$y=\alpha x+S$を解くことができない。したがってSを求めることができないだけでなく，Sに関する情報はまったくわからない（図2 (b)）。

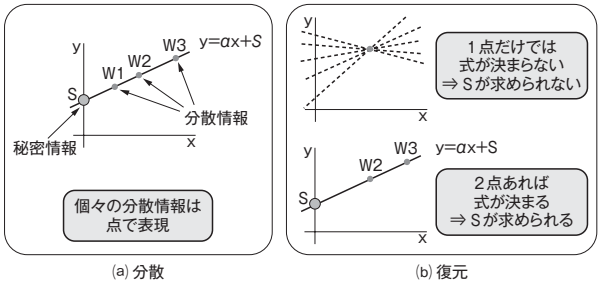

図2. (2, 3) しきい値法の実現方法 — 一次式のy切片を秘密情報Sとし，傾きαをランダムに選択して，一次式$y=\alpha x+S$を決定する。この一次式の直線上にある三つの点W1, W2, W3を分散情報とする。このうち2点が集まれば一次式を求められるため，秘密情報Sを復元できるが，1点では一次式が求められないため，秘密情報Sについてまったくわからない。

Implementation of (2, 3)-threshold secret sharing scheme

2.4 安全性

(k, n) しきい値法は，一般的に知られているAES (Advanced Encryption Standard)[注3]やRSA[注4]などの暗号とは，安全性の仮定が異なっている。

暗号は計算量的安全性に基づいている。計算量的安全性とは，現在の計算機では現実的な時間では解くことが困難なことをいう。例えば，RSA暗号は素因数分解が解けると解読できる。しかし，現在の計算機では大きな合成数の素因数分解は現実的な時間で解く方法が知られていないため，安全とされている。なお，将来計算機の計算能力が飛躍的に向上すると，現実的な時間で解読される可能性がある。

一方，(k, n) しきい値法は，計算量的安全性ではなく，情報理論的安全性に基づいている。情報理論的安全性とは，無限の計算能力と記憶装置を持つ計算機でも解けないことをいう。

3 高速な秘密分散法

当社は，排他的論理和[注5] (XOR：eXclusive OR) を用いた (2, n) しきい値法[8]と (3, n) しきい値法（但し，$n \leqq 7$）[9]を提案している。当社方式は，ビットごとのXORだけで秘密分散法を構成できるため高速な分散／復元処理が可能であり，またアルゴリズムが単純であるため，従来のような小容量データ（暗号鍵など）だけではなく，大容量データも容易に処理できるとともに，組込み機器への実装にも適している。

当社の (2, n) しきい値法について，n=5の例を用いて述べる。

(注3) 米国政府の次世代標準暗号方式。
(注4) 代表的な公開鍵暗号方式の一つで，3名の開発者（R. Rivest, A. Shamir, L. Adleman）の頭文字から命名された。なお，RSAはRSA Security, Inc.の登録商標。
(注5) $0 \oplus 0=0$, $1 \oplus 0=1$, $0 \oplus 1=1$, $1 \oplus 1=0$となるビット演算。ただし，$\oplus$はXORの演算子を表す。

3.1 分散アルゴリズム

Dは，以下の分散アルゴリズムでSから分散情報W1，…，W5を生成し，管理者P1，…，P5にそれぞれ配布する。

入力：S

出力：分散情報W1，…，W5

(1) 秘密情報Sを分割秘密情報S1，…，S4に等分する。

(2) 互いに独立な乱数R1，…，R4を生成する（ただし，各乱数のサイズ＝各分割秘密情報のサイズ）。

(3) 分割秘密情報S1，…，S4と乱数R1，…，R4のXORにより分散情報W1，…，W5を計算する（計算方法を**図3**に示す）。

ここで，各分散情報W1，…，W5は，同じサイズの乱数と排他的論理和されているため，一つの分散情報から元の秘密情報はまったくわからない。つまり，情報理論的安全性を満たす。

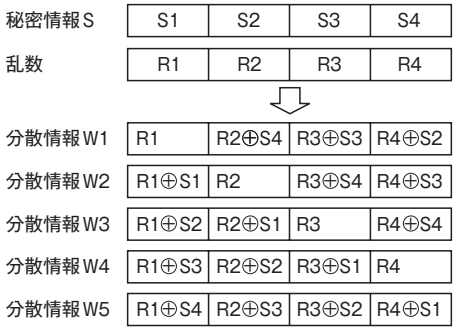

図3. (2, 5) しきい値法の分散アルゴリズム — 当社の秘密分散アルゴリズムは，排他的論理和だけで構成されるアルゴリズムで，分割秘密情報S1，…，S4と乱数R1，…，R4は各々同じサイズであるため，導出された分散情報からは元の情報はまったくわからない。

Encoding algorithm of (2, 5)-threshold secret sharing scheme

3.2 復元アルゴリズム

一方，任意の二つの分散情報を集めると，Sを復元することができる。例として，分散情報W4とW5からSを復元する場合について述べる。

入力：分散情報W4，W5

出力：S

(1) 分散情報W4とW5のXORにより分割秘密情報S1，…，S4を計算する（計算方法を**図4**に示す）。

(2) 分割秘密情報S1，…，S4を連結して，Sを復元する。

また，(3, n) しきい値法（ただし，n ≦ 7）でも同様に，XORだけで分散／復元処理が可能な方式を提案している。

3.3 性能

次に，当社が開発した秘密分散ライブラリの性能について述べる。当社の秘密分散ライブラリは，上記の (2, n) しきい値法，(3, n) しきい値法（ただし，n ≦ 7）の分散／復元アルゴリズムをC言語で実装している。秘密分散ライブラリの分散処理時間を**図5**に，復元処理時間を**図6**に示す。ただし，

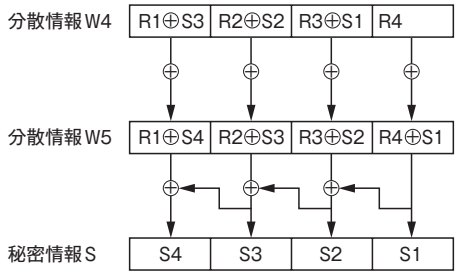

図4. (2, 5) しきい値法の復元アルゴリズム — 分散情報から元の秘密情報を復元するアルゴリズムも，排他的論理和だけで構成される。例では分散情報W4とW5から分割秘密情報S1，…，S4が求められる過程を示している。同様に他の組合せでも分割秘密情報S1，…，S4が求められる。

Decoding algorithm of (2, 5)-threshold secret sharing scheme

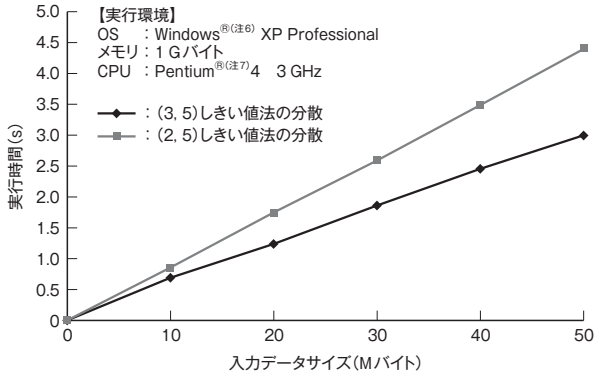

図5. 秘密分散ライブラリの分散処理時間 — 当社の秘密分散アルゴリズムを実装した秘密分散ライブラリの分散処理時間である。30 Mバイトのデータでも2秒前後で秘密分散できるため，大容量のデータ処理に向いている。

Processing times of encoding with secret sharing scheme library

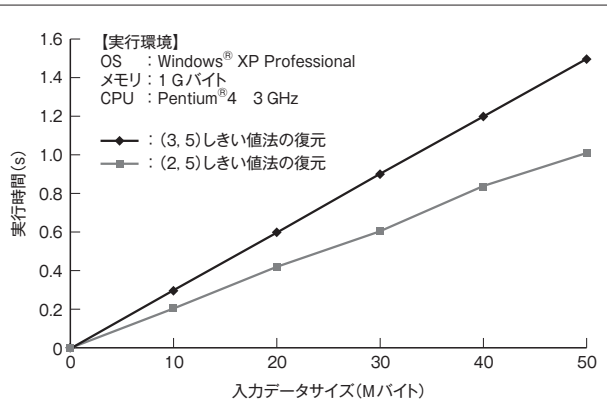

図6. 秘密分散ライブラリの復元処理時間 — 当社の秘密分散アルゴリズムを実装した秘密分散ライブラリの復元処理時間を示す。30 Mバイトのデータでも1秒以内で復元できるため，大容量のデータの移送やバックアップに向いている。

Processing times of decoding with secret sharing scheme library

(注6) Windowsは，米国Microsoft Corporationの米国及びその他の国における商標又は登録商標。

(注7) Pentiumは，米国及びその他の国における米国Intel Corporation又は子会社の登録商標又は商標。

乱数生成処理は別ライブラリを利用しているため，図5の分散処理時間には含まれていない。

処理性能は，分散処理で約90～130 Mビット/s，復元処理で約260～390 Mビット/sであり，十分に大容量のデータ処理に適用できる。ただし，乱数生成処理は分散処理には含まれていない。

4　秘密分散法の応用

当社は，文書管理システムやコンテンツ配信システムに秘密分散ライブラリを適用している。

また，秘密分散法の一般的な応用として，**図7**のように機密情報の安全な搬送にも利用することができる。

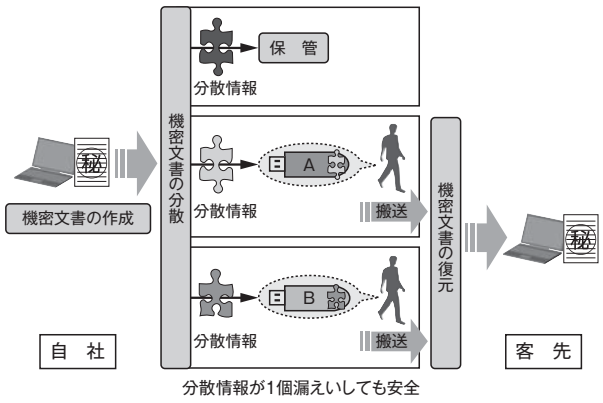

図7. 秘密分散法の応用 — 機密文書を秘密分散して搬送することで，搬送時の情報漏えいを防止できる。

Application of secret sharing scheme

例えば，自社で作成した機密文書（秘密情報）を客先まで安全に搬送する場合，まず，機密文書を(2, 3)しきい値法により三つの分散情報に分散し，そのうち二つの分散情報をUSB（Universal Serial Bus）メモリなどの記録媒体に格納し，別々の担当者が客先まで搬送する。

次に，各担当者は，客先で二つの分散情報を集めることで元の機密文書を復元できる。もし，どちらかの担当者が搬送途中で分散情報をなくしても，元の機密情報が漏えいすることはない。

また，搬送以外にも，記録媒体としてストレージを利用することで，データバックアップやディザスタリカバリ（Disaster Recovery）(注8)にも応用できる。

(注8)　災害などによって生じたシステム障害を復旧させること。

5　あとがき

ここでは，秘密分散法を紹介し，当社が提案した高速な秘密分散法について述べた。当社が提案する秘密分散法は，簡単なアルゴリズムで実現でき，従来方式よりも計算効率が良い。

今後は，提案方式の特長を生かしたシステムへの応用展開を図っていきたい。

謝　辞

この研究を進めるにあたり，日本大学生産工学部 専任講師 栃窪孝也氏から有益な助言をいただきました。心より感謝いたします。

文　献

(1)　(独)情報処理推進機構．“情報漏えい対策のしおり”．<http://www.ipa.go.jp/security/antivirus/documents/5_roei_v2.pdf>，(参照 2007-03-05)．
(2)　G. Blakley. Safeguarding cryptographic keys. Proc of AFIPS. **48**, 1979, p.313－317.
(3)　A. Shamir. How to share a secret. Communications of the ACM. **22**, 11, 1979, p.612－613.
(4)　日本認証サービス株式会社．“PKI用語解説”．<http://www.jcsinc.co.jp/support/faq_pki.html>，(参照 2007-03-05)．
(5)　PGP Corporation. “PGP White Paper The OpenPGP Standard & PGP Products.” <http://download.pgp.com/pdfs/whitepapers/OpenPGP-PGP-Products_050524_F.pdf>，(参照 2007-03-05)．
(6)　内閣官房情報セキュリティセンター．“情報取扱手順書 雛形”．<http://www.nisc.go.jp/active/general/pdf/dm3-02-051_sample.pdf>，(参照 2007-02-20)．
(7)　黒澤　馨，ほか．電子情報通信レクチャーシリーズD-8現代暗号の基礎数理 電子情報通信学会編．コロナ社，2004，198p.
(8)　藤井吉弘，ほか．“高速な(2, n)閾値法の構成法とシステムへの応用”．コンピュータセキュリティシンポジウム（CSS）2005予稿集．情報処理学会．愛媛，2005-10，情報処理学会CSEC研究会．東京，情報処理学会，2005，p.631－636.
(9)　多田美奈子，ほか．“閾値3の秘密分散法の構成法”．コンピュータセキュリティシンポジウム（CSS）2005予稿集．情報処理学会．愛媛，2005-10，情報処理学会CSEC研究会．東京，情報処理学会，2005，p.637－642.

保坂　範和　HOSAKA Norikazu
東芝ソリューション(株) IT技術研究所。
コンテンツ保護，暗号プロトコルの研究及び応用開発に従事。
Toshiba Solutions Corp.

多田　美奈子　TADA Minako
東芝ソリューション(株) IT技術研究所。
電子署名，暗号プロトコルの研究・開発に従事。
電子情報通信学会，情報処理学会会員。
Toshiba Solutions Corp.

加藤　岳久　KATO Takehisa
東芝ソリューション(株) IT技術研究所主務。
課金決済，プライバシー保護，ネットワークセキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Toshiba Solutions Corp.