秘密分散法の概要

西川　律子

個人情報保護法の施行や個人のプライバシー意識の高まりにより，ディスクの電子媒体などに格納された個人情報・機密情報の取り扱いについて厳しく管理されるようになってきた。それに伴い，それらのデータの管理に利用するセキュリティ技術が注目されている。

秘密にしておきたいファイルなどの情報を他人に知られないようにするためには，共通鍵暗号化方式*1) を用いて暗号化するのが一般的である。暗号，復号とも，同じ1つの鍵（共通鍵）を使う方式である。また，認証，機密通信などではPKI（Public Key Infrastructure）*2) が利用されている。しかし，鍵を使う方式は，秘密鍵の管理，証明書の発行・更新など利用に際し，運用コストがかかる。

電子割符は，これらの鍵暗号方式に比べ，運用が容易，セキュリティ強度が高いと期待されている。電子割符では，秘密分散法と呼ばれる方式を用いており，「秘密」にすべき情報を複数の「分散情報」に分け，それらがある決めた数集まらないと元のデータを復元することができない。

本稿では，秘密分散法の一般的な方式から，その応用例までを述べる。

秘密分散法の方式

秘密分散法とは，その使い方から「電子割符」とも呼ばれる暗号化技術の一つである。よく利用される鍵暗号化方式との大きな違いは，秘密分散法では，暗号化対象である元データを複数のデータ（「分散情報」）に分ける点にある。秘密分散法を用いて，複数の「分散情報」に分けられた元データは，分割したうちの決められた数片の「分散情報」を集めないと，復元されない。

秘密分散法は1979年，RSA暗号方式で有名なシャミア博士により，最初に論文発表された。この秘密分散法は，しきい値分散法と呼ばれ，最も一般的な方式である。その仕組みは，直線などを表す連立方程式で説明することができる。たとえば，ある秘密にしたい元データ「S」を

$$F(X) = aX + S$$

と表現できるとする。このとき，aが不明であるとした場合，Sを求めるためには，直線F（X）を決める必要がある。直線は，直線上の2点を決めると，求めることができる。このときの2点が，「分散情報」に相当する（**図1**）。

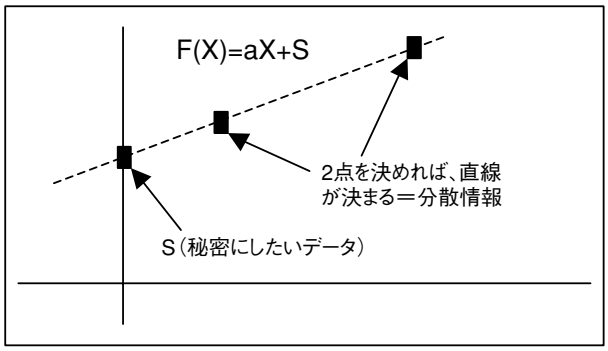

図１　しきい値分散法の例

例では，1次方程式を利用したが，連立方程式の作り方によって，復号に必要な分散情報の数を決めることができる。

沖電気は，トラステッドソリューションズ株式会社（以下，TS社）[1] と協業，TS社の提供する秘密分散法を利用している。TS社の秘密分散法は，しきい値分散法とは異なるAONT（All or Nothing　Transform）と呼ばれる方式を利用している。

AONTは，安全性を犠牲することなく効率的に暗号化するため，暗号化の前に行う変換である暗号化モードの一種である[2]。具体的には元データ（平文）に対し，適切な冗長データを付加，変換するといった処理を繰り返す。AONTの詳細な内容は，本稿で述べないが，AONTは，変換時に秘密情報を利用していない，暗号文の一部でも足りないと復号ができない，平文の安全性が数学的に証明されているといった特長がある。そのため，数学的安全性を立証された秘密分散法を実現することができる。

AONTを応用した秘密分散法では，分散情報は，暗号化データを分割して作成する。そのため，1片を1KBまで小さくすることができる。また，一般的な秘密分散法では1つの分散情報が元データと同じサイズになるのに対し，

＊1）共通鍵暗号化方式：暗号化，復号化に同じ鍵を用いる方式　＊2）PKI（Public Key Infrastructure）：公開鍵暗号化方式。一般に公開されている公開鍵と，公開していない個人鍵とで一対になり，暗号化・復号化を行う方式

表 1　秘密分散法の応用商品例

	商品概要	秘密分散法の利用法	秘密分散法によるメリット
1	暗号化ライブラリ	暗号化ライブラリ中で作成する共通鍵暗号の鍵データの保管に利用。	鍵を秘密分散法で暗号化することにより、安全に保管することが可能。
2	データ配送	データを複数分割し、別の経路で配送。電子メールと媒体、HTTPと媒体など。	配送経路上で漏洩しても、意味のデータであり、元データが復元できない。
3	パソコンデータの保護	機密情報などのファイルを複数種類のデバイスに分散保持。	パソコンが盗難にあっても元データの復元ができないため、データが漏洩しない。
4	セキュアファイルサーバ	ファイルサーバ上のファイルを秘密分散法で分割保持。	ファイルサーバ上のデータは、意味の無いデータであり、ファイルを盗んでも、元データが復元されない。
5	バックアップサービス	システムのバックアップデータを暗号化した上で分割、保管。	機密情報を複数の遠隔地で安全に保管する。

処理前後のデータ量が不変であるAONTを応用することにより，分散前後のデータサイズがほぼ同じといったメリットがある。

秘密分散法の特長

秘密分散法では，秘密にしたい情報を複数の「分散情報」に分ける。共通鍵暗号などの暗号化手法を用いた場合，データになんらかの暗号化のための変換を加えて，元データの復元を困難にしているが，データそのものが内包されているため，コンピュータにおけるCPUの処理スピードの向上，暗号解読技術の進歩などにより解読される可能性が残る。しかし，秘密分散法の場合は，データそのものが複数に分かれるため，たとえ，分散情報の1つを取得したとしても，その情報から，元データを復元することはできない。このことから，高い安全性が得られる。

鍵を使った暗号化と比較した場合，鍵の管理がないため，保管に関する運用の手間を削減，鍵の漏洩による暗号解読リスクがないというメリットもある。

また，一片を1KBまで小さくすることにより，分散されたデータの1片を，電子メールに添付する，ネットワークで送付するといったさまざまな応用システムを検討することができる。

秘密分散法の応用商品

近年，秘密分散法を応用した商品は，機密情報の管理，配送，保管など多岐に渡り展開されている。

沖電気では，会社間での機密情報の受け渡しに秘密分散法を応用した，eすぷりっと便™*3) を開発した。本商品では，機密情報を秘密分散法で意味のない2つのデータに分割，各々を電子メール，媒体などで配送，紛失，盗難に対策できると同時に，配送コストの削減を実現する。

また，沖電気は上記商品をはじめ，秘密分散を応用した多数の商品（**表1**）を販売，お客様に情報漏洩対策の一環としてご利用いただいている。

今後の展開

秘密分散法は，そのユニークな暗号化技術が注目され，各社で商品への応用例が増加している。今後も，各種認証への応用，ネットワークを利用したデータ保管など各種商品を展開していく予定である。 ◆◆

*3)eすぷりっと便は沖電気工業(株)の商標です。また，eすぷりっと便による情報配送方法は特許出願中です。

■参考文献

1）トラステッドソリューションズ社　ホームページ
http://trusted-solutions.jp
2）桑門秀典，神戸大学：暗号システムの安全性を向上させる暗号化モードに関する研究（継続），電気通信普及財団，研究調査報告，No.19，p.236，2004年

●筆者紹介

西川律子：Ritsuko Nishikawa. ネットビジネスカンパニー ソリューション開発部