個人情報管理システム「データジグソー™」

技術評価書

2006年2月

メディアスティック株式会社

目次

1　はじめに

メディアスティックの提供する個人情報管理システム「データジグソー™」は、極めて堅牢な個人情報保護機能と、導入企業のユーザビリティを兼ね備えたシステムである。

2005年4月より「個人情報保護法」が施行され、その厳守は企業存続自体をも左右する時代となってきた。その反面、顧客層の求めるサービスは告知手段の拡大、販路の充実などにより年々要望が高まってきている。

ここでは「データジグソー™」が顧客と導入企業をつなぐ最も信頼的かつ有効である個人情報管理システムであることを説明する。

2　「データジグソー™」の優位性

2.1　開発の経緯

「いかに個人情報や機密情報を取り扱うことができるか？」という課題のもと、「安心・安全・簡単」な情報管理・運用データベースシステムを目指し、「モバイルメタデータベースシステム」(*1)をベースに「データジグソー™」は開発をされた。

この「モバイルメタデータベースシステム」とは、発案・開発当初から、NTT ドコモ社が「i モード」サービスを開始したまさに「モバイルの黎明期」とも言える頃より、PC、携帯電話、Web などとシームレスに対応できるデータベースとして成り立っている。

これらを構成する技術は、国際特許(*2)でも守られている。

2.2　主要開発陣

基本設計	北川　高嗣　（工学博士） 筑波大学大学院システム情報工学研究科教授
監修 （暗号化技術）	辻井　重男　（工学博士） 情報セキュリティ大学院大学学長 CRYPTREC(*3)　暗号技術評価検討会メンバー （暗号技術評価委員会元顧問　暗号技術評価検討会元顧問）

2.3　政府事業採用

「モバイルメタデータベースシステム」は、

- 2001年度　経済産業省・IPA（情報処理振興事業協会）の「先端的・戦略的ソフトウェア」開発支援事業
- 2002年度　内閣府・e-JAPAN「電子政府情報セキュリティ技術開発事業」
- 2003年度　経済産業省・IPA「重点領域情報技術開発事業」

に選定されており、特にIPA関連案件においては、セキュリティセンターの厳しい審査基準（選定・納品）を辻井重男教授（現情報セキュリティ大学院大学学長）監修の下、クリアしている。

このほか大手企業、メーカ、通信キャリア関連の複数のセキュリティの専門家からの度重なるチェックを 2 年以上に渡り受け続けており、現在に至るまで、すでに80社以上・延べ100万人を超える運用実績がある。

「データジグソー™」は、この3年にわたる運用実績をベースに個人情報管理システムとして開発されたものである。

(*1) (*3) P.10 参照　(*2) P.9 参照

2.4 “分割多重暗号化方式”を採用した個人情報管理システム

2.4.A 「データ分割方式」

データは、あらかじめ指定されたデータの区分ごとに分割される。(この区分は任意に指定可能)
データの一部が漏えいしたとしてもデータ間の紐付けができないので、意味をなす情報が得られない。

2.4.B 「暗号化データベース」

分割されたデータは、それぞれ個別に異なった鍵で暗号化される。データは保管サーバ内で暗号化されたまま処理される。暗号化する際使用した鍵は、別プロセスによって管理されるので、たとえデータベースを丸ごと盗まれたとしても、そのデータベースを解読し、個人情報を構成・閲覧することはできない。

2.4.C 「多重暗号化方式」

暗号鍵は分割されたデータごとに異なる上に、個人ごとにも異なった鍵が発行され暗号化される。
このため、ある特定の暗号鍵を取得したとしても実質解読不能である。

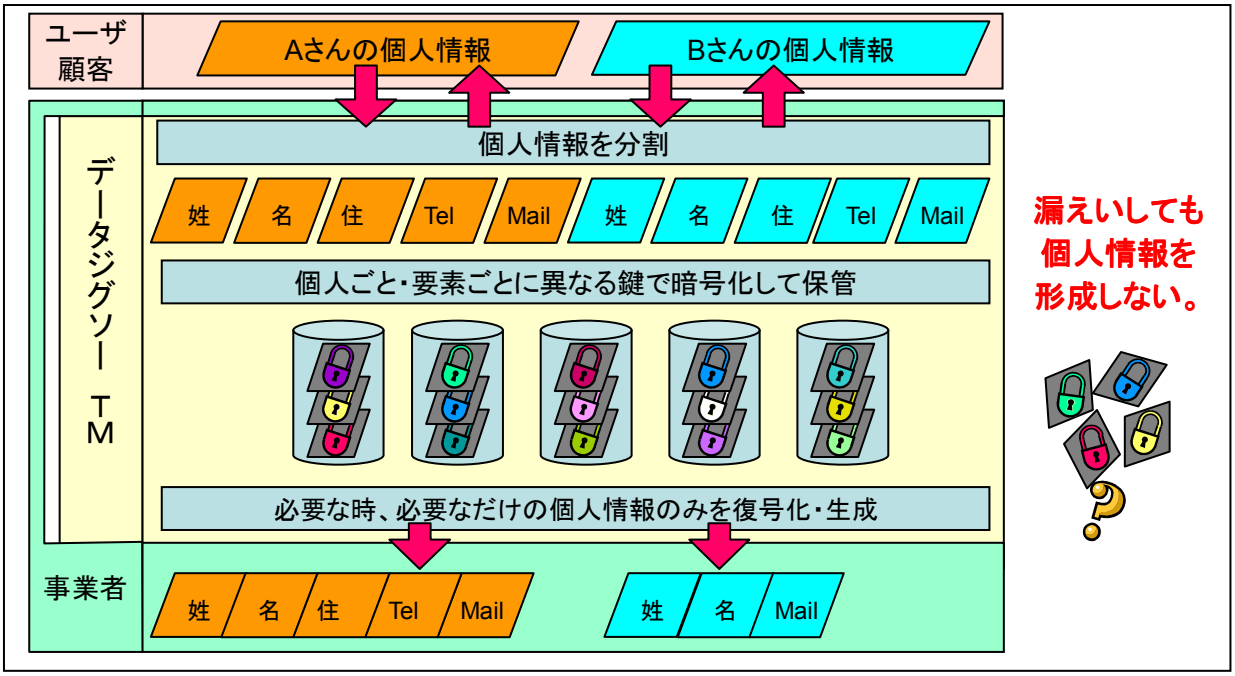


図1.「データジグソー™」概要図

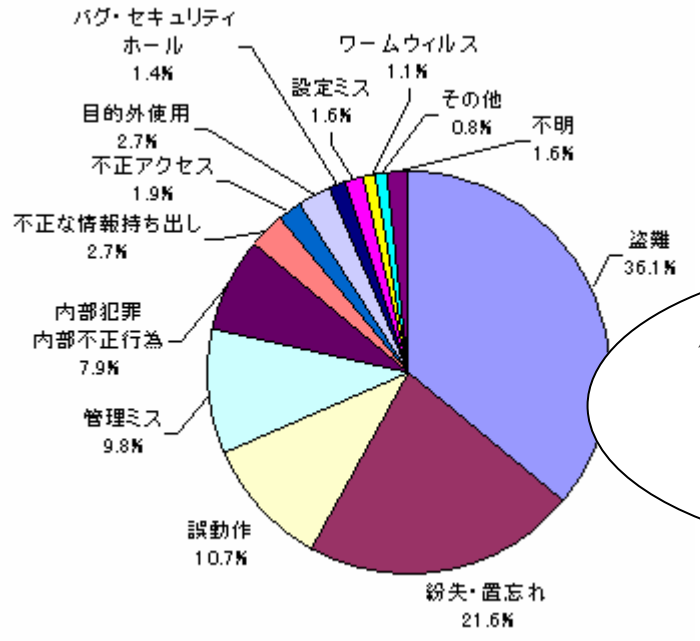
表1. 類似方式に対する、「データジグソー™」の優位性

方式	方法	欠点・短所	データジグソー™が解決するもの
データの暗号化 (データ対策)	記録媒体・格納場所・ファイル自体をそのまま暗号化して保護する。	暗号(暗号鍵)を持つ特定の管理者が持ち出そうとすれば、個人情報は容易に漏えいしてしまう。	実際にデータを分割した上でそれぞれ異なった鍵で暗号化しているため、特定の管理者が元データを構成できない。
割符方式 (鍵対策)	長い鍵を設定し、その鍵情報を分散して持たせる。	鍵が集まれば、元データを構成できてしまう。	多重かつ複合的に暗号化されるため、保護強度が格段に高い。
秘密分散(共有)方式 (データ&鍵対策)	複数人で秘密鍵情報を持ち合う。例えば 10 人のうち任意の3人が秘密鍵情報を持ち寄れば復号化できるなど。	秘密データ自体が分散されるわけではない。	秘密データ自体を分割している為、一部のデータが復号化されたとしても個人情報は構成されない。

表2. 蓄積データを活用する際における有効性　（当社による調査比較）				
要件	データジグソー™	データの暗号化	割符方式	秘密分散(共有)方式
管理者権限 (administrate)	◎ (管理者・システム担当者でも流出不可)	△ (管理者・管理者以外による持出懸念)	△ (全データの復号化必須)	○ (秘密鍵情報は1度しか有効性は無い)
検索 (Searching)	◎ (該当データのみ復号化)	× (全データの復号化必須)	× (全データの復号化必須)	△ (該当データ以外も復号化必須)
抽出 (Sorting)	◎ (該当データのみ復号化)	× (全データの復号化必須)	× (全データの復号化必須)	△ (該当データ以外も復号化必須)
分析 (Analyzing)	◎ (該当データのみ復号化)	× (全データの復号化必須)	× (全データの復号化必須)	△ (該当データ以外も復号化必須)

表3. 想定される情報流出リスクへの耐用性　（当社による調査比較）				
用件	データジグソー™	データの暗号化	割符方式	秘密分散(共有)方式
パスワード流出	◎	×	△	○
個人特定	◎	×	×	×
関連付け	◎	×	×	×

参考:個人情報漏えい原因の件数割合



NPO 日本ネットワークセキュリティ協会
「2004 年度情報セキュリティインシデントに関する調査報告書」　(2006/1/10)

個人情報漏えいの９０％以上は、部内関係者の不注意やうっかりミスから

「個人情報漏えい原因の分類」

No.	要素	原因	%	対応する原因
1	技術的	人為ミス	22.1	設定ミス、誤操作、管理ミス
2	技術的	対策不足	4.4	バグ・セキュリティホール、ウイルス、不正アクセス
3	非技術的	人為ミス	24.3	置き忘れ、目的外利用
4	非技術的	犯罪	46.7	内部犯罪、情報持ち出し、盗難
5	その他	その他、不明	2.4	その他、不明

3　「データジグソー™」の客観的評価

辻井重男 情報セキュリティ大学院大学学長（CRYPTREC 暗号技術評価検討会メンバー 暗号技術評価委員会元顧問 暗号技術評価検討会元顧問）が、「データジグソー™」について、客観的な視点で評価を行った。

暗号の分野では、「秘密分散（共有）」（Secret Sharing）という方式が知られている。それは、一言で例えるならば、3人に秘密を分け与えておいて、その内の2人と設定したならば2人が集まれば復元できるという手法である。

秘密を分割して暗号化するような誤解を与え易い名称だが、そういう方式ではない。

もともと「秘密分散（共有）」（Secret Sharing）とは、1人だけで秘密を持っていると危ないということから考案された方式である。例えば、某国の大統領が1人で勝手に判断して核ミサイルを撃ってしまうのでは危険であるから、権限のある何人かが合意しないと動けないようにしておこう、という動機から始まっている。

要するに、「秘密分散（共有）」とは、平文を分けるという目的でやっているのではないのである。

この「秘密分散（共有）」（Secret Sharing）をデータの暗号化に用いた場合、平文の上に、封筒を被せるようなものである。例えば A さんにはこの封筒、B さんにはこの封筒、C さんにはこの封筒と渡しておき、3人のうち2人、10人のうち6人（k-out-of-n 分散方式）と設定された人が集まって、その封筒を擦り合わせると、その封筒が消えて中身の全てが取り出せるようなイメージ（図2）である。

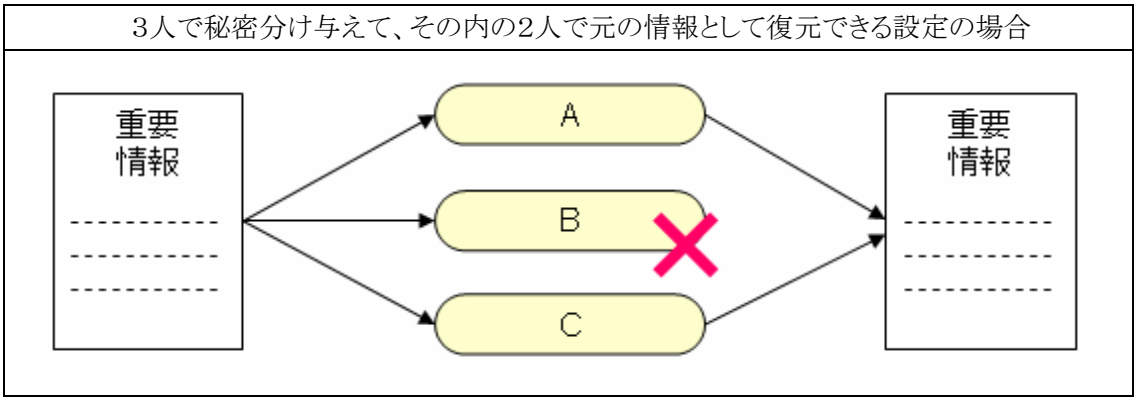
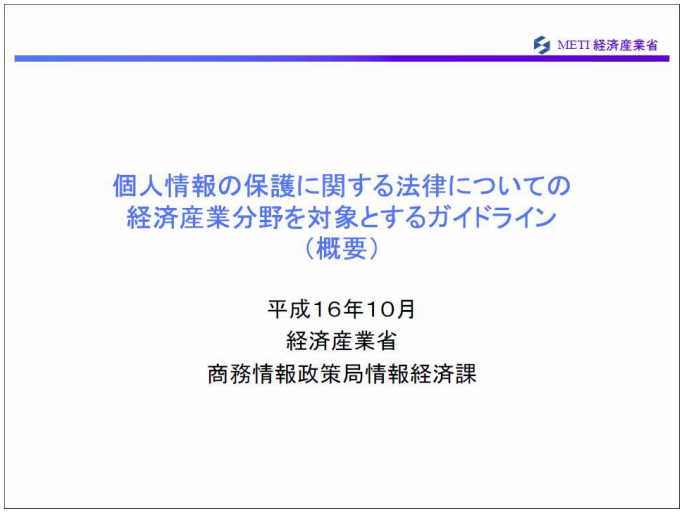


図2.「秘密分散（共有）」イメージ

従って、秘密保護という目的に対しては決して強いとは言えない。逆に分け合った人が集まってしまえばその秘密は見えてしまうからだ。

今日においては、個人情報保護法に関連して、「暗号化された個人情報は、個人情報と取り扱うべきか否か？」という議論があるが、「暗号化しても復号化できるのだから個人情報である」という認識がある。

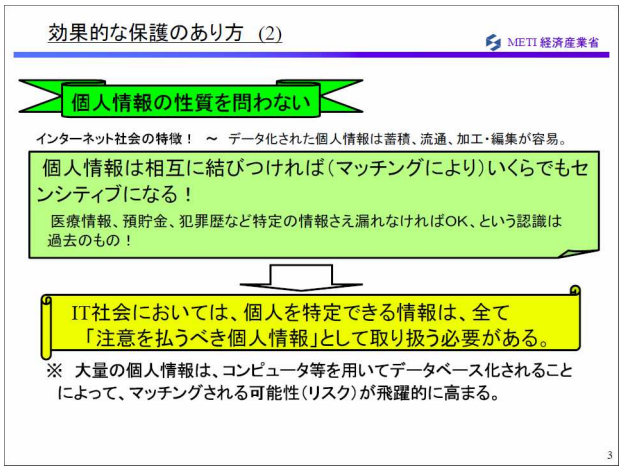
経済産業省 商務情報政策局 情報経済課の発表した、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（概要）」（ガイドライン検討委員会委員長 堀部政男 中央大学法科大学院教授）においては、個人情報に該当するものは、「暗号化されているかどうかを問わない。」と明記（図3）されており、それは経済産業省だけではなく、総務省・厚生労働省でも同じ認識である。



METI 経済産業省

個人情報の保護に関する法律についての
経済産業分野を対象とするガイドライン
（概要）

平成16年10月
経済産業省
商務情報政策局情報経済課



効果的な保護のあり方 (2)

METI 経済産業省

個人情報の性質を問わない

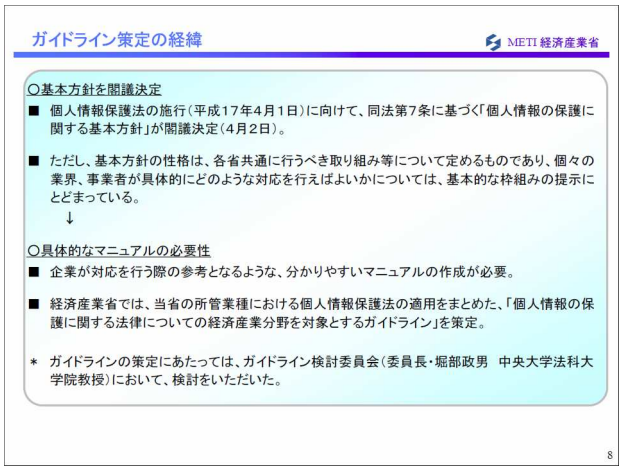
インターネット社会の特徴！ ～ データ化された個人情報は蓄積、流通、加工・編集が容易。

個人情報は相互に結びつければ（マッチングにより）いくらでもセンシティブになる！
医療情報、預貯金、犯罪歴など特定の情報さえ漏れなければOK、という認識は過去のもの！

IT社会においては、個人を特定できる情報は、全て「注意を払うべき個人情報」として取り扱う必要がある。

※ 大量の個人情報は、コンピュータ等を用いてデータベース化されることによって、マッチングされる可能性（リスク）が飛躍的に高まる。

3

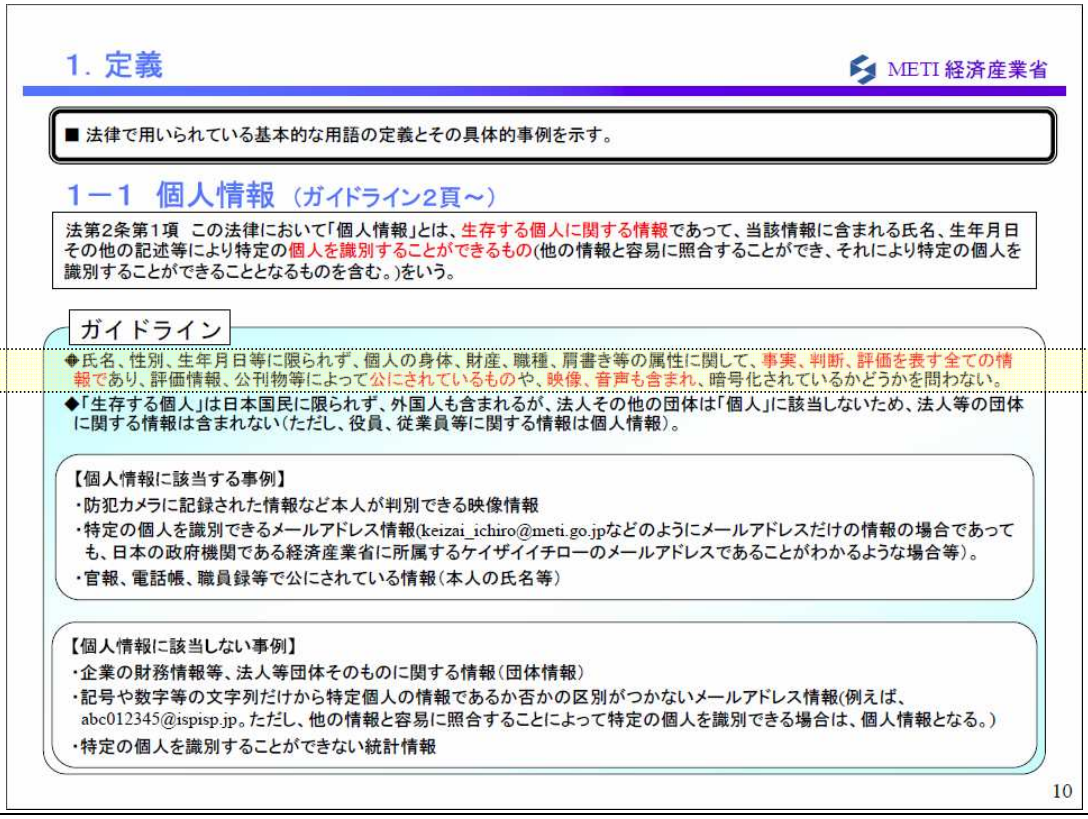


ガイドライン策定の経緯

METI 経済産業省

○基本方針を閣議決定
■ 個人情報保護法の施行（平成17年4月1日）に向けて、同法第7条に基づく「個人情報の保護に関する基本方針」が閣議決定（4月2日）。
■ ただし、基本方針の性格は、各省共通に行うべき取り組み等について定めるものであり、個々の業界、事業者が具体的にどのような対応を行えばよいかについては、基本的な枠組みの提示にとどまっている。
↓
○具体的なマニュアルの必要性
■ 企業が対応を行う際の参考となるような、分かりやすいマニュアルの作成が必要。
■ 経済産業省では、当省の所管業種における個人情報保護法の適用をまとめた、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を策定。
＊ ガイドラインの策定にあたっては、ガイドライン検討委員会（委員長・堀部政男 中央大学法科大学院教授）において、検討をいただいた。

8



1. 定義

METI 経済産業省

■ 法律で用いられている基本的な用語の定義とその具体的事例を示す。

1－1 個人情報（ガイドライン2頁～）

法第2条第1項 この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

ガイドライン

◆氏名、性別、生年月日等に限られず、個人の身体、財産、職種、肩書き等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされているものや、映像、音声も含まれ、暗号化されているかどうかを問わない。
◆「生存する個人」は日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体に関する情報は含まれない（ただし、役員、従業員等に関する情報は個人情報）。

【個人情報に該当する事例】
・防犯カメラに記録された情報など本人が判別できる映像情報
・特定の個人を識別できるメールアドレス情報(keizai_ichiro@meti.go.jpなどのようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等)。
・官報、電話帳、職員録等で公にされている情報（本人の氏名等）

【個人情報に該当しない事例】
・企業の財務情報等、法人等団体そのものに関する情報（団体情報）
・記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@ispisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。)
・特定の個人を識別することができない統計情報

10

図3.「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（概要）」
出典:経済産業省 商務情報政策局 情報経済課 より抜粋

しかしながら、仮に「暗号化してあれば個人情報として取り扱わない」としても、その暗号化の方式として、「秘密分散(共有)を施してあるから大丈夫だ。」という認識については、必ずしも適切ではない。

なぜなら、「秘密分散(共有)」の仕組みを数式で表すと、以下のようになる。(図4、図5)

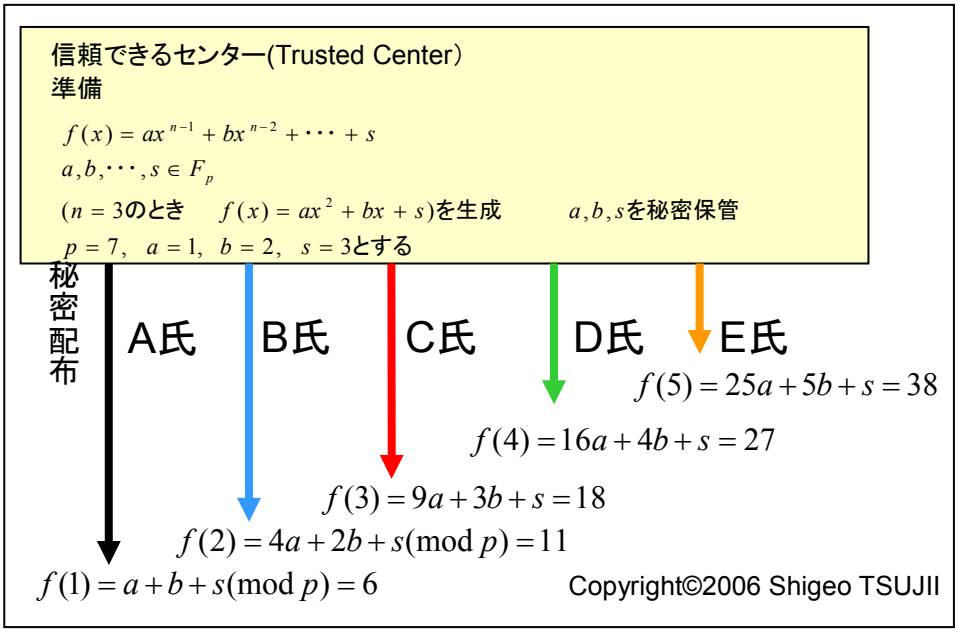


図4.「秘密分散(共有)」の数式

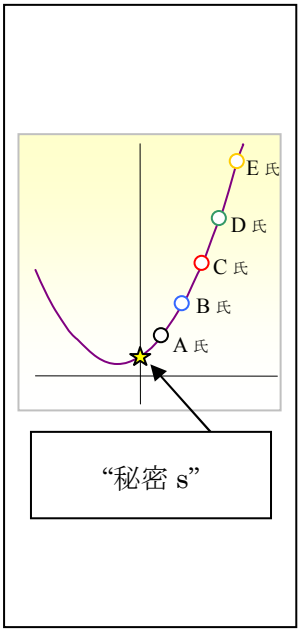


図5. 参考グラフ

詳細な説明については割愛するが、ここで一番重要なのは、”秘密 s”そのものを分けていないことである。確かに”秘密 s”に乱数を足してはいるが、それらはお互いに相関があり、何人かが(上の例では3人)が集まると解けてしまうのである。更に、1度”秘密 s”の値が分かれば、この暗号化をする意味がなくなる。つまり1回しかその有効性はないのである。

また、「個人情報データ」というのは基本的にデータベースに蓄積されるものであるが、通常は1人1人の暗号鍵を管理する際にも同じデータベース内に格納している。しかしデータベースを解読されたり盗られたりしてしまっては、その暗号化自体が無意味なことになってしまう。

やはり、重要なものはきちんと分けて暗号化し、それを個別に実施し、万が一解読されたとしても、限られた情報しか被害を受けない、ということにしないと安全性は向上しないのである。

「データジグソー™」の場合、まずデータを分割して暗号化している。つまり、“姓(例:山田)は見られても、名(例:太郎)は見られない。住所(例:東京都○○区××・・・)は見られない。”という特徴がある。
分割の単位もメタデータ単位・フィールド単位といった格納物単位に縛られるだけではなく、文字単位まで分割できるように設計されており、「秘密分散(共有)」に比べて安全性が格段に高いと考えられる。

更に、「データジグソー™」の場合は、その暗号鍵ごとデータベースを解読されたり盗られたりした場合に備えて、別プロセス・別方式で管理している。
その方式も単純ではなく、いくつもの解析方法を組み合わせないとできない、という方法を実施してある。重要な鍵を金庫に入れて、その鍵を某銀行の貸し金庫に預けるようなもの、と例えたら分かり易いであろうか。
リスクを分散するという手法は私達の普段の生活においても安全性を高める為に行う。通帳と印鑑は分けて保管しておきましょう、という概念である。

この一連のシステムを一言で表すのであれば、メディアスティック社が提唱する「分割多重暗号化方式」という新たな手法であると言える。

これらを実施する際には「SSL通信」(*4)を用いていることは勿論のこと、共通鍵についても、アメリカ政府が認定した世界標準暗号化方式を使っており、それだけではなく、日本の評価機関である“CRYPTREC” が認定した「電子政府推奨暗号リスト」(*5)に認定された「Camellia（カメリア）」(*6)などの日本で開発された方式も使うことができるように設計されている。

よくアメリカの方が暗号技術は進んでおり、日本の暗号技術が遅れているように言われるが、決してそうではない。ISO（国際標準化機構）において暗号標準が14種類で現在決定しつつある。そのうち少なくとも4つが日本製になりそうなのである。

「データジグソー™」は、将来的に更に強力かつ安定的・国際標準的な暗号方式が開発された場合、もしくは現在使われている共通鍵に脆弱性が発生した場合においても、速やかに対応できるように設計されてある。

このように「柔軟」かつ「分割多重暗号化」されたシステムは、世界的に見ても優れている。
更に付け加えると、本システムを運用するに際して個人情報の取り扱いについて法的にも考慮しているスタンスは、国際的にも着眼点が早かったのではないか。

「データジグソー™」の元となった「モバイルメタデータベースシステム」は、

- 2001年度　経済産業省・IPA（情報処理振興事業協会）の「先端的・戦略的ソフトウェア」開発支援事業
- 2002年度　内閣府・e-JAPAN「電子政府情報セキュリティ技術開発事業」
- 2003年度　経済産業省・IPA「重点領域情報技術開発事業」

に選定されたものであり、国際特許として米国・欧州に認可されている。その先見性と有効性は日本国内だけではなく、国際的にも客観的に認められており、培ったノウハウは「データジグソー™」にも引き継がれている。

以上の理由により、「データジグソー™」は、重要な情報を分割して管理しており、復号化した際に全てが分かるのではなく、断片的な情報しか取得できないという点において、「個人情報保護法」に対応しているシステムである、と言えるのではないだろうか。

(*4) (*5) (*6) P.10 参照

4 付録

4.1 工業所有権等

US(米国)特許	名称:Method and Apparatus for Retrieving Data (データ検索の方法および装置) 出願番号:08/904,149 出願日:1997 年 7 月 31 日 出願国:US 特許日:2000 年 10 月 24 日 名称:Integrated Database Systems (統合データベースシステム) 出願番号:08/904,274 出願日:1997 年 7 月 31 日 出願国:US 特許日:2001 年 7 月 31 日
EP(欧州:フランス、 ドイツ、イギリス)特許	名称:Integrated Database Systems (統合データベースシステム) 出願番号:0822505 出願日:1997 年 7 月 31 日 出願国:FR、DE、GB 特許日:2005 年 2 月 9 日
国内特許(出願済)	出願.....18件 請求項の数.....139件 システム関連特許 .....59件 セキュリティ関連特許.....13件 ビジネスモデル関連特許 ..67件
国際特許(出願済) 2001 年 3 月 9 日、 2004 年 5 月 19 日	出願.....PCT2件

4.2 主要開発陣 略歴

北川 高嗣 Takashi Kitagawa (工学博士)

筑波大学大学院システム情報工学研究科教授 (専門分野:メディア情報システムデザイン)

名古屋大学大学院博士課程(情報工学専攻)修了。スタンフォード大学コンピューターサイエンス科学科客員研究員、筑波大助教授などを経て現職。情報科学と数学との学際領域を専門とし、コンピュータを媒体として、人間の表現と認識の問題をテーマとする。
次世代情報社会・産業関連プロジェクト、領域横断型プロジェクトに多数参画。放送大学大学院客員教授(2000 年～現在)、慶應義塾大学理工学部(1994 年～現在)、東京大学工学部(1997～98 年)にて非常勤講師・併任講師を務める。

＜委員歴＞
コンピュータ数学に関する国際会議(ISCM 90)、「数学と情報学に関する国際会議」(HERMIS 94)組織委員、応用数理学会論文誌編集委員(1992～)、「情報学辞典」編集委員(東大情報学環他、1997～)、「4次元メディア研究会」委員長((財)海洋都市開発研究会、科学技術庁、1996～1998)、「放送経済研究会」委員(郵政省、1997～1999)、「2030 年委員会」委員(通産省、1998～1999)、「マルチメディアコンテンツ流通委員会」副委員長(通産省、1998～2000)、「モバイル街研究会」委員(2000～)、「ネットワークヒューマンインターフェイス研究会」委員(総務省 2002～) 他多数

辻井 重男 Shigeo Tsujii (工学博士)

情報セキュリティ大学院大学学長 (専門分野:情報通信・情報倫理・情報セキュリティ)
CRYPTREC 暗号技術評価検討会メンバー (暗号技術評価委員会元顧問 暗号技術評価検討会元顧問)

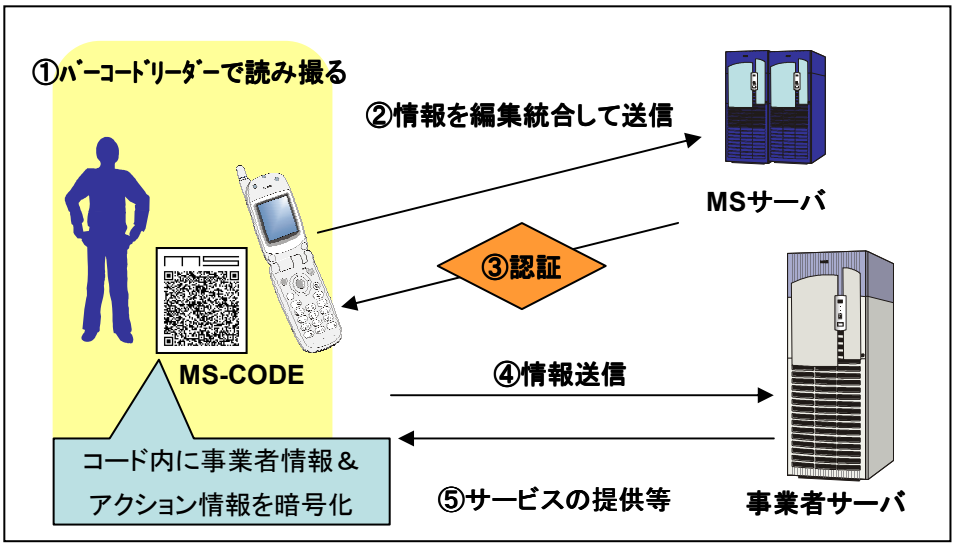
1958 年 東京工業大学電気工学課程卒業。同年 日本電気株式会社入社。1971 年 東京工業大学助教授。1978 年 東京工業大学教授。1985 年 郵政省電気通信技術審議会委員。1991 年 東京工業大学評議員。1992 年 東京工業大学図書館長。1994 年 東京工業大学名誉教授。同年 中央大学理工学部教授。1996 年 10 月～2002 年 12 月郵政省(総務省)電波管理審議会委員 2000 年 12 月～同会長。2002 年～CRYPTREC 暗号技術評価委員会顧問・暗号技術評価検討会顧問(現:暗号技術評価検討会メンバー)。2003 年 7 月～日本学術会議会員。2004 年 4 月より現職。

＜受賞歴＞
関東地方発明表彰(色彩テレビジョン符号変調方式・(昭和 46 年度)、郵政大臣個人表彰(昭和 49 年度)、日本エリクソンコミュニケーションアワード(平成 11 年)、米国電気電子学会(IEEE)3千年紀記念賞(平成12年)、第55回 NHK 放送文化賞、電子情報学通信会

論文賞、著述賞、功績賞

4.3 語彙説明

「モバイルメタデータベースシステム」

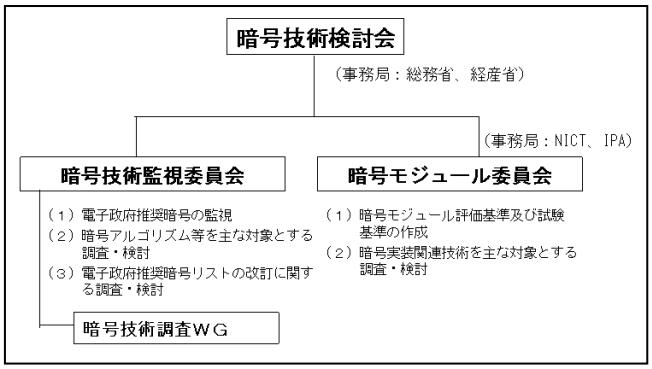


メディアスティックが「IT ストレスフリー」を目指し開発した。
e-Japan の「電子政府情報セキュリティ技術開発事業」に選定され開発されたもので、客観的に極めて高い評価を受けている。
「データジグソー™」は、本システムをベースに開発された。

「SSL(Secure Socket Layer)」
Netscape Communications 社が開発した、インターネット上で情報を暗号化し送受信するプロトコル。プライバシーに関わる情報やクレジットカード番号などを安全に送受信することができる。

「Camellia(カメリア)」
NTT と三菱電機が共同で 2000 年に開発した共通鍵ブロック暗号。欧州推薦暗号選定プロジェクト NESSIE において「米国政府標準暗号 AES と多くの点で同等の安全性と性能を有している」と評価されるなど、国際的にも認められている。現在では、AES と同等の安全性・処理性能を有しているほぼ唯一の暗号として国際的にも認知されつつあり、多くの国際的な標準暗号・推奨暗号に選定されている。
日本国産暗号としては、初めて IETF 公式標準暗号(Proposed Standard RFC)として承認された。
http://info.isl.ntt.co.jp/crypt/camellia/intro.html

「CRYPTREC(Cryptography Research and Evaluation Committees)」
電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト。
総務省及び経済産業省が共同で開催する暗号技術検討会(座長:今井秀樹東京大学教授)と、独立行政法人情報通信研究機構(NICT)及び独立行政法人情報処理推進機構(IPA)が共同で開催する暗号技術監視委員会(委員長:今井秀樹東京大学教授)及び暗号モジュール委員会(委員長:松本勉横浜国立大学教授)で構成される。
http://www.cryptrec.jp/index.html



「電子政府推奨暗号リスト」
CRYPTREC の暗号技術検討会において、暗号を公募の上、客観的に評価し、「電子政府」における調達のための推奨すべき暗号(電子政府推奨暗号)のリスト(電子政府推奨暗号リスト)が決定された。各府省は、情報システムの構築にあたり暗号を利用する場合は、可能な限り、同リストに掲載された暗号の利用を推進する旨が、 各府省の情報システム調達における暗号の利用方針として合意されている。
http://www.soumu.go.jp/joho_tsusin/security/cryptrec.html#01

リストの抜粋 [技術分類]-[共通鍵暗号] (平成15年2月20日 総務省・経済産業省) http://www.soumu.go.jp/joho_tsusin/security/img/cryptrec01.pdf				
64 ビットブロック暗号	CIPHERUNICORN-E	Hierocrypt-L1	MISTY1	3-key Triple DES
128 ビットブロック暗号	AES	Camellia	CIPHERUNICORN-A	Hierocrypt-3
ストリーム暗号	SC2000	MUGI	MULTI-S01	128-bit RC4

２００６年２月１日　初版発行

本資料のお問い合わせ先

メディアスティック株式会社

クロスメディア・ソリューション事業本部

TEL:０３－５４７５－５０１５
FAX:０３－５４７５－５０１６

http://www.mediastick.co.jp/
e-mail：info@mediastick.co.jp

〒150-0012
東京都渋谷区広尾五丁目８番14号９階
（東京建物広尾ビル）