Vol.2011-IS-116 No.3
2011/6/6

電子割符の先進社会基盤適用モデル

保倉 豊[†]　　川城 三治[†]

電子割符の技術的特長を活かした電子情報の不滅化システムの提案、及びその構成方法について述べる。本提案システムが大災害時においても有効な機能を示すとともに、その社会的電子情報シェアマネージメント手法及びそのシステムの確立方法と運用などの適用モデルを示す。さらに、社会基盤システムを実現した際の今日の法背景に対する若干の提言を行なう。

An Information System for a new Social Model using e-Tally

Yutaka Yasukura [†]　and Sanji Kawashiro[†]

This paper describes an information system for a new social model using e-tally. The main feature of the system is e-tally based on Threshold Secret Sharing Scheme. In the case of disaster where electronic data are destroyed or disappear, the system can recover the original electronic data. Also the managing procedure and some legal considerations of this system are described.

１．はじめに

我々は、電子データ自身の安全性をいかに確保すべきかを主たる対象として研究開発を継続して行い、電子割符という技術を創出して、本学会の研究会でも報告してきた[１]。原本の電子データのビットの並びが残存しない状況の電子割符を作り出し、更に一部を重複して各割符ファイルに所有させることで、数学（暗号）理論の秘密分散法で言う閾値設定した姿と同様な機能を持たせることができる。その際、重複させたとしても、その重複部分自体も原本情報そのものでは無いため、単体からは事実上原本情報が流出しない。また、復元が成功する場合は、処理対象の原本と同一の電子データに戻ることが特長。ここで言う電子データとは、現状社会においては情報資産や要機密情報等を指している。

電子データはバックアップをしても災害等で消失あるいはアクセス不能になる可能性がある。ここでは、電子データを電子割符化して分散保存し、その電子割符が災害等で消失あるいはアクセス不能になった場合にも、電子割符の技術的特長を活かした電子情報の不滅化システムを提案し、その構成方法について述べる。さらに、本提案システムの社会的電子情報シェアマネージメント手法及びそのシステムの確立と運用について、これまでの我々の調査研究活動の中で浮き彫りとなった課題と、上記社会基盤システムを実現した際の今日の法背景に対する考察についても述べる。

２．電子割符の特長と現状

電子割符は、電子データの基本的性質を利用した新たな情報運用管理を実現する技術。電子データは、０と１（デジタル）の組み合わせで様々な情報を表現しているので、その０と１のビットの並びが正しくなければ、本来の表現したい内容は表現できなくなる。この特長を活かしたのが一般的な暗号技術で、原本となる電子データを決められた法則に従い対象情報の全変換処理を行いますので、正しく逆変換すれば原本に戻る。電子データのもう一つの特徴は、０と１の組み合わせで何らかの表現をしているのであるから、その０と１（情報）が不足してしまえば、元の表現したい内容を表現できない。よって、原本の電子データを、ビットレベルでばらばらにしてしまい、それらをいくつかの塊にまとめることで、簡単には原本情報を類推することもできない状態を作ることができる。電子割符処理概要を図１に示す。

[†] グローバルフレンドシップ株式会社
Global Friendship Inc.

Vol.2011-IS-116 No.3
2011/6/6

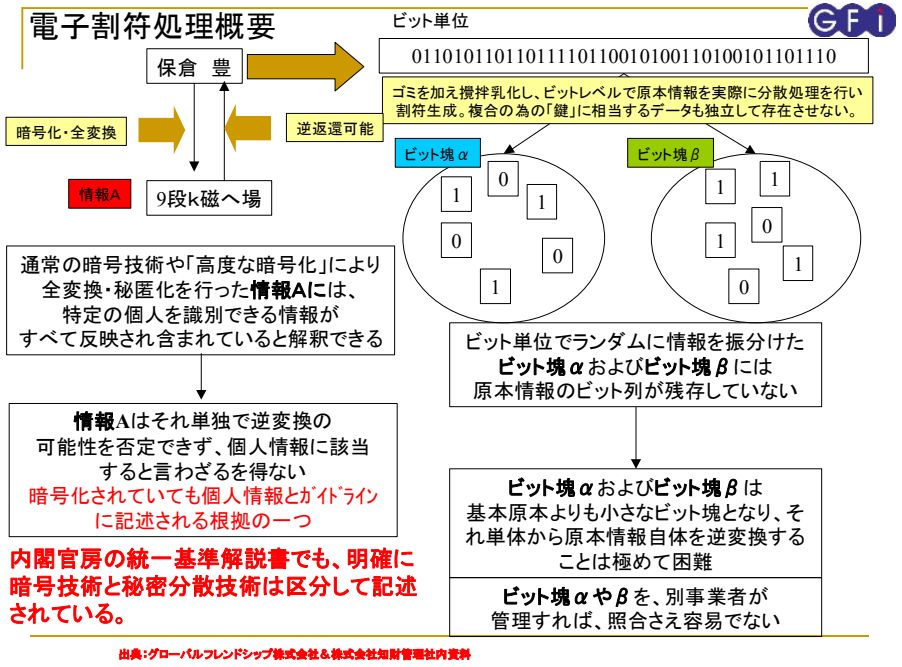

図 1　電子割符処理概要
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

割符は、正当な割符の相手が集まれば原本復元に必要な０と１のビット（情報）を揃えることができるので、原本に復元できる。つまり上記処理をした割符を関係当事等に付与すること自体が、原本情報復元に対する一種の認証であるとも言える。

この原本情報を欠損させることでの原本情報の保護機能を更に拡張させ、それらの原本情報が完全に残っていない割符ファイルの一部を重複させる等の工夫をすると、一部の割符が消滅してしまっても、残りの割符で原本情報を復元させること（リカバリー）の道筋が出来る。原本情報を欠損させることで個々の生成された割符ファイルからの原本情報漏洩の危険性を最小限にしつつ、その一部を重複させてそれぞれの割符ファイルに保有させるような仕組みを作ることで、実社会で発生するＰＣの故障や紛失といったことにも対処できるデータ管理ができるようになる。因みに最新の電子割符では、Ｎ－２個での復元も可能な機能を標準で実装している

この際、通常の暗号やレイド５などの一般的な既存手法で考えると、原本データと同じビット長の補完データが必要になり、その補完数によっては原本情報の何倍ものデータを管理する必要が出る。今後ますますデジタルコンテンツがリッチになっていく潮流からすると、大きな経済的、システム的負荷をかけ続けさせることになる。更に、通信環境や記憶メディアの容量等を鑑みると、原本と同じ大きさの電子データを移動させるのは、スマートな手法ではないと言える。

上記のような非常に簡潔な原理を元にした電子割符は、MEDIS実証事業での採用を皮切りに、民間での商用化に加え、総務省の「個人情報保護強化技術実装システムの開発・実証プロジェクト」での採用[２]、内閣官房情報セキュリティセンタの「政府機関の情報セキュリティ対策のための統一基準解説書」での利用シーンの具体的記述[３]を経て、電子割符を元にした秘密分散技術の定義と法律家の意見書を添えた公的調査報告書[４]が公開されるに至っている。

最近の電子割符技術は、復元時の条件を設定することも可能になっており、時間や場所、その他の複合や運用管理上の諸条件を設定して割符処理を行なうことで、例え復元に必要な数の割符ファイルを犯罪者等に糾合されたとしても、容易に復元させない機能も付いている。非常に特長的なのは、この技術は特定の数学理論（暗号理論）を根拠としていない、ありふれた手法と情報処理技術の組み合わせで構築されており、暗号技術として国際的には認知されていないが、日本で生まれた特長ある情報運用管理を実現するための基礎技術として認められている工学的成果である。

一方留意点としては、純粋な暗号技術の場合は、「完全秘匿」というレベルの秘匿性を付与することができるが、電子割符はそこまでのレベルのものではなく、不足している割符ファイル（ビット）を補完できれば復元可能性が発生する。つまり、「完全秘匿」を可能とする暗号技術の場合、社会保障上の観点から実社会に流通させてよいかの判断が純粋な技術としての良し悪しとは別に必要になるが、電子割符は、「完全秘匿」に至らない技術なので、一般市場での流通に阻害要因が少ない。

３．災害時における情報の消失の課題

これまでもアメリカ同時多発テロや個人情報への関心が高まる中、ＩＳＭＳ等で電子データのセキュリティに関して様々な論議がなされてきた。情報セキュリティの世

界では、ＣＩＡと言う表現が一般化している。Ｃとは、Confidentiality：機密性、Ｉとは、Integrity：完全性（保全性）、Ａとは、Availability：可容性で、その根底に電子データであるが故の脆弱性の問題と、それらを超越した課題とが横たわっていることが知られており、米国では連邦政府レベルのＢＣＰ（事業継続計画）やＤＲ（災害復旧）のガイドラインも策定されている。[５]

本年（２０１１年）３月１１日に発生した東北地方太平洋沖地震（東日本大震災）は、巨大地震、大津波、火災、そして原発事故（ＩＮＥＳ 評価レベル７）を引き起こした。被災地報道で海外を含め多くの人々にその惨状を見せつけた。我々の記憶にも近年の大規模震災や大水、火山活動等の壊滅的被害は生々しく残っている。日本が地理的条件等を踏まえれば人為的な事故だけではなく、本当の意味での災害の一つにこのような巨大な自然災害も含まれると覚悟すべきと考える。

今回の災害に対する政府発表を見ても、情報消失に関連した特別措置が急遽行なわれた事象が多い。これは前述の電子データの脆弱性に直接関わるリスクが顕在化したことを意味しており、本来であればそこでＢＣＰが実行され適切な対応を即実行されるべきところであった。その部分のリスク管理や対処に関する評価は、別な場所で行なわれるのを待ちたい。災害時の情報消失の課題としては、実社会を混乱させないための重要情報も、紙であろうと電子データであろうと今回の災害では一瞬にして滅失させた。我々は、同じ過ちを繰り返すことをいい加減に食い止めるべくアクションを起さなければならないと考える。

国家的課題として、同一地域や他地域において、災害時の情報消失による社会機能混乱を繰り返さないことが重要である。
その対象となる情報の種類を区分すると以下のようになると考える。
１、活動を継続させるための情報・資料等
２、サービスを継続させるための情報・資料等
３、個人・住民が必要とする情報（思い出含め）
更に、上記情報に関して、以下の観点で保全等を進めるべきである。
１、紙であれば電子化し、消失対策を施す
２、電子データであれば、消失対策を施す
３、これまで無かった情報を電子化して消失対策を施す

恐らく、「これまで無かった情報を電子化して消失対策を施す」の項が気になると感じるが、今頭に浮かぶ具体的な情報の一例は、「究極時の本人特定情報」に関する国家的な、安全安心な運用管理である（これについては５章で述べる）。

災害発生時に、対処に必要な情報が消滅している状況は、対処までの時間を長引かせ大きな社会不安と被害の拡大を招く。このような事態を繰り返すことを決しておこなってはならない。

４．電子情報の消滅防止の技術

これまでも官民問わず、様々な電子情報が消失防止対策を施してきたが、どれも今回のような大規模な災害には弱いと言わざるを得ない。特に、対象の情報が秘匿性を高めなければならない場合や、唯一無二のマイクロフィルム等といった場合である。なぜなら、そのような情報は、コピーをとること自体がリスク増大やその手法を選択したことに対する矛盾に直結してしまうからである。既存の情報消失対策は、これ以上は仕方が無いだろう。という諦めの上に成立していたというべき対策であり、ここに今回の災害の教訓を踏まえ、新たな消滅防止策を具体化する意義がある。古来、形あるものは壊れる。として人類普遍の真理としてきたが、新たな電子情報の消滅防止の技術として我々が提案するのは「不滅信用点」である。

実際に不滅の点を創出することのアイディアは無い。しかし、電子データの運用管理を受託し、その預託された電子データを不滅≒永遠に近い状態で、情報改竄や漏洩を防止して、社会に信頼される運用管理を実行する仕組みを作ることを指し、そのサービス主体は複数の責任主体で構成し相互運用管理されており、点という表現は、サービスの名称としてここでは次のように定義する。
１、長期間安定したサービス提供を行う。
２、受託した電子データ管理において、過去の消滅防止策のように、そのまま預かるのではなく、冒頭の電子割符の技術的特長を活かし、運用管理する。
３、不滅信用点は、複数の責任主体により構成され、それぞれが割符を管理し、相互監視する形となる。
４、ユーザーへの対応フロントサービスは、どの責任主体に問うても同じ回答になるよう設計され、所謂不滅信用点サービスは、一極集中の運用管理ではなく、あくまで概念として存在し、預けた実体は割符処理され、当該サービス提供を行う独立した個々の責任主体に再預託される。
５、更に第三者委員会を設置し、内外部でのファイルの受け渡し等に疑わしい動きが無いかを監視・指摘し、改善徹底し報告書を公表する。
上記５項の第三者委員会の外部監査機能は、システム的には面白くないかもしれないが、社会システムとして捉えた場合には、今後必要不可欠な体制と考えられる。以下、電子割符を用いた不滅信用点の仕組みに関する説明をする。

図２は、電子割符を用いたデータ消滅防止の仕組みの原型を示す。対象データの運用管理主体が、対象データを、α、β、γの３個に分割する、３－１型の割符生成を行い、消失防止対策を行なった状態を示している。割符αは、管理主体の社員証等に格納する。βは社内サーバー等に格納する。残りのγをネットワーク上のストレージに預託する。しかし、大規模災害が発生すると管理主体と同時に組織のサーバーも消滅する可能性があり、その場合は、３－１型の割符であっても二つの割符が消滅してしまう為、原本を復元できなくなる。しかし、個々の割符単体では原本情報が出てこない特性を鑑みると、αかβをコピーして、図３に示すように、クラウド等の安価なネットワーク上のストレージやメディアに記録し、地域を分散して保管することが考えられる。この場合には、他の割符が入手されないのであれば、原本情報漏洩等のリスクが容易に顕在化しない特長が効果を発揮する。

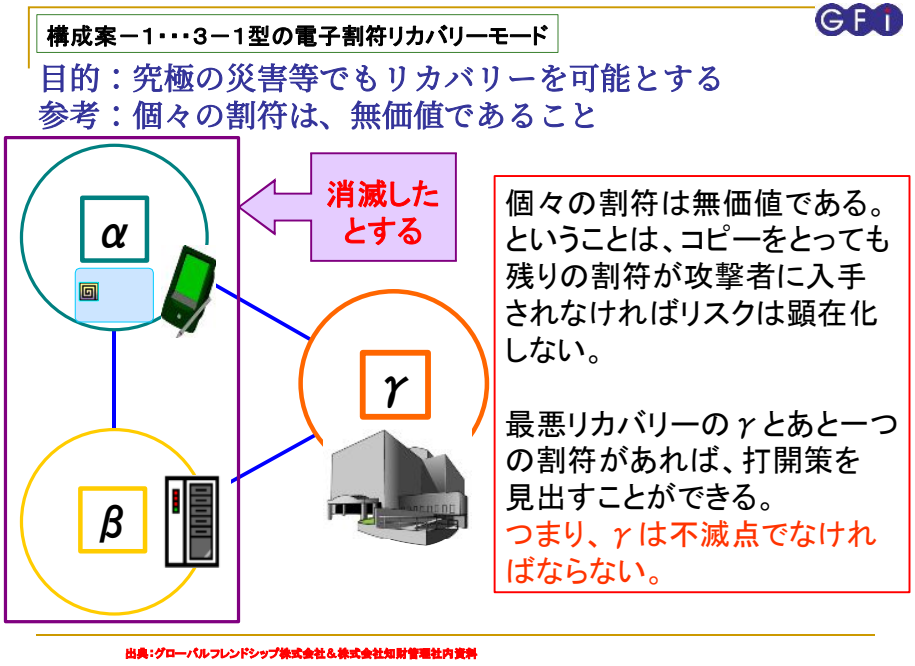

図 2　構成案－1
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

この状態で、γが確実に存在すれば、αまたはβを用いて原本情報を復元できる。ここで課題になるのが、γが本当に存在していないと困るということである。万が一、ＩＤＣ等の地域の選択が悪く、同時災害を被って、γが消失した場合にはこの対策が無意味になってしまう。すなわち、図３に示すような、単なる外部データストレージや信用点といった方法では、大災害時のデータ消失には万全とは言えなくなる。

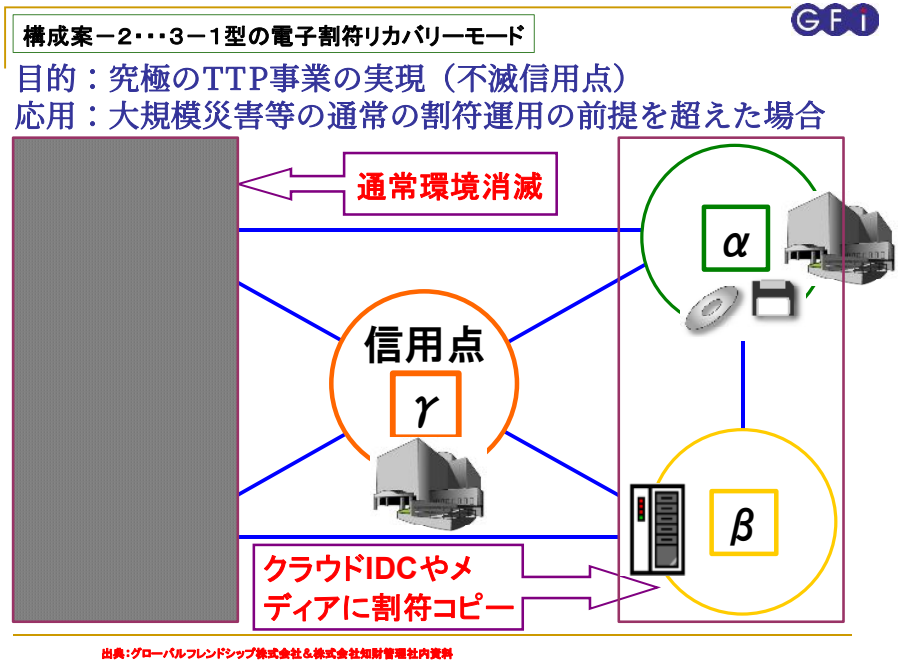

図 3　構成案－2
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

ここに、新たな解決策として「不滅」が付く、「不滅信用点」を提案する必要が出てくる背景がある。図４は、５－２型の割符機能を利用して、不滅信用点を介在させる電子割符リカバリーの構成例を示している。不滅信用点は、データ（割符γ）の預託者からその割符の運用管理を受託すると、自らを連携して構成する外部の責任主体に対して、受領した電子ファイルを再度割符処理して、自らは一つ持ち、残りの割符はそれぞれに一つづつ預託する。この場合の、割符のリカバリーモードの設定は、自

由であるが分割数があまりにも多くてもハンドリングが難しいと考えられるので、そこは留意しつつあとは閾値をいくつにするかを決定することになる。

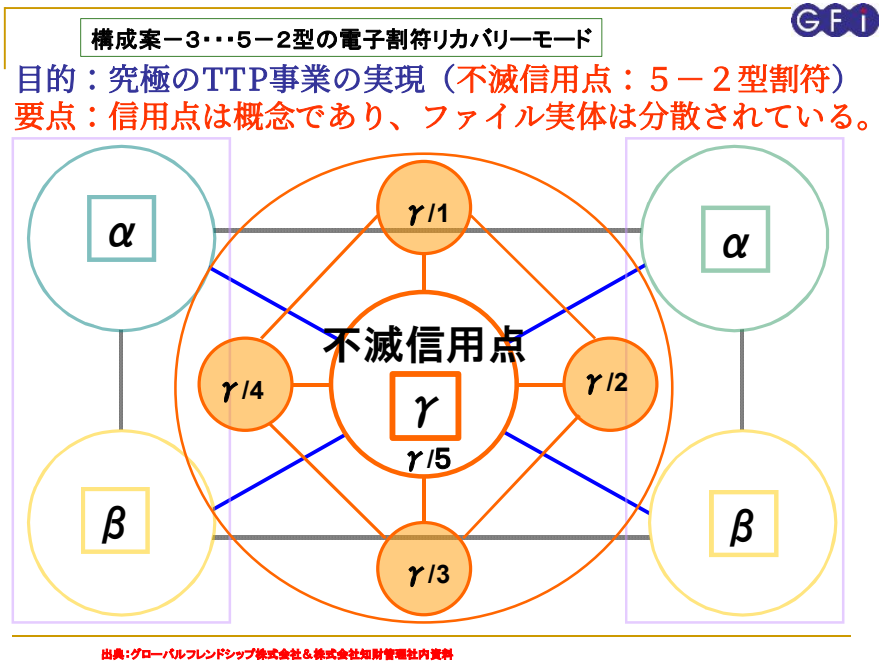

図　4　構成案－３
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

更に、純粋なＩＴシステムとしてだけ捉えるのではなく、実社会で有効に機能する社会基盤として考え、不滅信用点の情報交換等を第三者に監査させることを強く推奨する。あるいは、αやβ自身も再度割符処理することもできる。

この不滅信用点に関しては、異なる責任主体が運用することとするが、その主体の役割を、図５に示すように、分野ごとに区分けすると、各主体が相互に牽制しあう状況を意識的に作ることを推奨する。この図で示したように、各分野の構成信用点を統合する不滅・構成信用点を構成すると、情報毎に信用点が整理されるので国民も混乱しないのではないかと考える。　図４に示したβも構成信用点に預託する仕組みとなるが、αは当事者の管理として、あくまで自らが責任主体であることの動機付けをさせると共に、今後議論が再燃するであろう「自己情報コントロール権」の管理にも資する仕組みとする。

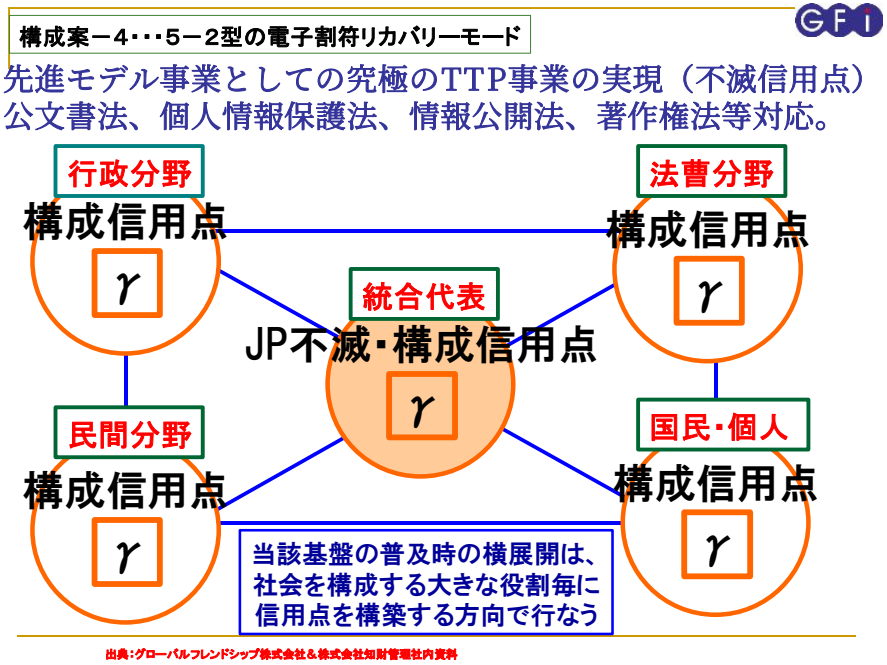

図　5　構成案―４
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

他方、当該不滅信用点は国内に限った内容ではないので、国際的な連携も視野に入れて設計することが望ましい。更に、電子割符の特長の一つでもある、復元条件の指定機能を併用すれば、安全安心な社会基盤を構築できると考える。この仕組みを日本発で海外に提供できる新たなサービス事業として展開すれば、日本の新たな世界貢献の姿にもなろう。この社会基盤のモデルの例を図６に示す。

Vol.2011-IS-116 No.3
2011/6/6

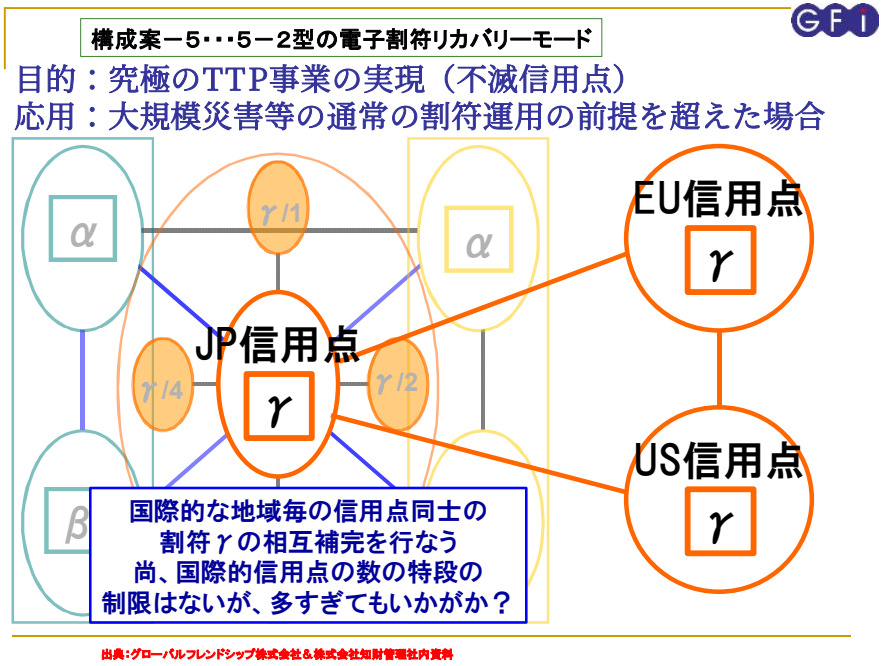

図６　構成案―５
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

５．今後の電子情報の運用管理に対する提案

この論文を記述するにあたり、東日本大震災のことが大きな契機となったのは偽らざる事実である。３章で後述するとした、「本人特定情報の国家的運用管理」を例にして提案をしてみたい。

被災地で一番我々国民の心を揺り動かした光景に、被災者の方々のご遺体に関するＮＥＷＳ映像ではなかっただろうか。ここで憲法論議をする考えは無いが、日本国は、国民に対して、健康で文化的な最低限度の生活を営む権利（２５条）を保障しているはずで、個人として尊重され、生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とされてるいはずである（１３条）また、財産に関する権利（２９条）も保障されているはずである。海外での災害でも、邦人救出等ではどうしても本人確認・特定が必要になる。国家として国民の生命と財産を守るための基本情報を管理していなくて、どうするのか。

今頭に浮かぶこの不滅信用点を組み入れた新たな社会基盤で運用すべき具体的な情報の一例は、「究極時の本人特定情報」に関する国家的な、安全安心な運用管理だと考える。基本的な仕組みは前述までのとおりであるが、その時に使用する本人特定情報のファイルイメージの例を図７に示す。

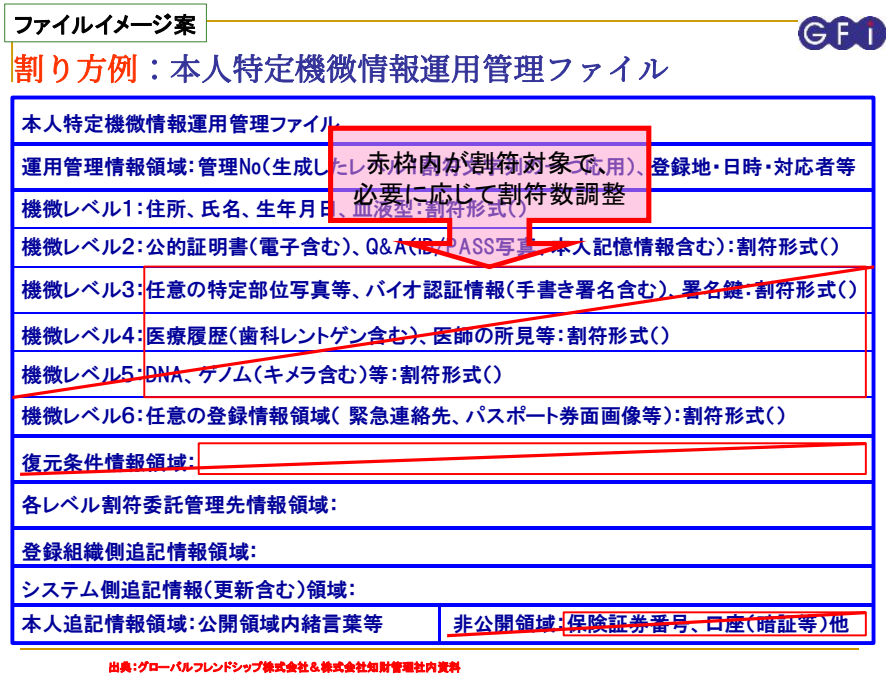

図７　ファイルイメージ案
出典：グローバルフレンドシップ株式会社＆株式会社知財管理

個人情報等の適切な運用管理を可能とする、国民と日本国政府とが相互信頼できる情報管理を可能としたシステムについて述べる。

基本要件：
１､究極の本人特定から日常軽微な本人確認まで適応できる情報管理を可能とする。
２､緊急時に役立つと本人が選択した情報を､安全安心に運用管理できる情報基盤。
３、本人希望の行政発行のＩＣカードに、機能付与させることを可能とする。

システム概要：
１、公開領域と非公開領域（割符数や開示条件で複数設定）を電子割符機能の特長を用いて設定し､非公開領域の情報は少なくとも３－１型で対象情報を分割し、運用管理する。
２、割符の一つは、本人管理（ＩＣカード)、他の一つは、個人情報に関する第三者機関に預託し、残りは、本人の任意の第三者機関に預託する。
３、更に、個人情報に関する第三者機関が設立できれば、不滅信用点での割符開示要求等の状況や履歴を継続的に監視することで、不正な国民からの預託情報の使用等の未然防止を行い、疑わしいアクセス等のある場合は、徹底的に調査し情報を対象個人情報を除き範囲公開し、不正行為等があった主体等に対し、厳しい罰則が適応されるよう関係省庁に申し送りをする。
注：ＥＵ指令対処も含め、申し送りされた事案は法に則り罰則が下るようにする。そして、日本とＥＵとの個人情報に関する理解度の溝を埋めることに寄与できる。

先般の震災における現地混乱等も念頭に置きつつ、以下の適用対象を提案する。
１、大規模災害時の邦人確認に必要な、ＤＮＡや人ゲノムを含む最高度の本人特定情報を運用管理する国家的社会基盤。
２、国民ＩＤ等の社会基盤や名寄せシステム等のキー管理への応用。
３、民間営業機密やＳＯＸ関連情報等を含む法的証拠保全が必要な情報への応用。
４、公文書を含めた、国家的情報管理への応用。
５、著作権対象情報や個人プライバシー関連情報への応用。

法的提言としては、以下のとおり。
１.国家として究極の本人特定に資する社会基盤を､関係法を成立させ整備すべし。
２．法的原本として電子データを全ての法規に関して認めるべし。
３．個人情報に関しては、信用第三者機関を設置し、本提案の不滅信用点を監査させることとも含めて法制化すべし。

二度と身元不明のご遺体が出ないような社会にすべきである。次に、過去の法体系で紙を原本とする法律の運用を、電子データを原本とすることを正式に認め、ある年度からはすべて電子データを原本とする社会作りを行ない効率化と現場の混乱を解消するべきである。また、同じ過ちを繰り返さない為に、前倒しで既存の紙原本は電子化を強く推進させ、新たに社会基盤構築等を行なう場合は、最初から本提案のような災害に強く且つ、プライバシーも保護できるような仕組みで、運用管理することが望ましいと考える。そして、ＥＵとの会話をまともに行うためにも、体制、法体系、システムとしても大きく見直しを行なうべきである。

最初から電子データを原本として扱う社会であれば、裁判等でも原本の内容に集中すればよく、現代の紙原本のような、その現物に隠れる事実を読み取るといった途方も無い労力を裂く必要も無くなる。その代わり、契約書なら契約書の締結されるまでの過程といった部分も合わせて、電子化して証拠保全することが組織としての基本になると考える。よって、本提案の電子割符の技術的特長を活かした社会基盤で原本情報を運用管理することで、都合の良い改竄等が事実上できなくなる特長を活かし、法的な意味での電子データの証拠保全も実体として兼ねることも強調したい。

６．　おわりに

人類の歴史は、情報管理の歴史だったとも言える。原始時代には壁画、粘土板に楔形文字、亀の甲羅に甲骨文字、文字の進化もありましたがメディアは更に、石版、羊皮、木簡、パピルス（紙）へと進化し、過程で暗号や割符や勘合符といった情報保護措置に関する工夫も生まれ、現代はデジタルメディアに二進法０と１のデジタル言語と暗号技術等が情報を集中管理している。しかし犯罪者はその集中管理されたポイントを攻めることで効率的に犯罪を犯す。情報もリスクも責任も分散させることが今後の社会システムに必要な観点であると、警鐘を鳴らすものです。

参考文献

1) 保倉　豊、川城 三治：「電子割符」のデジタル社会への応用、情報処理学会研究報告. EIP, [電子化知的財産・社会基盤] 2000(56), 19-25, 2000-06-02
2) 総務省個人情報保護強化技術実装システムの開発・実証プロジェクト報告書：平成 18 年 3 月
3) 内閣官房情報セキュリティセンタ:「政府機関の情報セキュリティ対策のための統一基準（2009 年 2 月版［第 4 版］)」
4) ECOM　2009年度情報セキュリティＷＧ成果報告書「ECにおける情報セキュリティに関する報告」秘密分散技術検討ＴＦ
5) JETROニューヨークだより2006年5月、事業継続対策コンソーシアム報告書

その他、首相官邸、内閣府、国土交通省、総務省、経済産業省、警察庁等のＷＥＢで公開されている情報も参考とした。