3G-7

秘密分散技術（電子割符）の標準化提言ー市場先行事例調査結果を受けてー

保倉　豊†　　川城三治‡
グローバルフレンドシップ株式会社†　　グローバルフレンドシップ株式会社‡

１．はじめに

電子割符は電子データに対する簡明な処理手法の技術総称であり、近年集合論や秘密分散法（1）を技術評価上の理論的背景とした秘密分散技術と呼ばれる新たな基礎技術となってきている。この手法は高度な数学的知識の無い者でも理解し易い技術で、人類の叡智である割符を根源とした実社会で使用できる工学的な技術研究成果と言える。当該技術は対象となる電子データを実際に分割してしまうことで、原本情報全体に対する原理的な秘匿性を最初から備えており、更にその分割方法等を工夫すれば秘匿性を向上させることや、データリカバリも可能となる技術である。これを適切且つ健全な利用モデルで市場普及させることが社会安全保障等の観点からも重要である。特に中・長期の耐用期間中、利用者が安心して技術やサービスを利用し続けることができる技術標準化が必要である。東日本大震災発生以降、当該技術の持つ基本的な特性が広く社会に有用であることが認知されるに至り、市場要求を踏まえ同技術の認定・登録主体の設立も含め標準化の提言をする。

２．電子割符の特徴

特定の他の技術に大きく依存せず、あくまで保護対象の電子情報自体（原本）をビットレベルで分割し、更にランダムに複数の割符ファイル（分割片）に割り振ることで、個々の割符ファイル（分割片）単体からは原理的に原本全体を復元できない処理を行なう。この結果原本に対し割符単体は情報量が不足した状態となり、割符ファイル単体は原本に対し集合論で言うところの部分集合に相当する形となる。この電子割符の基本的特性が実社会に幅広く応用できることは文献（2）で述べている。また閾値を設定した電子割符が、災害時に流失・消失した場合の情報復旧に有効な手段となることを文献（3）で述べている。更に、他の要素技術への依存度が低く、暗号技術やＩＴ技術との併用等の親和性が良いことも特徴である。良く比較される既存暗号技術とは根本から異なる特性を持つ。参考まで双方の特徴等を比較する。一般に利用される暗号は、原本を所定のアルゴリズムで全変換し一定期間原本情報を秘匿する目的で開発されている。これは原本を全変換する仕組みである為に逆変換の可能性を否定でない。よって暗号技術の多くはアルゴリズムを敢えて開示し、それでも一定期間解読されないことを広く示す必要がある。一方電子割符の場合は、そもそも部分集合を生成する技術である為、容易に母集合を特定できない基本的な特性を持つ。更に、前述のように部分集合としての特長を活かしつつ、個々の割符ファイル（分割片）を生成する際にビットの振り分け方等を工夫すれば、既知の秘密分散法で言うところの閾値を設定し、ｎ個に分割したうちのｋ個で原本復元を可能とする割符ファイル（分割片）の生成も可能である。これをＢＣＰモードと呼ぶ。尚、部分集合を生成する当該技術は、相当程度の秘匿性を当初から有している。敢えて秘匿性向上も考慮して実現された秘密分散技術の場合、詳細な実装アルゴリズムを開示することは、国内のみならず世界的な社会安全保障上の観点から、現時点では相当慎重な判断が必要である。図１に割符と暗号の基本的な特徴比較図を示す。

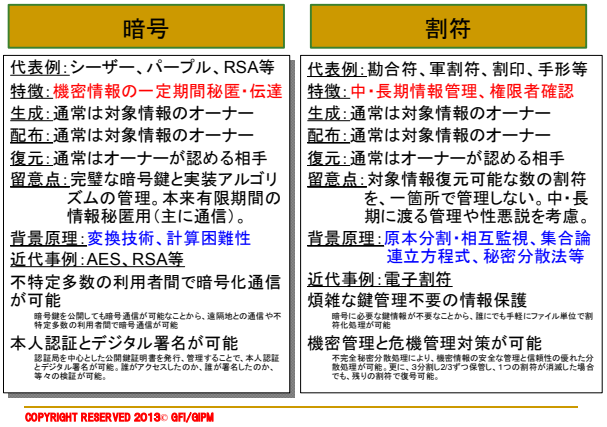

図 1．電子割符と暗号の比較

３．標準化の必要性

秘密分散技術は、内閣官房情報セキュリティセンター（NISC）公開の「政府機関の情報セキュリティ対策のための統一管理基準解説書」等に記載され（4）、次世代電子商取引推進協議会（ECOM）（現：一般財団法人日本情報経済社会推進協会（JIPDEC））より「EC における情報セキュリティに関する活動調査報告書 2009」の中で、割符と電子割符及び秘密分散技術に関し、一連の調査報告と初期のガイドラインが法的意見書を付されて公開されている（5）。要保護情報や情報資産等を安全・安心に保護できる技術として東日本大震災の教訓を踏まえ、個人情報保護等と同時に広域災害対策も可能とする技術として大きく注目されている。情報化の法整備も進む中、中・長期間の電子情報に対する運用管理に資する技術として当該技術標準化が必要である（図２参照）。

「An Initiative of the Standardization of Secret Sharing Scheme(e-Tally)~from an issue of market survey」
†「Yutaka Yasukura: Global Friendship Inc.」
‡「Sanji Kawashiro: Global Friendship Inc.」

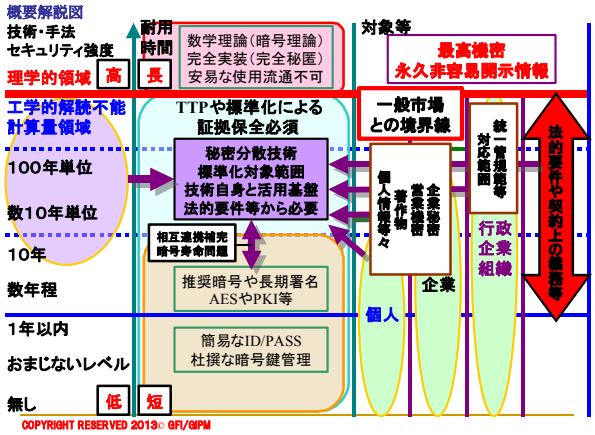

図 2. 電子割符の社会的役割と標準化背景

４．標準化への動きの現状

電子割符は、秘密分散技術として 2012 年から技術標準化に向けた準備活動を開始。初年度は経済産業省と関連組織、各界有識者との意見交換等と、同技術を用いた市場先進事例の調査、現場の声の吸い上げを行った。市場先進事例の一例を、図３に示す。

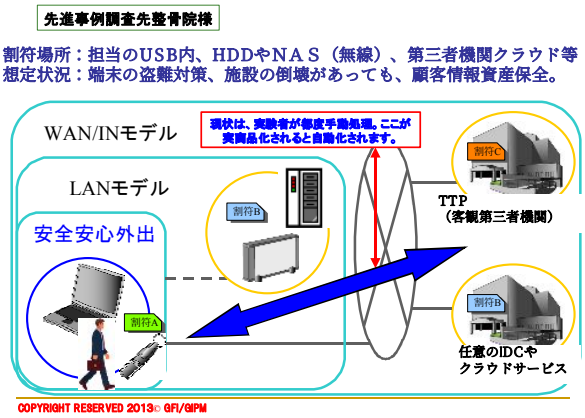

図 3. 電子割符の標準化に向けた実験システム例

５．標準化に向けての提案

図２及び図３のように、実社会での事例や法的環境整備の観点からも中・長期間の電子データの安全・安心を担う技術への要求もあることから、大きく以下のように新たな標準技術区分を提唱する。

暗号は、情報資産の一定期間の秘匿性確保を主たる目的とした技術である。

割符は、情報資産の中・長期間の運用管理を主たる目的とした技術である。

実データを実際に分割することで派生的に生じる副次的効果（ＢＣＰ対処、権利保護、要保護情報への対処等）は、社会や利用者が利活用できる事例の一つに過ぎず、丁度暗号を利活用した結果、認証が派生的に出現したことと同様な現象。また割符は、既存暗号技術と相互補完できる関係であり、双方が調和したシステムを具体化できれば、それぞれ独立した技術同士で合理的なＩＴ環境構築に資する成果が得られる。そこで相互に協調するには暗号とは異なる新たな標準技術区分として、割符（秘密分散技術）の具体化が必要。技術標準化の基本的内容は、１、基本的な概念や用語定義。２、同技術を中・長期間安全に運用する為の技術及びシステムの評価手法、３、割符ファイルの少なくとも一片を管理する外部組織等の定義。４、当該技術等に対する認定と登録受付を行なう第三者組織の実現。５、関連する主体の健全な運用状況の監査手法、６、利活用、応用編等々となる。標準化と普及スキーム案を図４に示す。

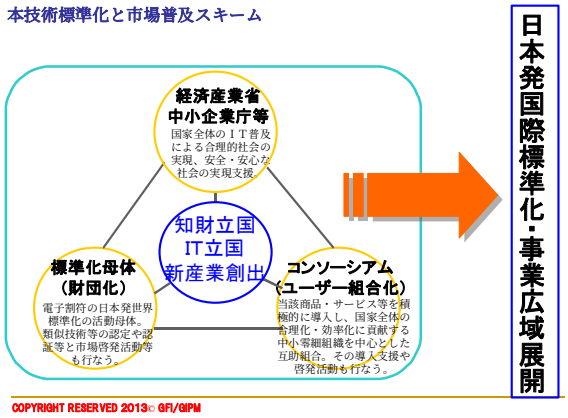

図 4. 標準化と普及スキーム案

６．まとめと今後の計画

当該技術を健全に利活用することでプライバシー保護や広域災害、著作権保護等々多くの電子情報の中・長期の運用管理に貢献できる。今後は本提唱に則り、対象となる技術概念の定義から始まり、システムに関する認定と登録受付を行なう組織やその認定基準となる基本的な技術定義等を順次具体化して行く。活動計画は、2013 年市場事例調査（2012 年継続と応用含む）と市場啓蒙（初期段階）ＪＩＳ化標準原案検討開始、2014 年市場事例調査（応用含む）とＪＩＳ化初期案取りまとめと市場啓蒙（継続）、2015 年市場事例調査と啓蒙及び、ＪＩＳ化原案取りまとめとＩＳＯ化等検討、2016 年市場事例調査と啓蒙及び、概念部と用語ＪＩＳ化実現目標年度。その後もＩＳＯ化等を含む国際標準化も視野に入れ継続的に活動を行なう。最後に、本発表の事例並びに提言に関して、行政、団体、大学、企業の多くの方々から貴重な助言や協力を賜ったことに感謝します。

７．参考文献

(1) Adi Shamir :How to Share a Secret, Communications of the ACM, vol.22,No.11(1979)
(2) 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
(3) 保倉　豊、川城　三治:電子割符の先進社会基盤適用モデル、情報処理学会研究報告.IPSJ SIG Technical Report, IS116-3(2011-06)
(4) NICS 統一管理基準解説書：http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf
(5) JIPDEC 秘密分散技術ガイドライン：http://www.jipdec.or.jp/archives/ecom/results/h21seika/H21results-10.pdf