

2013年1月14日

グローバルフレンドシップ株式会社 御中
代表取締役社長 保倉 豊 殿

「秘密分散技術（電子割符）」の標準化に向けた市場先進事例調査への意見書

東海大学・辻 秀一

1. 総論

参考資料(1)、(2)に示されている、秘密分散技術（電子割符）に関する定義、意義、特徴については十分に理解できるものです。また、市場事例調査対象や本技術の JIS 化や国際標準化の必要性についても了解するものです。しかしながら、現実の運営時における安全性確保レベルが十分に明らかになっているとは言い難いと考えます。参考資料(2)にも運用管理面での課題があることが指摘されており、運用管理ルールや実装方式などを整備し、さらに運用時におけるリスク分析や脅威分析などにより安全性レベルを評価する課題があると考えます。これらの課題を解決することにより、運用時においても安全性が確保された秘密分散技術の提供が行えるものと考えます。

2. 了解内容

・定義、意義、特徴

秘密分散技術を適用することにより、発生していた1箇所での運用・管理リスクを複数個所での運用・管理リスクに置き換えることで、リスクの分散をはかることができる。

・市場事例調査対象

先進事例概要－1（整骨院様）、および先進事例概要－2（本人特定情報運用管理実験）などの市場事例

・JIS 化や国際標準化の推進の必要性

導入等の事例から市場が本技術に期待している機能等を汲み取り、先駆者より開示されるノウハウ等に照らし合わせ、無秩序に展開させるのではなく、社会的に受容できる技術等としての基準を踏まえ、明確な定義をしておくことが重要である。

3. 課題

参考資料(2)における「秘密分散に関する技術ガイドラインおよび秘密分散技術利活用に関するガイドライン」の「3. 秘密分散技術を実現するソフトウェアプロダクトにおける必須要件」、「4. 秘密分散技術を実現するソフトウェアプロダクトにおける任意要件」と「5. 秘密分散技術を活用するシステムにおいて考慮すべき必須要件」が記載されていますが、記述が定性的で断片的で不十分な内容となっています。これらについては、定量的で網羅的な検討と整理が必要と考えます。

また、参考資料(2)における「情報分散管理技術（電子割符技術を利用した情報管理）に関する法的意見書」の「第1 技術と運用に関する基本的視点」に「―― ②その技術を運用する運

利用者側の運用ルールや、運用実態、リスク分析などを踏まえた運用の評価、――②は実用を評価対象とするものではないため、問題点の指摘にとどめ、今後の電子割符技術の利活用に資する問題点を指摘し、―― 」と記述されており、運用時における様々な検討が必要であることが指摘されています。この指摘にあるように、具体的で詳細な運用管理や実装の方法を検討・整備し、さらに運用時におけるリスク分析や脅威分析などにより安全性レベルを評価することが必要であると考えます。

<参考資料>

- (1) 保倉 豊：「秘密分散技術（電子割符）を用いた先進事例の調査～技術標準化のための事前市場調査～」、JIPDEC 電子記録応用基盤フォーラム eRAP 中間報告会、2012年10月2日。
- (2) 「ECにおける情報セキュリティに関する活動報告書 2009（情報セキュリティ WG:SWG1・SWG2・TF の各報告書）」／「秘密分散技術利活用検討における活動成果報告書 2009（TF1）」、次世代電子商取引推進協議会、平成22年3月。

以上