秘密分散技術関連提案

2011年12月23日

(株)IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp

秘密分散技術活用への期待

- 高度情報化が進む中、企業が扱うデータ容量の爆発が急進中。企業にとっては、その爆発するデータの安全・確実な保存が大きな課題。
- 爆発するデータの保存は、コスト・BCPの観点から、企業内での対策から、社外サービスの利用へとシフトの見込み。
- 企業情報の社外保存においては、高度な安全性と確実性が求められ、暗号技術および秘密分散技術の活用に期待。

秘密分散技術活用の課題

- 暗号技術については、CRYPTRECやJCMVPなどの制度や体制により、方式の安全性、実装の安全性についての第3者体制が確立され、利用者はその評価結果を利用し、安全な方式・実装を選定可能。また、監査や認証の制度により、運用の安全性についても第3者評価が得られ、利用者は信頼できるサービス事業者を選定可能。
- ところが、秘密分散技術については、方式の安全性、実装の安全性、運用の安全性に対する第3者評価の仕組みが存在せず、秘密分散技術を活用したサービスの利用には利用者が全てのリスクを背負う必要があり、活用の決断には大きなハードルが存在。

秘密分散技術の活用促進のために

- 秘密分散技術は、企業情報の安全な保存と確実な保存を同時に実現できる技術。
- 秘密分散技術は、これからのクラウド時代にこそ活用が期待される技術。
- 利用者が安心してその技術の恩恵を受けられるよう、適切な、方式・実装・運用かどうかの第3者評価体制を確立することが必要。
- 不適切な方式・実装・運用による事故の発生は、秘密分散技術の健全な応用展開を阻害しかねず、この観点からも、適切な方式・実装・運用かどうかの第3者評価体制を確立することが必要。

＜提案＞ 秘密分散技術の応用進展に不可欠な第3者評価体制の整備

安全性評価の視点	暗号技術の応用に関する評価	秘密分散技術の応用に関する評価
運用上の安全性	監査、認証制度	検討が必要
実装上の安全生	JCMVP	
方式上の安全性	CRYPTREC	

セキュアクラウドストレージサービスへの期待

- 秘密分散技術の応用により、安全性を維持しつつ、広域分散保存が可能。
- 秘密分散技術を応用した安心安全な、セキュアクラウドストレージサービスの利用やビジネス拡大が期待。
- クラウドサービスのグローバル化の進展により、セキュアクラウドストレージサービスも国境を越えた広域分散サービスへの発展の期待。

セキュアクラウドストレージサービスの普及の課題

- 秘密分散技術に基づき生成された分散片の保管サービスが、独立したサービスとして提供されていないため、秘密分散技術応用サービス事業者がそれぞれ保管サービスも一体として提供せざるを得ない状況。
- 分散片の生成機能と保管機能の分離により、保管サービスビジネスへ世界の中小のサービスベンダーも参入可能とし、保管サービスの安価さと広域分散可能性を実現する必要がある。
- 保管サービスインフラの出現により、秘密分散技術を応用した様々の情報サービスの提供が容易となり、秘密分散技術の応用進展が期待される。

＜提案＞ 秘密分散技術の応用進展には分散片管理のフレームワークが必要