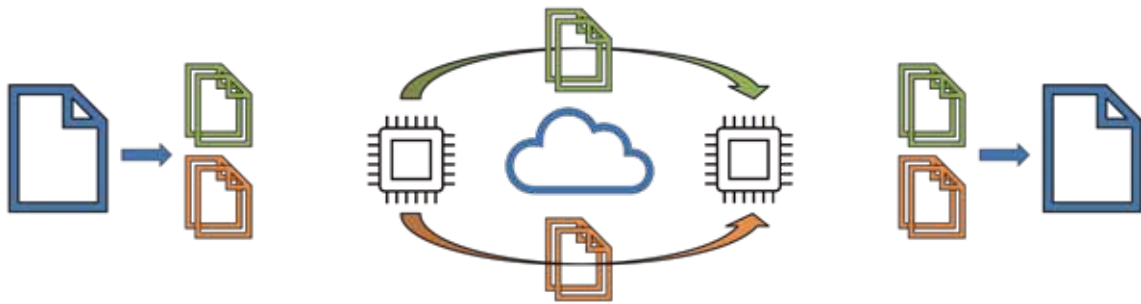


秘密分散法とは？

今、注目されている新たなデータ秘匿化手法

代表的なデータ秘匿化手法として鍵暗号方式がある一方で、近年のセキュリティ対策の高まりによって新たなデータ秘匿化手法の注目が高まっています。秘密分散方式はデータ自体をいくつかの断片 (= 分散片) にすると共に、秘密鍵を分散片に埋め込みます。分散化したデータは、全ての分散片を集めなければ復元できません。異なる地点、または経路で分散片を保管 / 送信することで、データ漏洩に対して堅牢性が上がります。



どのような情報漏えいに対応できる？

秘密分散法は標的型攻撃に有効

標的型攻撃や、マルウェア等のサイバー攻撃によって発生する情報漏洩のリスクに対して、秘密分散法を応用したシステムの有効性について考えてみましょう。分散片をそれぞれ別のサーバーに保管することで、攻撃者は全てのサーバーを攻撃する必要があり、また正しい順序で復元する必要があります。expist[®]IoT では更に鍵暗号化方式を組み合わせた秘密分散法を使用しているため、よりセキュアにデータを守ることが可能です。

秘密分散法が注目を集める理由の一つとして、自民党デジタル社会推進特別委員会による推進の提言がされている点が挙げられます。PC やクラウドにおけるストレージの保護や、総務省主導の電子カルテ秘密分散バックアップ技術の研究等、今後更に社会実装が進むことが予想されます。

エイチアイにおける特許の取り組み（秘密分散法）

エイチアイは秘密分散法に関する独自の特許を出願しています。この特許では、秘密分散技術で作成した分散片をシャッフルして複数のサーバに分散配置することにより、セキュリティを向上させる技術について出願したものととなります。

・特願：2022-083844 情報分散方法及びプログラム