# 最新の暗号を用いた 安全・安心なファイル共有方法の開発

暗号というと数学的で、生活になじみがないと思う方が多いと思います。しかし実際には、ウェブサイトでのショッピングや銀行での取り引きなどの裏側では暗号が利用されており、現代のデジタル社会において利用者の安全・安心を確保しつつ利便性を向上させるために、暗号は必要不可欠なものとなっています。また近年、デジタル情報の流出などが、個人情報保護の観点などから問題となるケースがあります。対策として、暗号化機能付きノートPCやUSBメモリの利用、個別のファイル・フォルダの暗号化が行われています。今回、属性ベース暗号というペアリング暗号の一種を用いて、安全性を確保したファイル共有方法を開発しましたので紹介します。

情報技術グループ 主任研究員
大平 倫宏

## 開発背景

情報化社会の発展により、利用する電子的なファイルの総数や容量は、今後ますます増加していくことが予想されています。そこで、管理コストなどの低減のため、外部にあるクラウドストレージなどの利用が考えられます。しかし、多くのクラウドストレージでは、利用規約として、サービス提供側が利用者のファイルを閲覧できるように定めています。このため、マイナンバーなどの個人情報の載っているファイルの流出が起こった際や、悪意のあるサービス提供者が存在した場合などには、大きな問題となります。

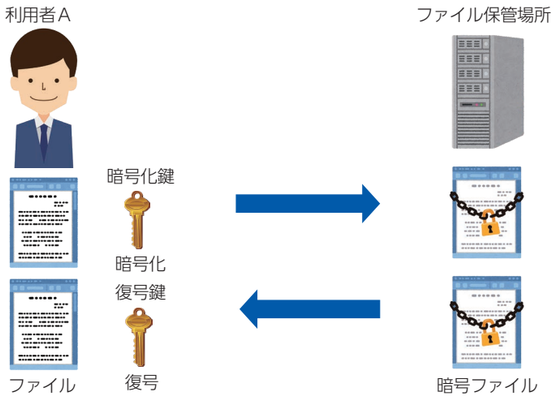



図1 ファイル保管における暗号の利用例

そのような問題に対応するために、図1のように、ファイルを暗号化鍵で暗号化してからクラウドストレージなどのファイル保管場所に保存し、利用時には対応する復号鍵で復号してから利用する方法が考えられます。今回は、ペアリング暗号の一種である属性ベース暗号という暗号を用いて、安全にファイルを共有する方法を紹介します。

## ペアリング暗号

これまで利用されてきている多くの暗号では、素因数分解や離散対数問題の計算量的な難しさを、その解読の難しさの根拠としています。例えば、RSA暗号などは、図2のような素因数分解の困難性を利用しています。

p, qを素数として、x = pqとする。

・p, q ⇒ xを計算することは簡単。
・x ⇒ p, qを計算することは難しい。

図2 素因数分解の困難性

このように、計算を行う際に、一方(この場合ではp, q)から一方(x)を計算することは簡単ですが、逆方向に計算することは難しいといった性質が、暗号ではよく利用されます。xに対応するものを公開しても問題ないため、公開鍵として暗号化する際に利用することが可能です。一方で、p, qに対応するものを復号用の秘密鍵として秘密にしておきます。こうすることで、暗号と復号で別々の鍵を利用するとともに、暗号化用の鍵を公開することが可能となります。

近年、従来から利用されているRSA暗号や楕円曲線暗号に次ぐ次世代の暗号として、ペアリング暗号の利用が見込まれています。ペアリング暗号は、離散対数問題に基づく暗号で、2001年に開発されています。ペアリング暗号が注目されている理由として、これまでの暗号では考えられなかった、さまざまな応用が実現可能であることが挙げられます。

実際には、以下のような応用が考えられています。

**IDベース暗号**

公開鍵として、任意の文字列を利用できる暗号で、メールアドレスなどが公開鍵に利用されています。

**属性ベース暗号**

特定の属性を持った者だけが復号できる暗号。暗号自体にアクセス権の制御に相当するものが組み込まれています。ストレージサービスなどで利用されています。

**検索可能暗号**

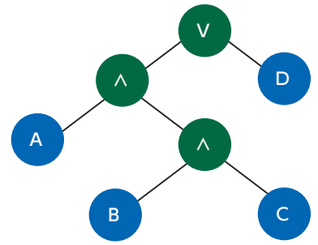
データを暗号化したまま、データの内容自体を知ることなく、キーワード検索などができる暗号です。化合物データベースなどで利用されています。

## 属性ベース暗号を利用したファイル共有方法(特許出願中)

属性ベース暗号では、利用者それぞれに「開発部」、「総務課」などの属性を複数割り当てます。暗号化を行う際には、暗号文に対するアクセス構造を定めます。アクセス構造は図3のように属性の「または」(∨)、「かつ」(∧)の組み合わせで表わされます。図3のようなアクセス構造を持つ暗号文の場合は、「開発部」かつ「海外支社勤務」かつ「2017年度在籍者」、もしくは「総務課」の属性を持つ者のみが、復号することが可能となります。

このため、ファイルの暗号化時に、適切なアクセス構造を定めることで、図4のように異なる属性を持つ利用者の間で、ファイルの共有を行うことが可能です。図4でAさんは、「開発部」と「IT」の属性を割り当てられているため、上から二つのファイルを利用することが可能ですが、三つ目の「総務課」の属性のみのアクセス構造であるファイルは利用することができません。また、上から二つ目の「開発部連絡先」ファイルは「開発部」または「総務課」のアクセス構造となっていますので、Aさん、Bさんともに利用が可能です。

このようなファイル共有方法に対して、さらに安全性を高めるための対策を施して、特許出願を行っています。興味を持たれた方は、ぜひ情報技術グループまでご相談ください。




**論理式**
∨：または
∧：かつ

**属性**
A：開発部
B：海外支社勤務
C：2017年度在籍者
D：総務課

図3 属性ベース暗号のアクセス構造の例

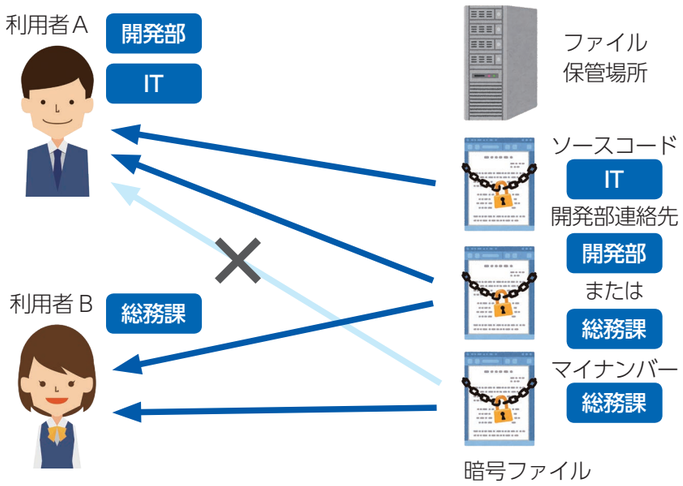



図4 属性ベース暗号を利用したファイル共有

お問い合わせ：情報技術グループ〈本部〉 TEL 03-5530-2540