属性ベース暗号を用いた安全・安心なファイル共有方法の開発

特許出願中

安全・安心

情報技術グループ　大平 倫宏
TEL 03-5530-2540

特徴

従来よりも安全な属性ベース暗号を構築しました。これを利用して、ファイルの流出等があった際にも安心なファイル共有方法を開発しました。属性による細かなアクセス管理が可能です。

①属性ベース暗号

属性ベース暗号は、「総務課」、「開発部」等の属性を基に、ある属性の組み合わせを持つ者だけが、暗号文を復号可能となる暗号です。例えば、図1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。利用者のアクセス権限を詳細に設定可能であるという特徴を持つため、活用が見込まれています。

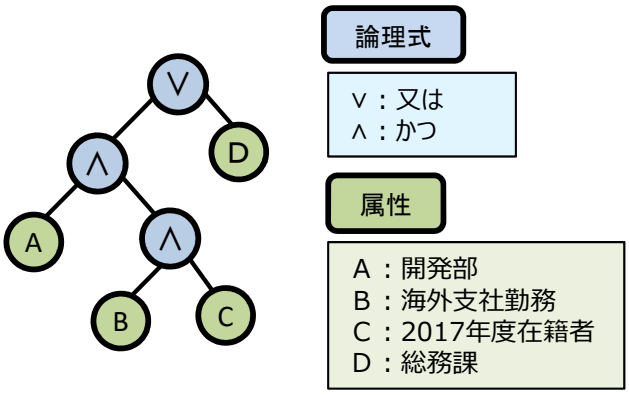

図１　属性ベース暗号のアクセス構造の例

②安全・安心なファイル共有システム

今回は、従来よりも安全な属性ベース暗号を構築し、それを利用して安全なファイル共有方法を開発しました。図２の例では、「マイナンバー」ファイルは、「総務課」のBさんのみがアクセス可能となり、暗号レベルでアクセス制御が行えています。

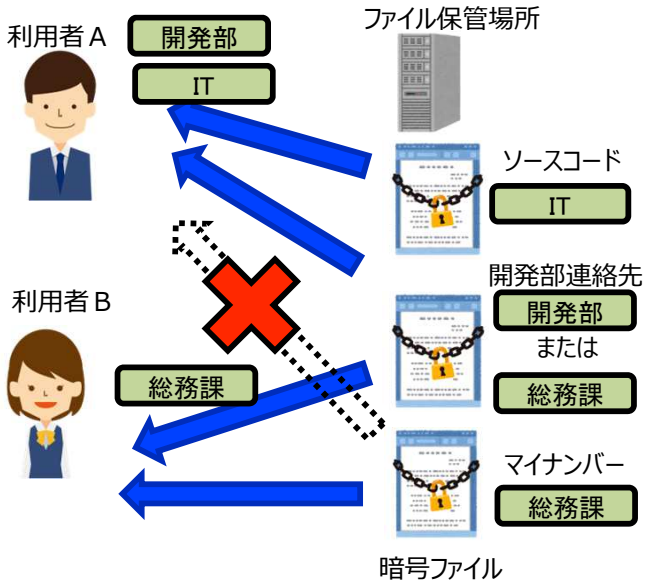

図２　属性ベース暗号を利用したファイル共有

従来技術に比べての優位性

- 安全(マスタ秘密鍵がないなど)
- 細かなアクセス制御が可能
- ファイルが流出しても安心

研究成果に関する文献・資料

- TIRI NEWS 2018年12月号

今後の展開

- ファイル共有サービス
- 動画配信サービス
- IoTデータの管理

研究員からのひとこと

この技術で安全・安心なファイル共有が可能です。

暗号技術に興味のある企業様との共同研究・事業化を受け付けております。