属性ベース暗号を利用した安全かつ効率的なファイルシステムの開発

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

属性ベース暗号は、アクセス権限の設定が可能な暗号で、ビッグデータやIoT技術での活用が期待されています。属性ベース暗号を利用して、書き込み・読み込み権限を詳細に設定可能なファイルシステムを開発しました。

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。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。

従来の属性ベース暗号では、ファイルの読み込み時のアクセス制御が可能でした。今回の研究では、ファイルの書き込み時にも同様のアクセス制御が可能なファイルシステムの開発を行いました。図の例では、「マイナンバー」ファイルは、「総務課」のAさんのみがアクセス可能であり、「緊急連絡先」ファイルは、「総務課」のAさんと「部長」のCさんのみがアクセス可能になっており、暗号レベルでアクセス制御が行えています。

クラウドストレージ等を利用した場合でも、安全にファイル共有が行えます。

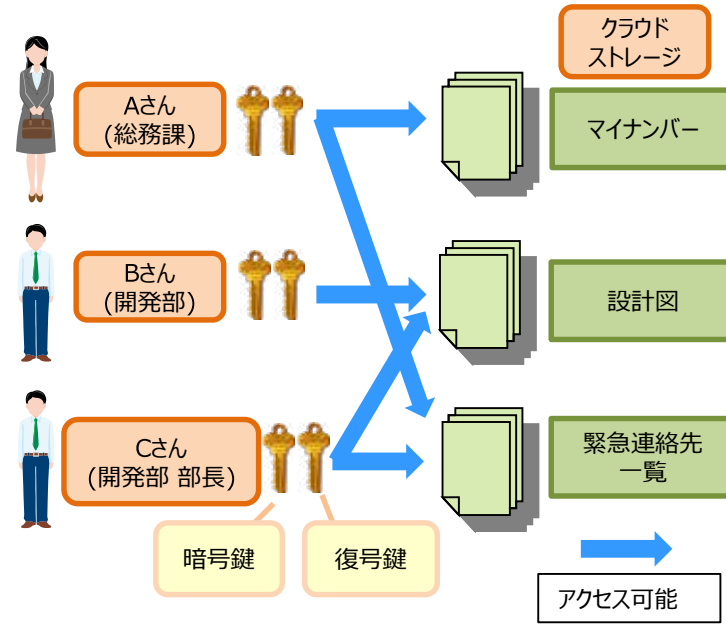

図　属性ベース暗号を用いたファイル共有システム例

従来技術に比べての優位性

- ファイルアクセス時に、細かなアクセス制御が可能
- ファイルが流出した場合でも安全
- プライバシーの保護が可能

研究成果に関する文献・資料

- TIRI NEWS 2018年12月号, P.02-03

今後の展開

- クラウドストレージでのファイル共有
- 動画配信サービスでの応用
- IoT・AIデータの管理

研究員からのひとこと

この技術で安全かつプライバシーに配慮したファイル共有が可能です。

暗号化技術に興味のある企業との共同研究・事業化を募集しています。