地方独立行政法人 東京都立産業技術研究センター TOKYO METROPOLITAN INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE

7月13日 16:00～16:20
2階 研修室241

属性ベース暗号を利用した安全なファイル共有方法の開発

情報技術グループ　大平 倫宏
TEL：03-5530-2540

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る。安全な属性ベース暗号を新規に開発して、それを利用したファイル共有方法を開発した。

内容・特徴

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ある。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る。

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る。

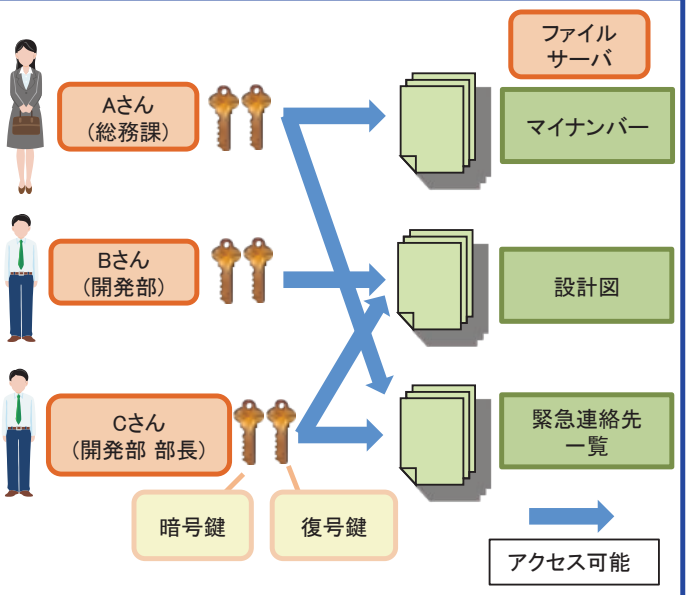

図　属性ベース暗号を用いたファイル共有例

従来技術に比べての優位性

❶安全（マスタ秘密鍵がないなど）

❷細かなアクセス制御が可能

❸ファイルが流出しても安心

予想される効果・応用分野

❶ファイル共有サービス

❷動画配信サービス

❸IoTデータの管理

提供できる支援方法

- 共同研究
- 技術相談
- オーダーメード開発支援

属性ベース暗号以外でも、暗号技術全般に関する技術相談を受け付けております。

知財関連の状況、文献・資料

- 知財関連

特許出願中