

属性ベース暗号（ABE）によるプライバシー保護

属性ベース暗号の柔軟かつ動的なアクセス制御により、
パーソナルデータの漏洩や不正閲覧を防止します

#レジリエンス

属性ベース暗号(ABE) の概要

Attribute-Based Encryption (ABE)

属性(所属・役職)に応じて復号可否を決定する暗号技術。

動的属性や1ファイル内の部分的暗号化にも対応可能。

ABE is an encryption technology with attribute-based access control. It supports dynamic attributes and partial encryption of specific sections within a file.

適用例：生徒の成績データの閲覧制御

Application Example： Access control for student grades



担任
Homeroom teacher

生徒名 Name	国語 Japanese	数学 Math	理科 Science	..
Alice	80	58	38	..
Bob	58	29	81	..
Charlie	97	61	56	..

担任の先生は全科目閲覧可能
Homeroom teachers can access all scores.



国語の先生
Japanese teacher

生徒名 Name	国語 Japanese	数学 Math	理科 Science	..
Alice	80	国語の成績以外閲覧不可 Japanese teachers can access only the Japanese scores.		
Bob	58			
Charlie	97			

※数学の先生の場合は数学の成績以外閲覧不可
Math teachers can access only the math scores.



リモート勤務者
Remote worker

生徒名 Name	国語 Japanese	数学 Math	理科 Science	..
-------------	----------------	------------	---------------	----

学校外からのアクセスのため全て閲覧不可
Access from outside the campus is not permitted.

///技術課題

消費者のプライバシー意識の高まりや、データ漏洩事故の増加により、企業はより機微なデータの扱いに配慮する必要があります。

///研究目標

機微情報などの漏洩リスクを低減するとともに、プライバシーに配慮したデータ利活用を促進し、競争力を向上します。

---要素技術

NTTグループが開発した技術により以下を実現

- ・ 高速な暗号化・復号処理
- ・ AND,OR,NOTを用いたポリシーを使用可能
- ・ 複数鍵発行権利者への対応
- ・ 共通鍵暗号方式（AES）とのハイブリッド方式に対応

---適用ビジネス

機微情報を扱う領域に置いて、機微情報が記載されているデータ、またはそのデータの特定の部分に対する、閲覧者の役割や属性に応じたきめ細やかな閲覧制御に活用

例：学校の成績データにおいて、担任教師は全科目の成績を閲覧できる一方、各科目の担当教師は自身の担当科目のみ閲覧可能。

（PoC対応およびシステム・アプリケーションへの組み込み可能時期：2024/4Q頃）

---市中技術差異点

- ・ 復号者の属性に応じて、閲覧範囲を切り替えるなどきめ細やかなアクセス制御が可能
- ・ 時間や場所などの動的属性を使用可能
- ・ ファイル自体に暗号化とアクセス制御が適用されるため、データの保存場所を問わずガバナンスを確保可能（例：ファイルサーバ外）