

IOWN INTEGRAL

NTT R&D FORUM 2024

BUSINESS

β 03-01

Privacy protection using Attribute-Based Encryption (ABE)

ABE prevents personal data leakage and unauthorized access through flexible and dynamic access control

#Business Resilience

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.

///Technical Issue

Companies should be more considerate in handling sensitive data due to the increasing consumer privacy awareness and the rise in data breaches.

///Research Goal

Improve competitiveness by promoting data use with privacy protection and reducing the risk of sensitive data breaches.

---Technology

With NTT Group's technology, the following can be achieved

- Fast encryption and decryption.
- Policy implementation using AND, OR, and NOT operators.
- Management of multiple authorized key issuers.
- Support for hybrid scheme combining AES.

---Applicable Business

It is possible to implement fine-grained access control for data containing sensitive information, or specific parts of such data, based on the attributes of the viewer.

Example: In the context of student grades, homeroom teachers can access all scores, whereas math teachers can access only the math scores.

Scheduled PoC and system/service integration support timeframe: 2024/4Q

---Novelty

- Fine-grained access control that adjusts viewing permissions based on the attributes of the decryption user.
- Support for dynamic attributes such as time and location.
- Encryption and access policies are embedded in the file itself, maintaining governance irrespective of storage location.

Related Exhibition=[β03-02](#) Exhibitors= NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION

[Contact URL](#)