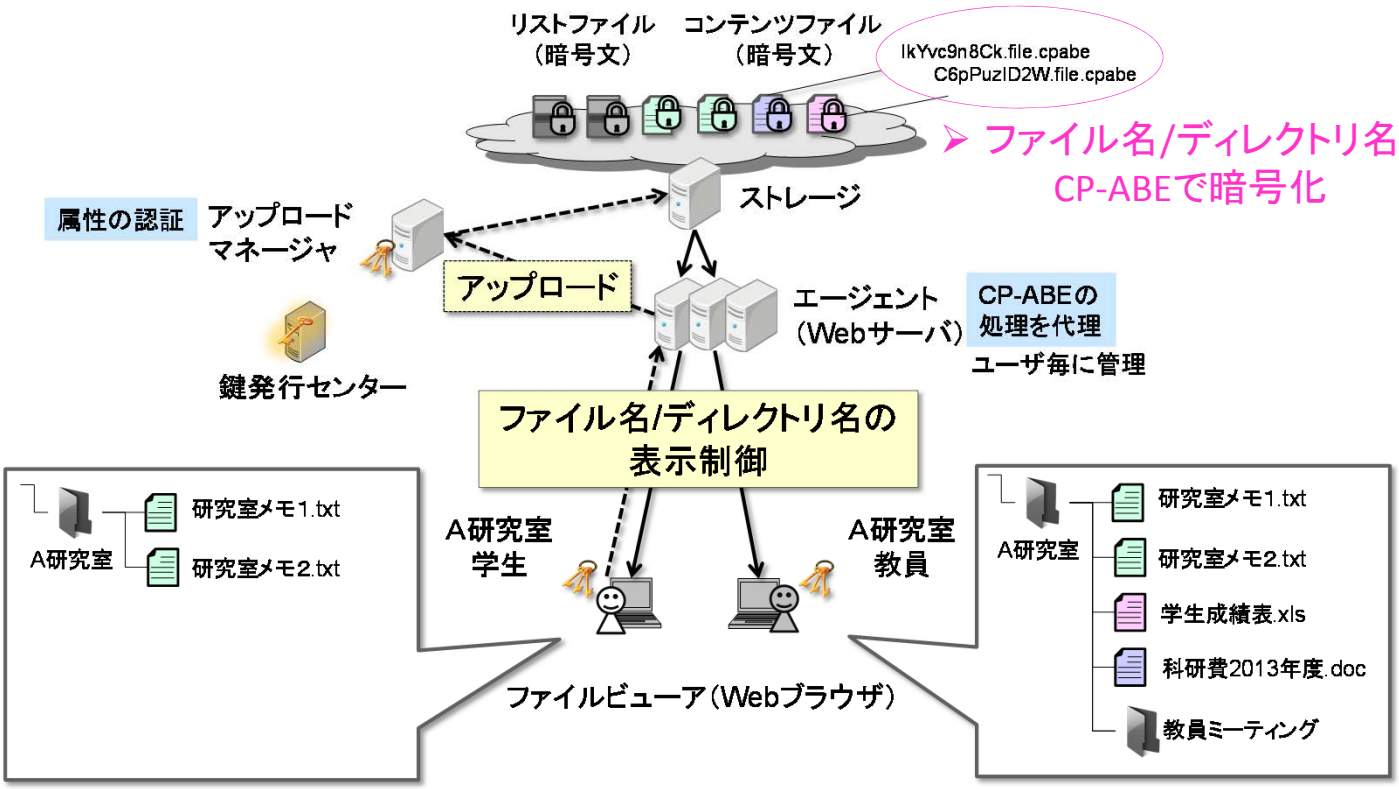
# ファイル名/ディレクトリ名を秘匿可能なクラウド向け暗号化ファイル共有システム

後藤 めぐ美　大東 俊博　西村 浩二　相原 玲二（広島大学）




➢ ファイル名/ディレクトリ名はCP-ABEで暗号化

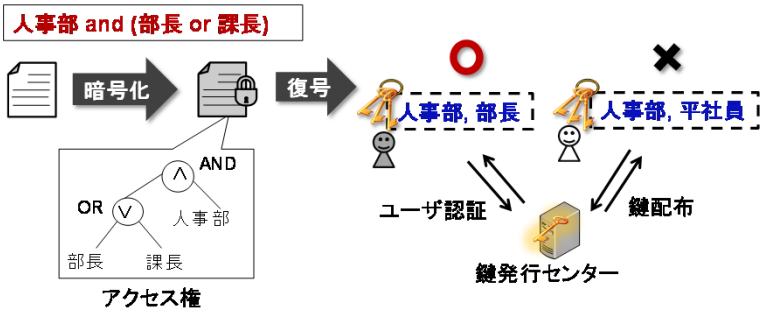
➢ ユーザの属性に応じて、ファイル名/ディレクトリ名を表示制御

## 暗号文ポリシー属性ベース暗号

◆ CP-ABE
（Ciphertext-Policy Attribute-Based Encryption）

**暗号化鍵**は
属性を使った論理式で表現可能

**復号鍵**に埋め込まれた属性集合が
アクセス権を満たすとき復号可能




## 各サーバの役割

[1] コンテンツの復号
[2] ファイル名/ディレクトリ名の復号, ディレクトリ構造の取得
[3] ストレージ上への暗号化ファイルの作成

| | [1] | [2] | [3] |
|---|---|---|---|
| ストレージ管理者 | × | × | × |
| アップロードマネージャ管理者 | × | ○ | ○ |
| 一般ユーザ[属性合致の場合]（＝ エージェントサーバ管理者） | ○ | ○ | × |
| 鍵発行センター管理者 | ○ | ○ | × |

ファイル名/ディレクトリ名を暗号化
編集権限の管理
コンテンツの暗号化・復号
ファイル名/ディレクトリ名表示

[関連発表]
・後藤 めぐ美, 大東 俊博, 西村 浩二, 相原 玲二, “属性ベース暗号を利用したファイル名暗号化ファイル共有サービス,” 情報処理学会研究報告, Vol.2012-IOT-16, No.36, pp.1-6, 2012年3月.
・後藤 めぐ美, 大東 俊博, 西村 浩二, 相原 玲二, “属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と評価,” 電子情報通信学会技術研究報告, ICSS研究会, ICSS2012-53, pp.49-54, 2012年11月.

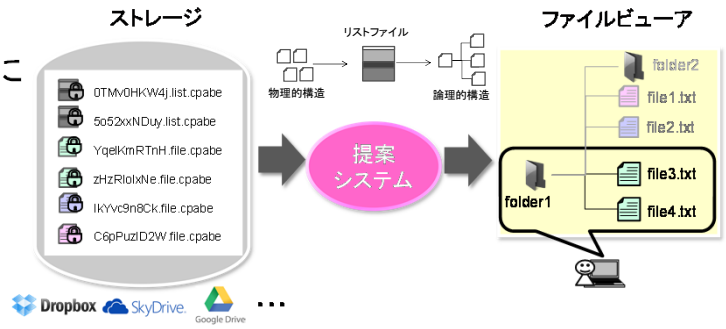
※本研究の一部は、科学研究費補助金　基盤研究(B)(課題番号23300026,24300025)の助成を受けている.

広島大学

## システムの特徴

◆ ファイル名/ディレクトリ名を高速に表示制御

- ファイル名/ディレクトリ名はコンテンツの要約など重要情報を含む場合がある
  （例）20130122_●●部長人事面接.zip
- ファイル名/ディレクトリ名を閲覧権限毎に一括してCP-ABEにより暗号化
  ⇒ 高速化を実現




◆ ファイルの閲覧権限と編集権限はユーザ側で決定

- 属性を認証する機能を備えたアップロード用のサーバ（アップロードマネージャ）を導入することで、ストレージに手を加えることなく編集権限の管理が可能

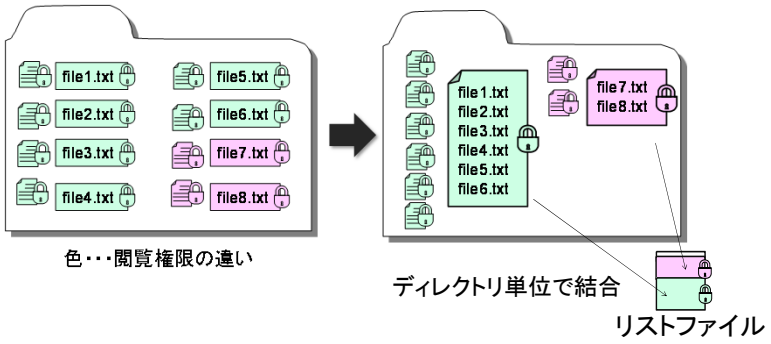
◆ マルチプラットフォームで動作

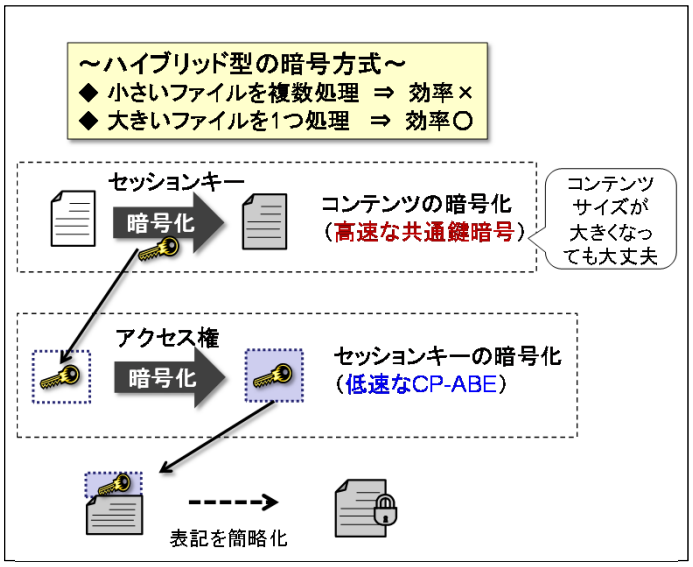
- ユーザ単位で管理されたエージェント（Webインタフェース）がCP-ABEの処理を代理で実行

## 表示の高速化のポイント

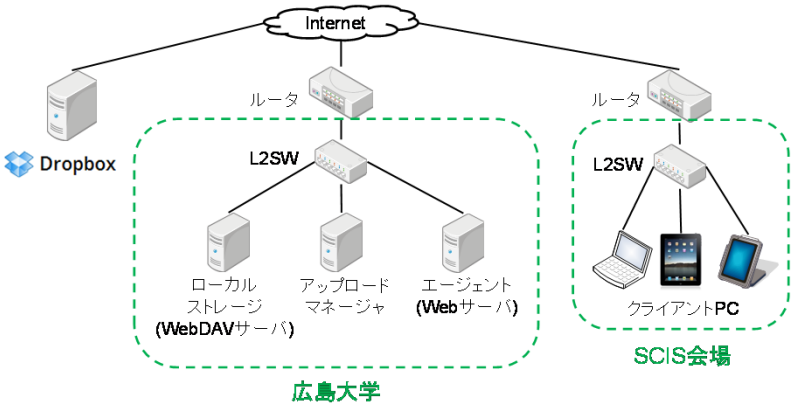
＜一般的な手法＞
◆ファイル名を個別に暗号化

＜提案手法＞
◆同じ閲覧権限のファイル名をまとめて暗号化




## デモの構成




[デモ1] ファイル名/ディレクトリ名の表示
[デモ2] ファイルのアップロード

## プロトタイプシステムによる性能評価

| ファイル名表示時間（ブラウザ上でディレクトリ遷移） | | | |
|---|---|---|---|
| 表示するファイル名の数 | 200個 | 2,000個 | 20,000個 |
| ローカルストレージ | 0.20秒 | 0.30秒 | 0.89秒 |
| Dropbox | 2.07秒 | 4.99秒 | 16.53秒 |

※エージェント上でファイルを復号し終えるまでの時間
（エージェントからクライアントPCへファイル名を転送する時間は含んでいない）

| コンテンツのアップロード時間（コンテンツサイズ1KB） | | | |
|---|---|---|---|
| コンテンツを追加するディレクトリに存在するファイルの数 | 200個 | 2,000個 | 20,000個 |
| ローカルストレージ | 2.95秒 | 2.99秒 | 3.39秒 |
| Dropbox | 10.68秒 | 15.82秒 | 41.36秒 |