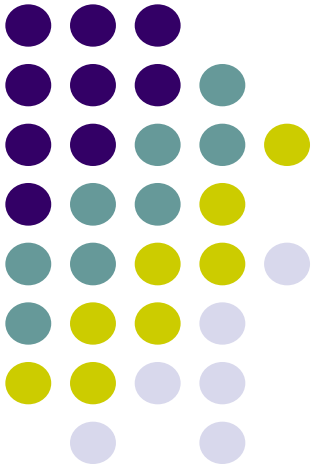
カームコンピュータ株式会社

クラウド向けセキュリティ
@SECURE/KeyShare-Encryption for Cloud



国の開発委託事業費により開発

@SECURE/KeyShere-Encryption for Cloudは経済産業省による「平成22・23年度産業技術開発委託費」により開発されました。

参照HPhttp://www.meti.go.jp/information/data/c100921aj.html

クラウドへのセキュリティー対策

- クラウドではデータの情報漏洩、安全性が不安。
  （ネット上へのデータ流出）
- クラウドシステムへの不正ログイン（なりすまし）の脅威

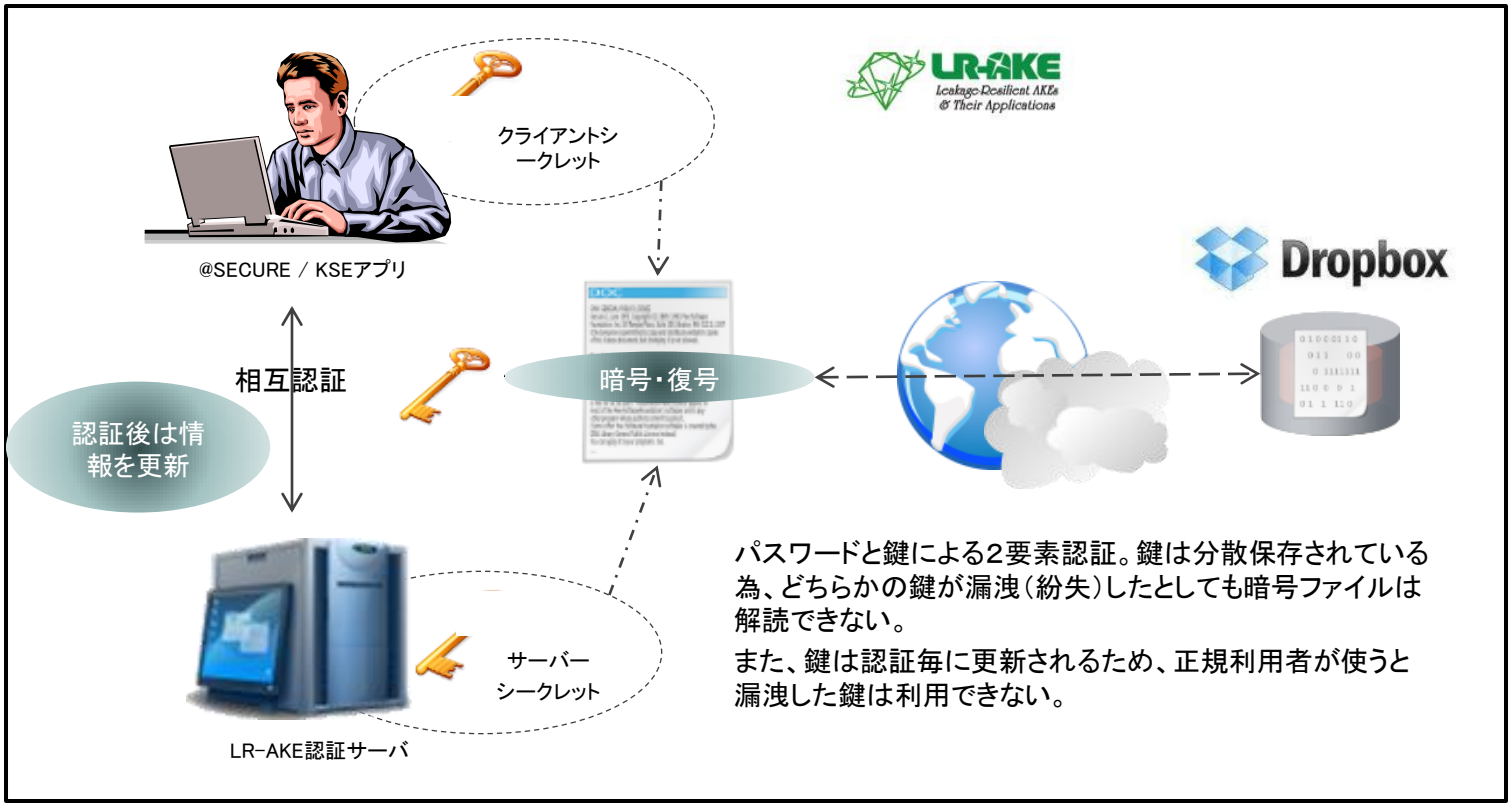
対策

- クラウド上に、より安全な暗号化方式でデータを保存
- クラウドシステムへのログイン方法をより強固な物に
  （ID+パスワードにさらに暗号鍵をプラス）

信頼性の高い暗号技術で安全に

パスワード＋分散鍵で暗号化しファイルをクラウドストレージに保存。

暗号アルゴリズムに、「産業技術総合研究所」が研究開発した「LR-AKE」を採用。



強固なセキュリティー（暗合鍵分散技術）

- **暗合鍵分散技術**（LR-AKE）・・・産業総合研究所にて特許を所得済み
  - 利用者はパスワードと**分割された暗合鍵**を用いて認証サーバと認証を行います。正しく認証が終わると両者間で**認証に利用する情報の更新**を行い、次回認証時は前回と同じ情報を利用せずに認証を行います。

→メリット

- 暗合鍵情報を分散して管理する為、片側から情報が漏洩したとしてもそれ単体では意味の為さない情報となり、**セキュリティを強化出来ます。**
- 正規利用者が認証を行う度にサーバと同期し、分割鍵情報の更新を行います。これにより不正利用者が認証を行った際、**情報が更新される為、異変を検知することが出来ます。**
- **従来のデバイスによる認証装置（指紋認証装置等）は必要ありません。**

クラウドストレージを安全に活用

専用アプリケーション「CE-Explorer」を利用して暗号ファイルをクラウドストレージに保存、閲覧することが可能です。また、あらかじめ指定しておいたグループメンバーで共有し暗号化・復号化することが可能です。

Mac OS X

WindowsXP

Windows7

iPhone

iPad

複数デバイス対応

会社のWindows
端末で作成

自宅のMacintosh
端末で編集・保存

外出先のiPad/iPhoneで閲覧

グループ対応

同一グループの
メンバに共有可能

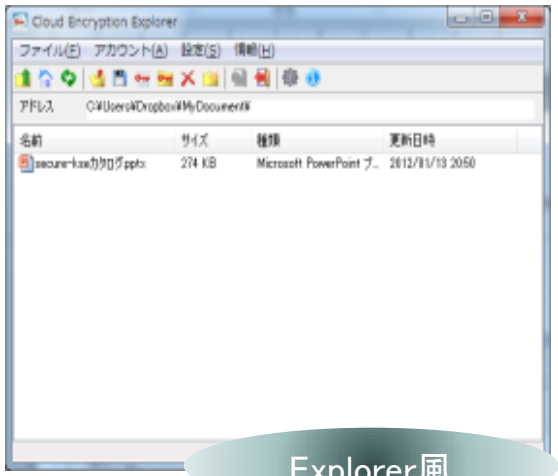
※閲覧や編集を行う場合はアプリケーションソフトを各デバイスにインストールする必要があります。

※iPhone / iPad は ZumoDriveには対応していません。

スマートなGUI

専用アプリケーション「CE-Explorer」は各デバイスに応じたGUIに対応。操作性もスムーズなので使い慣れた環境で違和感なく操作できます。

Windows



Explorer風

iPad

Dropbox風

※専用クライアントアプリケーションは各デバイスにインストールする必要があります。

※Dropboxなどのクラウドストレージサービスのアカウントが必要です。

集中管理機能

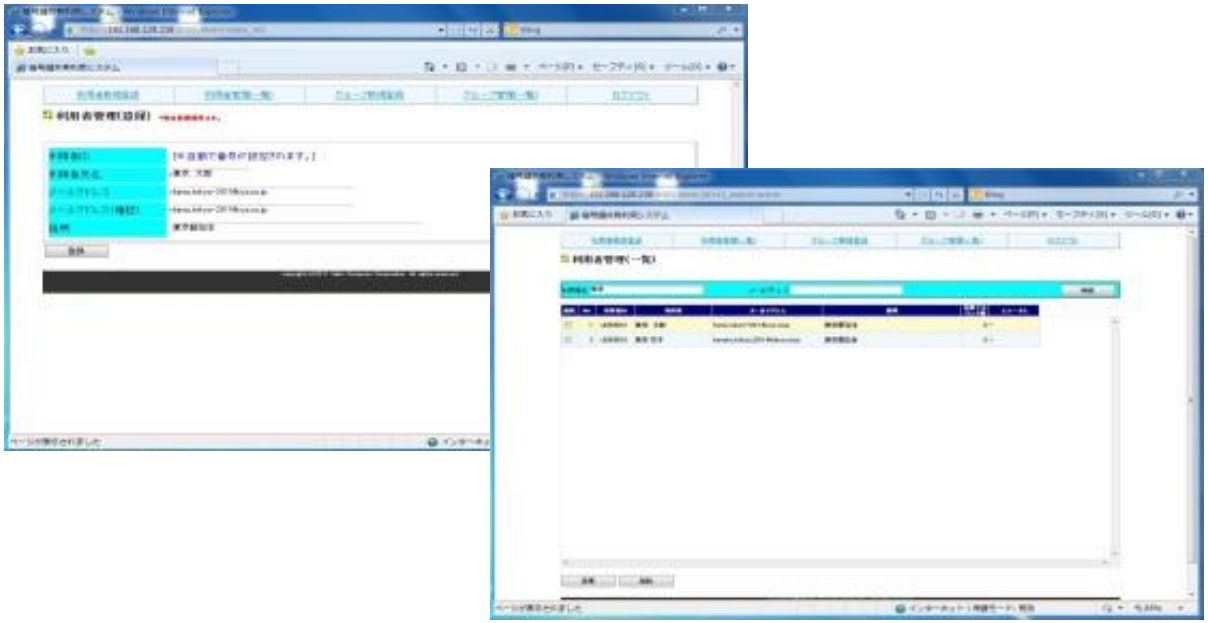
ブラウザにて、各種設定を一元的に管理できます。

・利用者設定

・グループ設定

・アカウント発行、停止、一覧検索

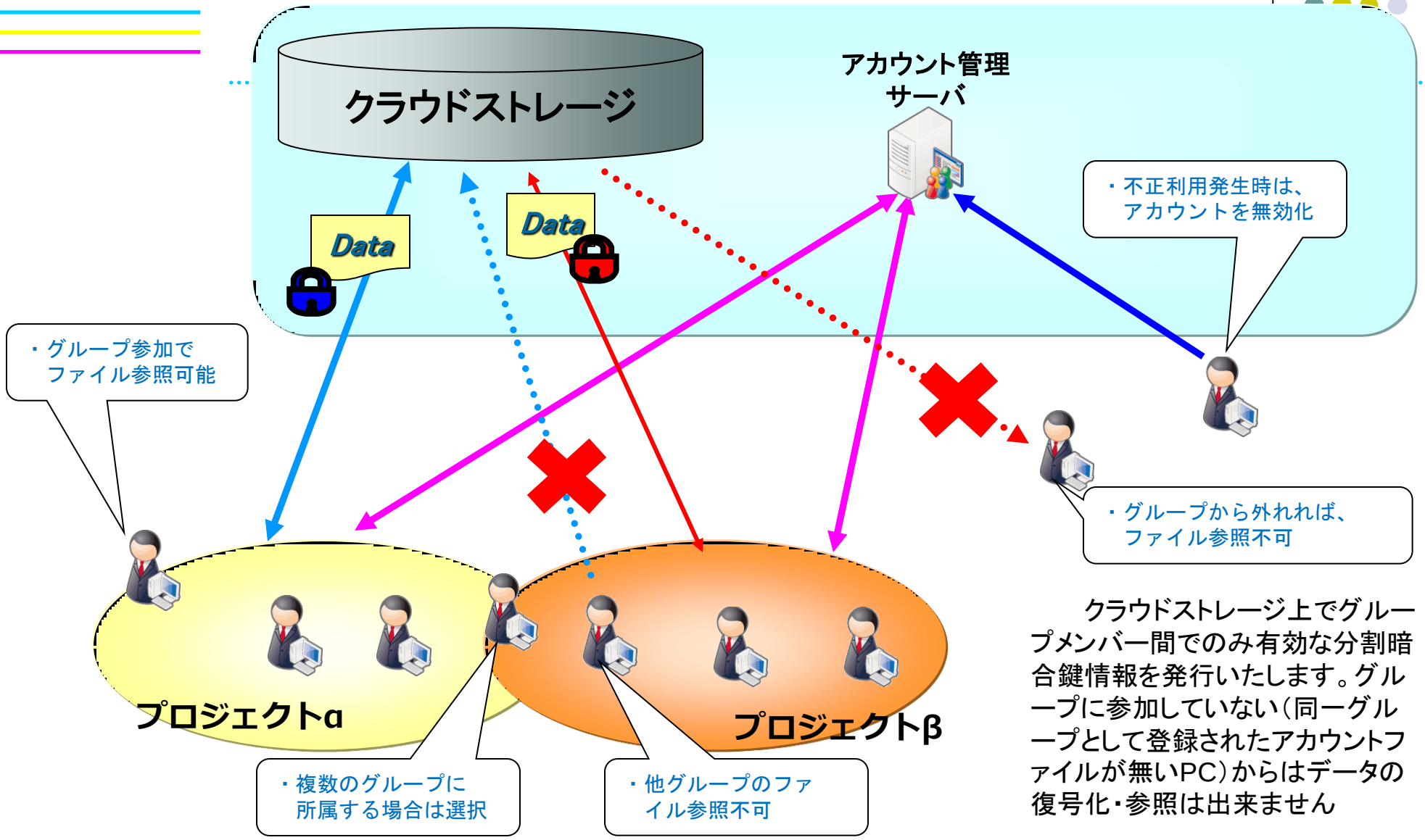
・管理者設定



他の認証方式との比較と特徴

認証および鍵管プロトコル	通信路の盗聴	並列オンライン攻撃	記録情報漏洩への耐性				パスワードの数	フィッシング詐欺への耐性	
			クライアント側から	サーバー側から	時間差で両方から	同時に両方から		偽公開鍵の受け入れ	入力箇所間違い
従来のパスワードベースプロトコル	×	×	○	×	×	×	複数	○	×
PKI(サーバー認証+PW)	○	×	○	×	×	×	複数	×	×
PKI(サーバー認証+PW+OTP+マトリクス)	○	○	○	×	×	×	複数	×	×
PKI(相互認証)	○	○	×	○	×	×	一つ	×	○
LR-AKE	○	○	○	○	○	×	一つ	○	○

グループでの安全便利な利用



クラウドストレージ上でグループメンバー間でのみ有効な分割暗合鍵情報を発行いたします。グループに参加していない（同一グループとして登録されたアカウントファイルが無いPC）からはデータの復号化・参照は出来ません

皆様にお願いしたい事

【営業面】

お知恵を拝借出来ませんでしょうか？

（セキュリティーはお金になりにくい・・）

いいんだけどねー・・予算無いし・・（笑）

アライアンス希望！！

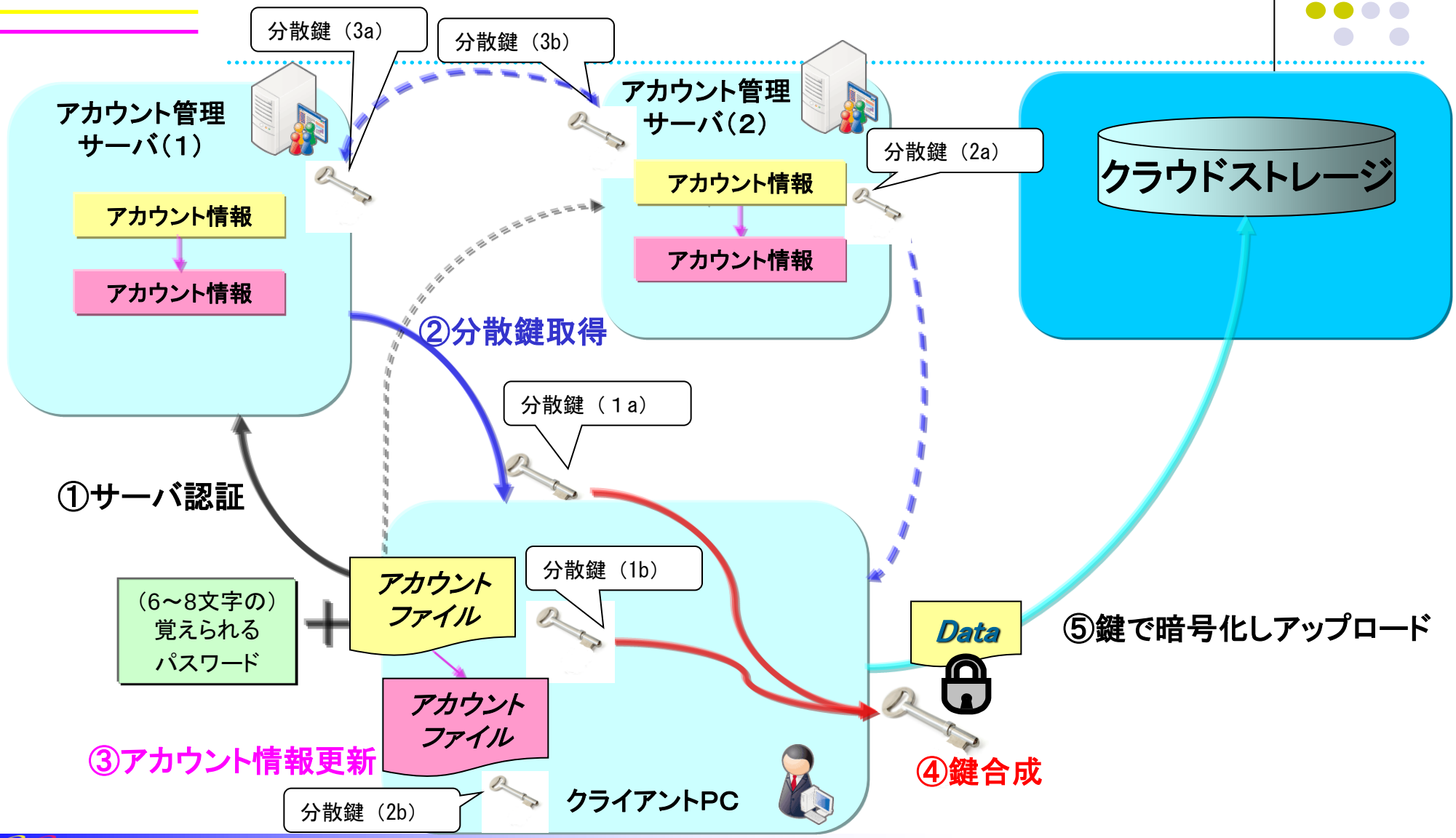
【技術面】

技術協力（コミュニティー）を希望・・

（正直、開発力がプアーです。このままでは埋もれしまうかも）

※是非、お助け下さい！！

LR-AKEの認証フロー



動作環境

Windows / Macintosh

■プラットフォーム	WindowsXP / 7 Mac OS X 10.6 以降
■CPU	Intel® Pentium® 4 3GHz以上
■メモリ	256MB以上
■HDD	20MB以上の空き領域

※Windows7は32bit/64bitに対応しています。

iOS

■プラットフォーム	iPhone 3GS以降 iPad

※iOSで利用できるクラウドストレージサービスは
Dropboxのみとなります。

認証サーバ / 管理サーバ/その他

■プラットフォーム	CentOS 5
■CPU	Intel® Pentium® 4 3GHz以上
■メモリ	1GB以上
■HDD	200MB以上の空き領域
■ブラウザ	Internet Explorer 8以降 Safari 4以降
■その他	WebServer　Apache / Tomcat Database　PostgreSQL8以降 アカウントファイル送付用メールサーバー