

プロキシ再暗号化

Proxy Re-encryption Systems



氏名
Name

中村 太
Futoshi Nakamura

早坂 健一郎
Kenichiro Hayasaka

井山 政志
Tadashi Iyama

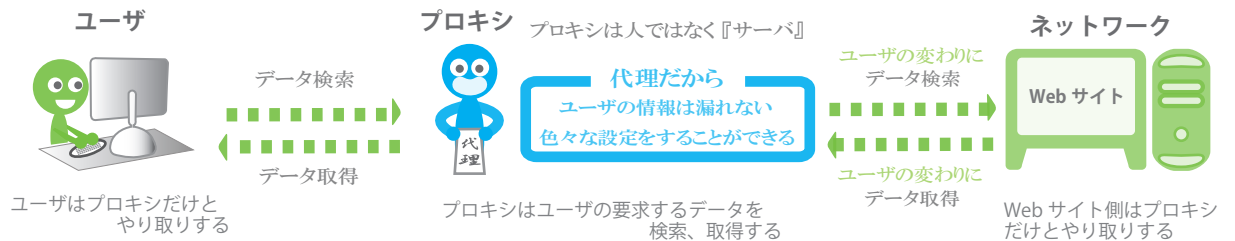
概要

Uploder Proxy Transform Alice's contents

我々が作製した【UP太】は暗号化されたデータを管理、保存するアップローダ・アプリケーションである。『プロキシ再暗号化』を利用して、複数人でのデータ共有が安全で簡単に行えるようになった。

プロキシ

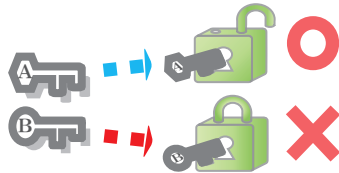
プロキシとは、「代理・仲介」という意味である。プロキシは、ユーザとネットワークの間に存在し、『データ取得』や『他のユーザとのやり取り』などの作業を代理処理する。



再暗号化

暗号化しているデータを再び暗号化することである。この操作によって権利を譲渡する。つまり、自分しか復号化できない暗号文を自分以外の人が復号化できるものに変換する。ここでは南京錠を暗号文として説明している。南京錠の鍵が開いていない状態を『暗号化』、開いている状態を『復号化』と表している。

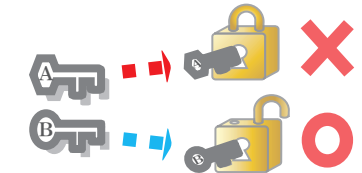
南京錠を開ける鍵が二つある。しかし、この南京錠はAの鍵しか開けられない。



緑の南京錠にBの鍵の情報を加え、再び暗号化を行う。これを再暗号化鍵と呼ぶ。

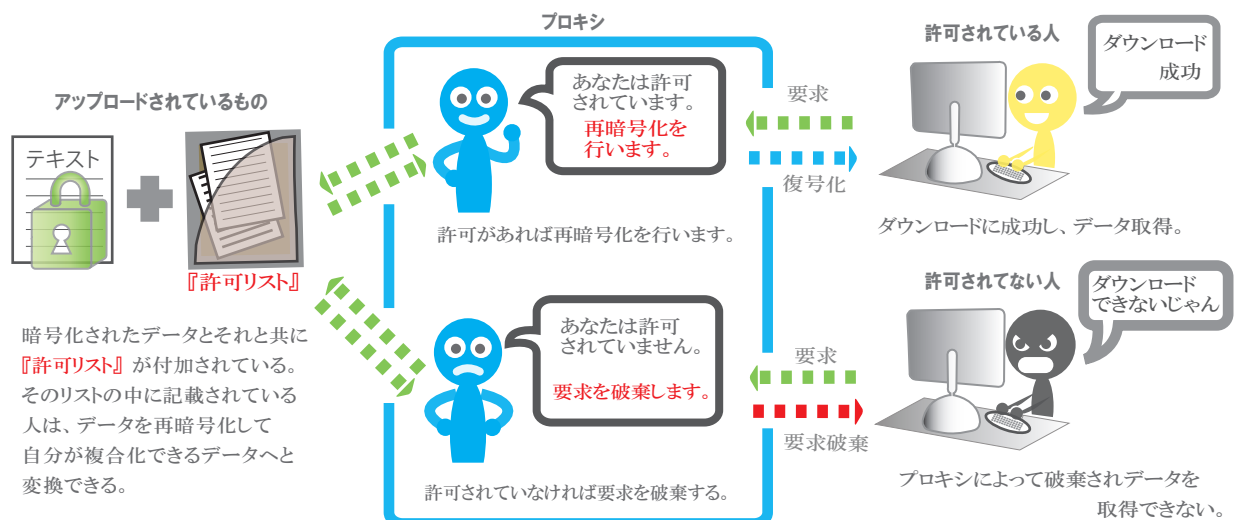


再暗号化鍵は、Aの鍵は開けられない。Bの鍵は開けることができるようになる。



我々が作製したアプリケーションは暗号化されたデータを管理、保存している。その暗号化を解くことができるのは、アップロードした本人とその人が許可を出した人のみであるため、データの中身を傍受するとはできない。また、このアプリケーションでは『プロキシ再暗号化』の応用として実現するアクセスコントロールを用いている。アップロードしたデータに付加する『許可リスト』をプロキシが判断し、ダウンロードできる人を制限する。

UP太



このアプリケーションの活用としては、会社や学校などのその内部だけでデータ共有を行う場所などが上げられる。今後の応用例としては、携帯など小型端末への組み込みで『転送システム』などが考えられる。