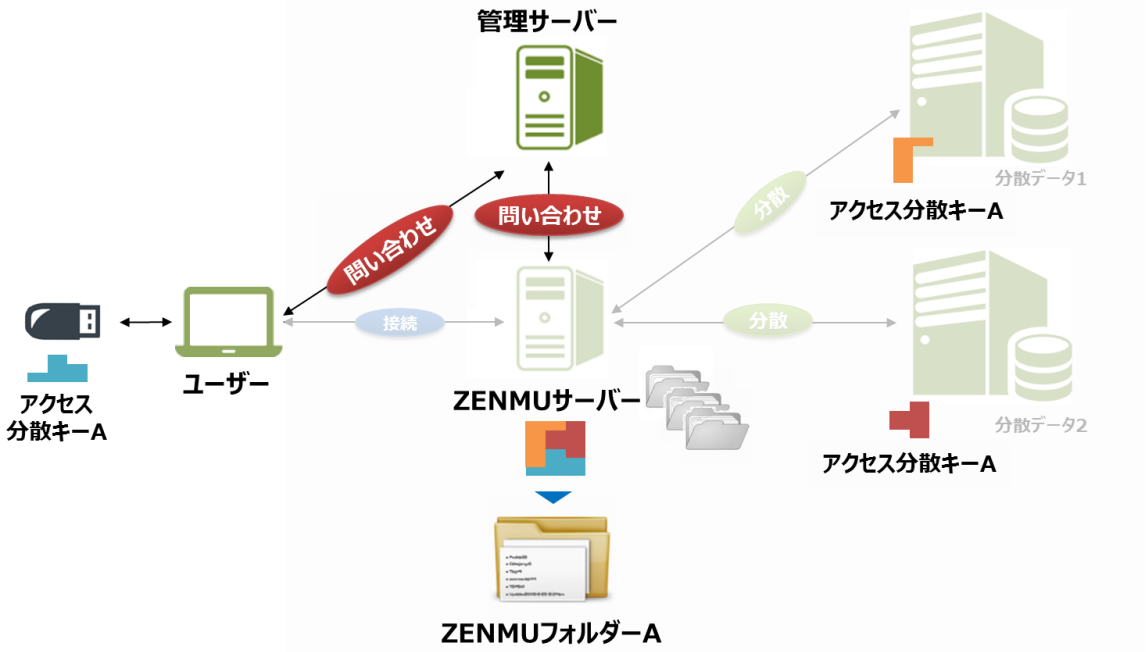
【添付資料】

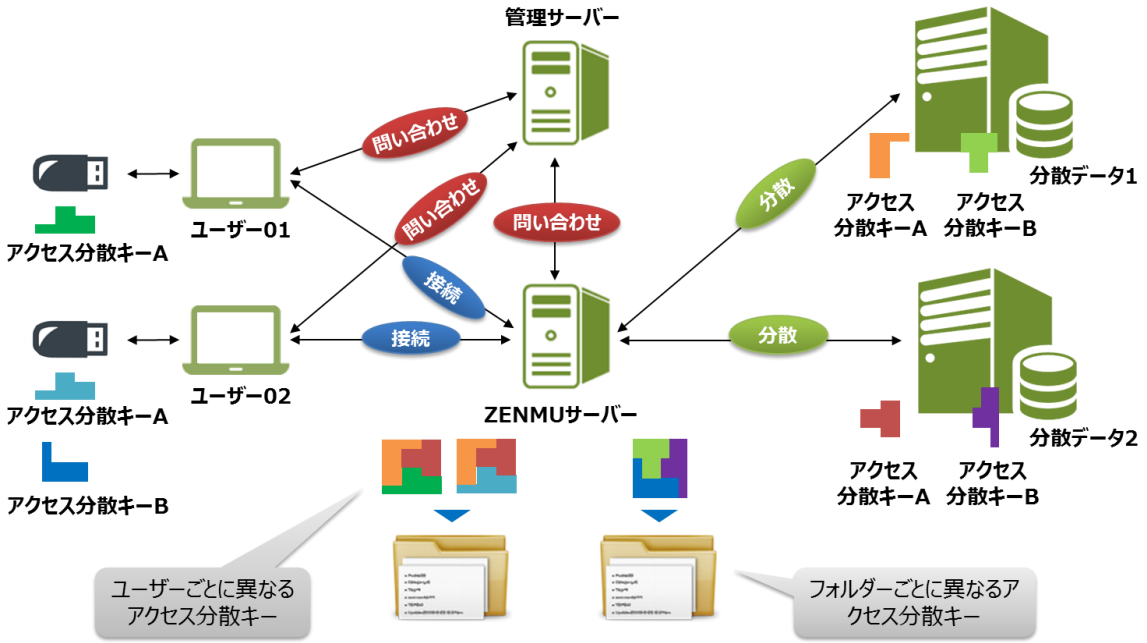
1. 「システム管理」と「情報管理」の分離と「アクセス制御」

- 従来の無意味化データの分散管理に加え、データへのアクセス制御の機能を追加
- 情報（ここではフォルダーA）にアクセス許可されたユーザーは、情報のオーナーからアクセス分散キーを取得
- アクセス分散キーは、情報の分散データの格納先にもあり、3 つのアクセス分散キーが揃うと、情報を分散・復号するために ZENMU のアルゴリズム・パラメーターが復号し、分散・復号プログラムが有効となる
- それにより、分散データが情報として利用可能となる



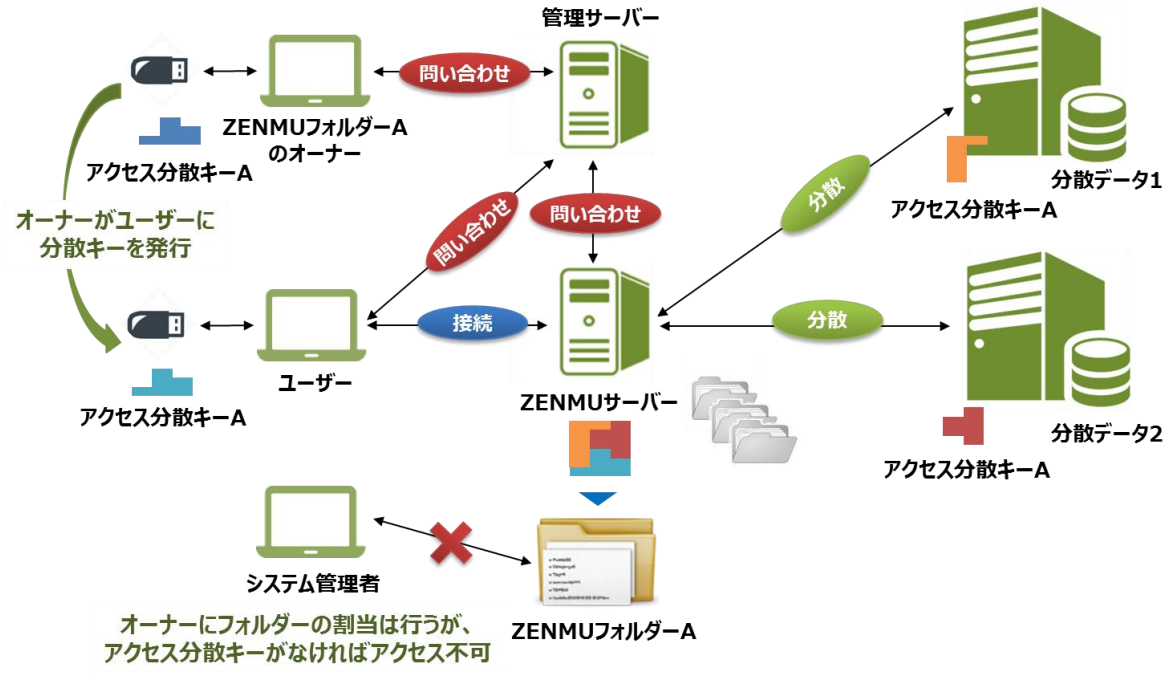
2. アクセス制御

- ユーザーは、フォルダーごとのアクセス分散キーを持つ
- ユーザーごとにアクセス分散キーが異なるので、他人のアクセス分散キーを使用することはできない
- ユーザーのアクセス分散キーはそれぞれ異なるが、どの分散キーでも復号可能（シャミアの秘密分散法）



3. 「システム管理」と「情報管理」の完全分離

- システム管理者がオーナーに、フォルダー領域の割当を行う
- オーナーは、領域を ZENMU フォルダーとして有効化。同時に、アクセス分散キーが生成される
- オーナーが、フォルダーにアクセスを許可するユーザーにアクセス分散キーを発行。アクセス分散キーは、ユーザーごとに異なる
- アクセス分散キーが無ければ、分散データを復号することができないため、たとえシステム管理者であっても情報にアクセスできない



4. アクセス分散キー

- 情報を分散・復元するための ZENMU のアルゴリズム・パラメーターの分散片
- 3 つ（各分散データ保管先のアクセス分散キーとユーザーのアクセス分散キー）が集まるとアルゴリズム・パラメーターが生成され、情報の分散・復号のプログラムが有効になる。
- シャミアの秘密分散 (k,n)閾値分散の技術を利用。3 つが揃うと復号可能なため、ユーザーごとに異なる分散キーでも、復号可能。

以上