秘密分散と LR-AKE クラスターモードとの違い

秘密分散方式は、手元でデータを複数のシェア（分割情報）に分割し、それらを「何らかの方法でどこかに」持って行き、元データを復元する際には、逆に「何らかの方法で」それらのシェアのいくつかを手元に集め元データを復元する方式です。

ＰＣ上のデータとＵＳＢメモリ上のデータに分割するという方法がよく利用されています。しかしながら、データを復元するためには、その両方が必要となるため、カバンの中には、ＰＣとそのＵＳＢメモリが一緒に入っており、カバンを盗まれると情報が漏えいするというケースもあると思われます。あるいは、ＵＳＢメモリを紛失するとデータを復元できなくなるため、バックアップのＵＳＢを様々な場所に置いており、気付いたらその１つが盗まれており、後日ＰＣも盗まれデータも漏えいするというケースもあると思います。

逆に、この「何らかの方法でどこかに」を「通信により遠隔地に」とした場合に問題となってくるのが、遠隔サーバと相互認証を行い安全な通信路を確立するための認証鍵共有方式として何を採用するかです。

例えば、SSL/TLS サーバ認証とパスワード認証を採用した場合、サーバから情報が漏れると、「単にシェアが漏れるだけでなく」、利用者に成り済ますためのパスワード情報も漏れてしまいます。（オフライン全数探索でパスワードを特定することは非常に容易になってきております）。
利用者の多くはパスワードを複数のサイトで使い回しているため、このような場合、攻撃者は別のサーバにログインして、残りのシェアも入手でき、本来であればしきい値以下のシェアしか漏えいしていないにも関わらず、元データの復元が可能となります。

逆に、利用者にサーバに接続するための鍵を持たせた場合、利用者がそれを落としたり、盗難に遭ってしまうと、その利用者はサーバにログインできなくなり、元データを復元するために、その利用者は各サーバを周り、個別にシェアを集めて来なくてはならなくなりますが、今度はそこでのユーザ認証が問題になります。逆に、その鍵のバックアップを取った場合には、バックアップからの漏えいが問題となります。

LR-AKE は秘密分散方式をオンラインで使う場合に、その情報漏えい耐性と可用性を最も高めることができる相互認証鍵共有方式であり、**秘密分散方式と連携させて使う技術になります。**

LR-AKE は秘密分散とは競合する技術でございません。

その上、LR-AKE は利用者がサーバにログインする度に、シェアや認証情報を更新させるため、時間差でしきい値以上のシェアが漏えいしたとしても、元データを復元できないという利点もあります。