ネットワーク分散型プライベートストレージの提案

Private Network Storage Using (*k*,*n*)-Threshold Secret Sharing Scheme

粂田　悠甫*,　　本間　啓道*
Yusuke KUMEDA*,　Yoshimichi HONMA*
*奈良工業高等専門学校専攻科　電子情報工学専攻
* Faculty of Advanced Engineering at Nara National College of Technology
Email: {kumeda, honma}@info.nara-k.ac.jp

あらまし：データの重要性が増し，秘匿性と対故障性を持つバックアップ手法が求められている．データを暗号化し，ネットワーク上に分散させるネットワーク分散型プライベートストレージを提案する．
キーワード：(*k*,*n*)しきい値秘密分散法，ハイブリッド P2P，ゼロ知識証明

1. はじめに

データのバックアップ手法として，従来では，DVD やテープなどの記憶媒体に記憶する方法があるが，物理的な破損による耐故障性の問題が存在する．近年では，ネットワークストレージに保存する方法があるが，サービスの管理者がデータにアクセス可能であるといった秘匿性の問題がある．そこで，本研究では，データを暗号化し，ネットワーク上に分散させるネットワーク分散型プライベートストレージを提案する．また，災害などで手元のデータが完全に消失したとしてもバックアップから復旧が可能で，秘匿性を持つことを要件とする．

2. 研究理論

提案手法では，暗号化したデータを，P2P ネットワークの参加者の端末にバックアップする．データを復旧する際はそれらを回収し，復号する．データの暗号化に使用する(*k*,*n*)しきい値秘密分散法，ハイブリッド P2P，データを回収する際の認証に使用するゼロ知識証明について述べる．

2.1 (*k*,*n*)しきい値秘密分散法

(*k*,*n*)しきい値秘密分散法[1]は，データを *n* 個のシェアに分割・暗号化する暗号化方法である．復元は *n* 個のうちの任意の *k* 個のシェアがあれば可能である．そして，シェアが *k* 個集まらない限りは復元が不可能で，参加者たちが持っている分散情報からは秘密情報の推測も不可能である．実装するにあたり，復元する際に必要な情報が書かれた鍵ファイルを作成することが必要となった．鍵ファイルには，分散したシェアのファイル名や元のデータのメタ情報を格納する．復元の際には，鍵ファイルの情報から分散したシェアを回収する．

2.2 ハイブリッド P2P

ネットワークは，その形態によって二種類に分類される．一つは，処理を要求するクライアントと要求に結果を返すサーバで構成される関係がサーバクライアント型である．対して，もう一つは接続されている端末(以後，ノード) 同士が通信を行い，互いに処理を要求したり，結果を返したりする，対等な関係で構成される P2P 型である．サーバクライアント型と P2P 型のネットワークの概略図を図 1 示す．

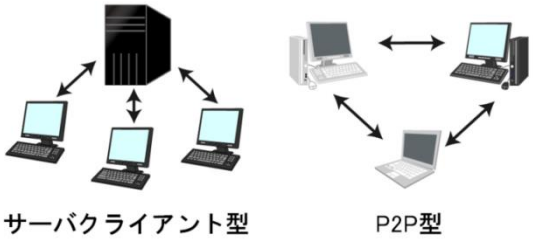

図 1　サーバクライアント型と P2P 型

P2P 型の中でもハイブリッド P2P 型[2]は，特定の機能に関してのみサーバクライアント型の関係を許し，サーバのような役割をする特別なノードを用意する．このノードをスーパーノードと呼ぶ．ハイブリッド P2P 型のネットワークの概略図を図 2 示す．

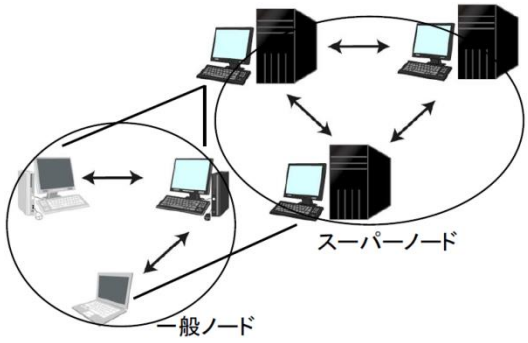

図 2 ハイブリッド P2P 型

2.3 ゼロ知識証明

ゼロ知識証明[3]は，証明者が情報 S を知っていることを，情報 S 自体は検証者に伝えることなく，検証者からの問に答えていく形式で証明する．本研究では，ユーザ認証にゼロ知識証明を用い，パスワードを相手に伝えることなくユーザ認証を行う．パスワードを知らない第三者が 1 回の検査をすり抜ける確率は$\frac{1}{2}$であり，検査を *t* 回繰り返すと$\left(\frac{1}{2}\right)^t$となる．

3. 提案手法

3.1 前提条件

提案手法の前提条件を以下に示す.

A) スーパーノードは遠隔地に 7 台設置する.
B) 7 台のスーパーノードが存在する地域で，7 区分にして一般ノードの管理を行う.
C) データは 7 区分に均等に分散する.
D) スーパーノードは常に 4 台以上稼働している.

災害に遭った後にデータの復元を行う場合には以下のような条件を仮定する.

E) 被災以前のデータは，記憶しているアカウント名とパスワードのみである.
F) 自分の居る区分のデータは消失したとする.
G) 他の区分のデータも 20%が何らかの理由で消失したと考える.
H) データの回収を開始する時点では，データを持っているが電源が点いていないなどで，アクセス不可能である端末が 30%あるとする．それらの端末の 50%は 1 日待つことでアクセスが可能となり，データを回収できると考える.

3.2 暗号化

バックアップしたいデータ D を(k,n)閾値分散法，$k=k_1,n=n_1$ で秘密分散をすることで，n_1 個のシェア D_i(i は変数，以後も同様とする) と鍵ファイル C が生成される．シェア D_i を k_1 個と鍵ファイル C を集めることで，データ D を復元することができる．さらに，生成された鍵ファイル C を再び(k,n)閾値分散法，$k=k_2,n=n_2$ で秘密分散することで，n_2 個のシェア C_i，鍵ファイルの鍵ファイル Ca が生成される．Ca は各 C_i に付属させる．よって，鍵ファイル C は C_i を k_2 個集めることで復元が可能となる．データの暗号化のイメージ図を図 3 に示す.

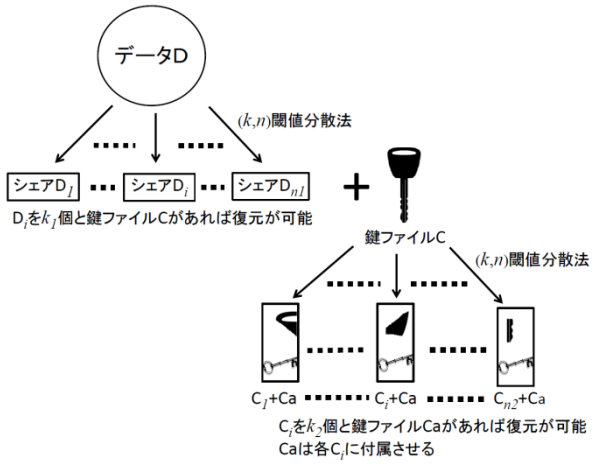

図 3　暗号化のイメージ

3.3 シェアの分散

シェア D_i はネットワークの各ノードで保管する．なお，各ノードの管理者はシェア D_i が誰のものであるか，どのようなファイルであるかを，知ることができない．各 C_i はスーパーノードが 1 つずつ保管し，ダウンロードするには認証をする必要がある．分散したデータのイメージ図を図 4 に示す.

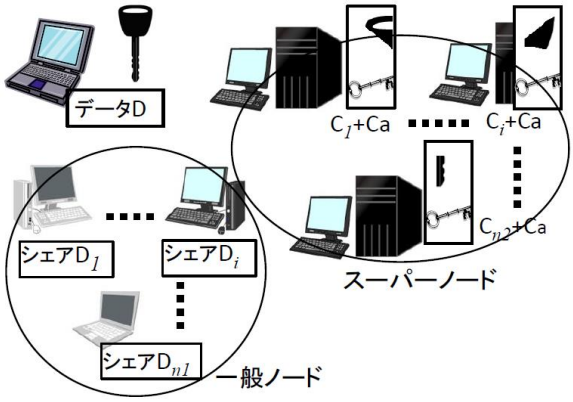

図 4　分散したデータのイメージ

3.4 データの復元

復元する際には，鍵ファイルCを復元する必要がある．そのため，スーパーノードがゼロ知識認証で本人確認を行った後，C_iをダウンロードする．C_iが k_2個集まれば鍵ファイルCが復元でき，データDを復元するために必要な断片の情報がわかる．その情報から必要なシェアD_iを検索し，ダウンロードする．D_iをk_1個集めて，元のデータDが復元される.

3.5 安全性

一般ノードの管理者は自分のもとにあるデータが誰の物であるか，どのような物であるか知ることができないため，特定のファイルを復元することができない．また，スーパーノードが管理する鍵ファイルの断片 C_i はダウンロードする際には認証が必要であり，しきい値 k_2 までならば，スーパーノードが乗っ取られたり，管理人が悪意を持って行動しても特定のファイルを復元することはできない.

4. 今後の計画

シェアを保管するノードの位置が物理的に散らばるようにノードを選択する方法，分散したシェアを効率良く回収する方法を考案する．最終的には，規模を縮小したプロトタイプを実装し，実用性や安全性について検証を行う.

参考文献

(1) 尾形わかは：“情報理論的に安全なパスワード付秘密分散法の安全性と効率化”，2013 年 暗号と情報セキュリティシンポジウム概要集（2013）
(2) 岩田真一：“なるほどナットク! P2P がわかる本”，オーム社（2005）
(3) 小林信博，岡本隆司，桜井幸一：“零知識証明技術のコンピュータ間認証への適応”，情報処理学会第 44 回全国大会講演論文集 pp.265-266（1992）