

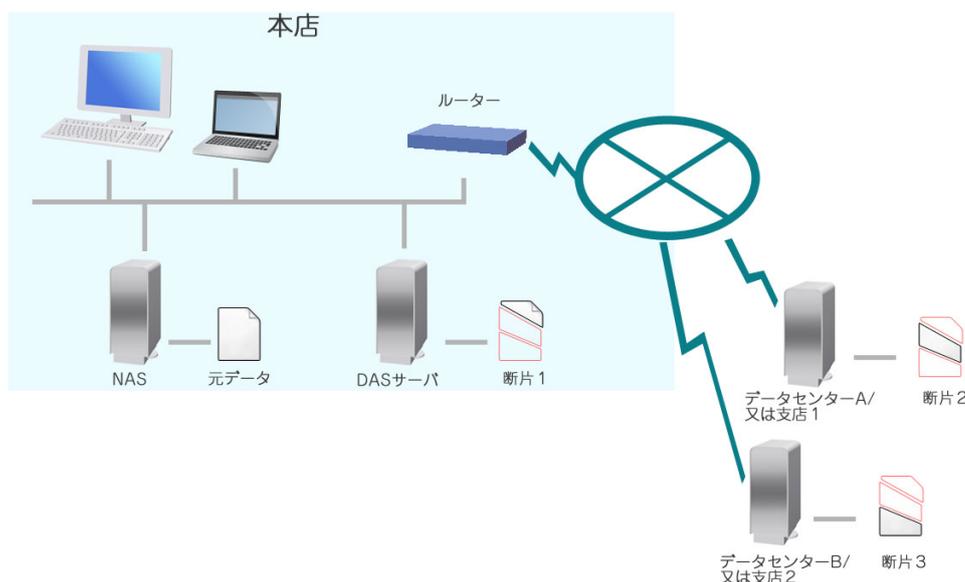
Data Alive System

低価格の投資でデータを長期・安全保管を求める方へのご提案

*1

*2

D.A.S.は、「電子的割符」技術による「しきいち秘密分散方式」を用いて、対象データを暗号化された3つの断片に分割し、各断片をそれぞれ別々の場所に保管することで、元のデータを天災や事故あるいは盗難などから守ろうとするものです。



D.A.S.を導入するメリットは？

データのバックアップは？

パソコン内のファイルはデータの共用とバックアップのために、RAID機能を組み込んだファイルサーバや、NASの様なネットワークに直接接続される冗長型ディスクに格納するのが、ごく一般的な使い方でしょう。

それだけでは、

一極集中型で特定のサーバやNASにいくら設備投資をしても、ハードウェアのトラブル、火事や地震等の天災盗難などの人災から逃れることはできません。

そこで、

「電子的割符技術」で分割された断片データを別々の離れた場所(地震等が発生しても、影響を受けないように、たとえば、北海道と東京と大阪)に保管しておけば、その内2カ所の断片データが入手できれば、元のデータを復元することが可能です。

さらに、

データの盗難や紛失などが発生しても、断片自身は暗号化されており、さらに原理的に1断片だけでは元データを復元することができません。従来の様に一極集中ではなく、暗号化した上で分割・分散することで、より安全で、確実なバックアップ方式の提供が可能となります。

これがData Alive Systemです。

電子的割符ってなに？

「電子的割符」は、割符の名の通り元データを分割するのですが、単純に分割している訳ではありません。

例えば、

「電子的割符」は、割符の名の通り元データを分割するのですが、単純に分割している訳ではありません。例えば、コーヒーゼリーを3つに分けても、その断片はやっぱりコーヒーゼリーです。これでは分割した意味がありません。ですから「電子的割符」では、元データの一部に、別の不純物データをわざと添加し、ランダムにかき混ぜた後、3分割しています。

ちょうど、コーヒーゼリーにミルク（別の添加物）を入れてかき混ぜた後、それを3つに分けたイメージです。一端ミルク入りコーヒーゼリーとなったものは、その後いくらかき混ぜ続けても、元のゼリーとミルクに分離することはありません。一度不純物が添加されると元に戻すのが如何に困難であるかは、容易に想像できると思います。



データ保管の安全性に優れている!!

「電子的割符」でできた断片は同じ場所に保管しません。別々の場所に保管します。ですから、もし断片の一つを入手し、例えば、大量のCPUリソースを使って暗号を解いたとしても、断片一つではデータが欠落していますから、もとのデータを再現することは原理的に不可能です。また各断片ファイル名は、それ自身が暗号化されていますから、各断片単独では、自身の組み合わせ相手がありません。正しい組み合わせは、相互の断片関係を記録している管理情報にのみ記載されています。この点でも分散保管されていることのセキュリティ上の優位性は明らかです。

写真などの元データ



元データから分割した断片データ

巨大なCPUパワー



元データの一部のまま。復元しようにも、断片の1部では元には戻すことが出来ない。

しきいち秘密分散方式ってなに？

分割断片は単に分割されている訳ではありません。3つの断片のうち、2つがあればもとのデータを復元できるように内部で論理的に冗長化されています。データをA B Cの3つの論理的ブロックに分け、個々の断片がA B、B C、C Aの論理ブロックを持っているならば、任意の2つの断片があれば、もとのデータA B Cが再現できます。このような秘密分散方式の事を、しきいち秘密分散方式と呼びます。

D.A.S.概要

- | | | | |
|----|--------|---|---|
| 1. | サーバOS | : | Linux |
| 2. | サーバCPU | : | インテル系 CPU Core 2Duo 相当 |
| 3. | メモリ | : | 512MB |
| 4. | 専用ハード | : | PCI Express16 × 1 の分割・暗号化専用アクセラレータボードを使用。 |
| 5. | その他 | : | 保管できるファイルフォーマットやファイル数には特に制限はありませんが、使用量に応じてローカルハードディスクの容量を調整する必要があります。 |
| 6. | クライアント | : | Mac OS X (10.4 以降) Windows XP 以降 |

*上記仕様は予告なく変更する場合がありますので、ご了承ください。

D.A.Sを組み込んだシステム構築されたい方は是非ご相談ください。
お客様のご希望されるシステム形態をご提案・お見積もりいたします。

お問い合わせ：

株式会社 羅針ネット

〒650-0022 兵庫県神戸市中央区元町通4丁目4-8 タイムビル6階

TEL：078-362-1102 FAX：078-362-1107

E-Mail: request@rashin.net.co.jp

http://www.rashin-net.co.jp/

2010.08 現在