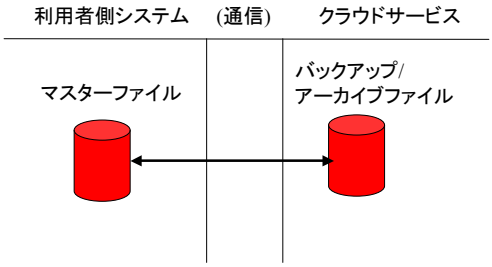
秘密分散技術と
セキュアクラウドストレージ

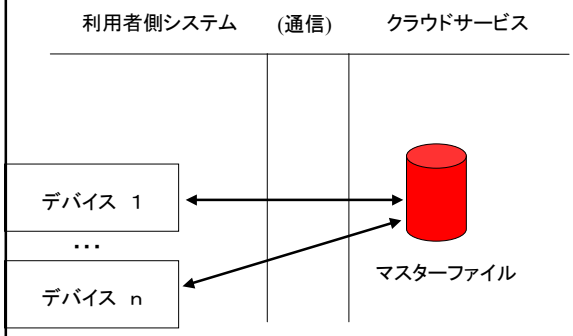
2012年2月8日
（株）IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp

クラウドストレージの利用場面

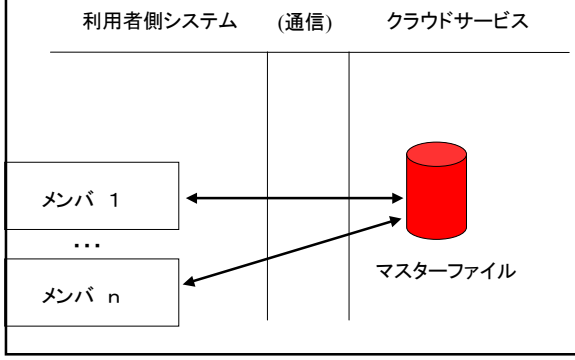
バックアップ/アーカイブをクラウドサービスへ



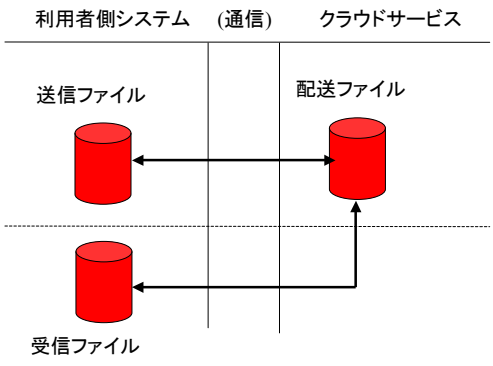
個人マスターをクラウドサービスへ



グループマスターをクラウドサービスへ

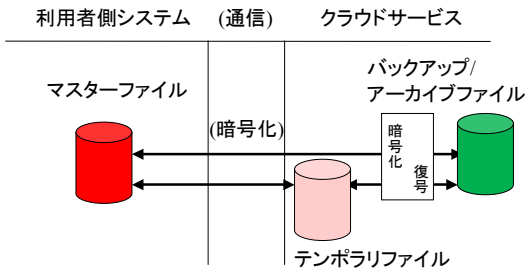


配送チャネルとしてクラウドサービスを



安全なバックアップ/アーカイブ

暗号技術を応用した
安全なバックアップ/アーカイブ（1）



サービス例

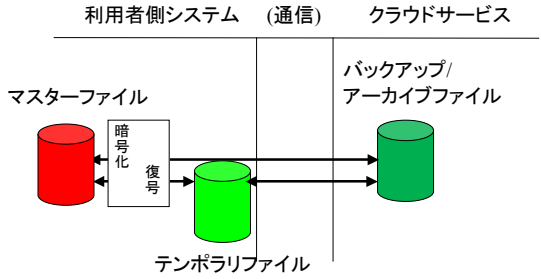
＜有料サービス＞

（1）KDDIセキュアシェア（KDDI） HTTPS AES
（2）Nomadeskファイルサーバ（ハイパー） HTTPS? AES
（3）ベライゾンクラウドストレージ（ベライゾン） HTTPS AES

＜無料サービス＞

（1）Dropbox（Dropbox） HTTPS AES

暗号技術を応用した
安全なバックアップ/アーカイブファイル（2）



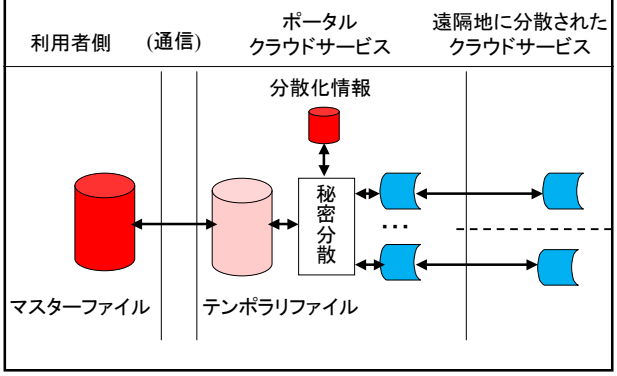
サービス例

＜有料サービス＞

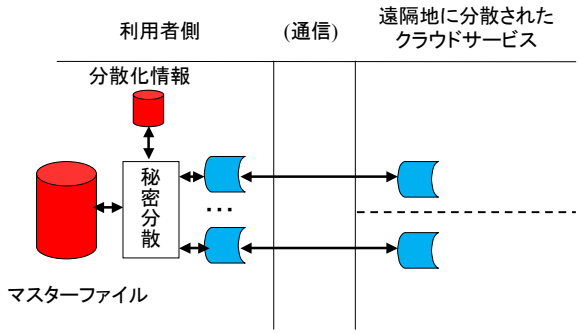
（1）マクニカネットワークス
　＊StorSimple社の
　　ハイブリッドクラウドストレージアプライアンス
　＊ニフティクラウドでのサービス展開

（2）バリオセキュアネットワークス
　＊DataProtectアプライアンス
　＊国内IDCでのサービス展開（ブルーシフトとの連携）

秘密分散技術を応用した
安全なバックアップ/アーカイブ（1）



秘密分散技術を応用した安全なバックアップ/アーカイブ（2）



サービス例

（1）SecureCube / Secret Share（世界分散ストレージ）

＊NRIセキュアテクノロジーズ(株)

＊グローバルフレンドシップの独自アルゴリズム「GFI電子割符」を 採用

＊秘密分散技術によるデータ管理サービス公開実証実験

＊IIJがクラウドストレージを利用した秘匿分散のためのアプリケーション開発と検証のPJを平成22年度実施（NRIセキュア協力）

＊日立ビジネスソリューションも「GFI電子割符」を採用した製品、電子割符データエスクローおよびモバイル割符、を提供中

（2）PrivSHELTER（ASP型の個人情報管理サービス）

＊(株)プライブ・シェルター

＊NTTコミュニケーションズが開発した「情報量依存型暗号化技術」（独自のアルゴリズムによって重要データを1つでは意味の成さない3つのデータに分散保管する技術）を採用

（3）MultiSHELTER

＊(株)レグニア

＊秘密分散（乱数化）技術を利用した記録管理システムで、データの重要度に応じ、秘密分散、暗号化、平文で保管

＊日本ユニシスグループが、クラウドサービスビジネスに採用

（4）TRUSTAS/TRUSTASフレーム

＊リアルシス(株)<トラステッドソリューションズ(株)>

＊AONT(All or Nothing Transform) 方式を採用

＊セキュアなバックアップサービス（メディア＋オンライン）およびセキュアな文書管理・閲覧サービス

＊日本通運(株)のメディア保管サービスと連携

（5）J2ET（ジェッツ）エスクローサービス

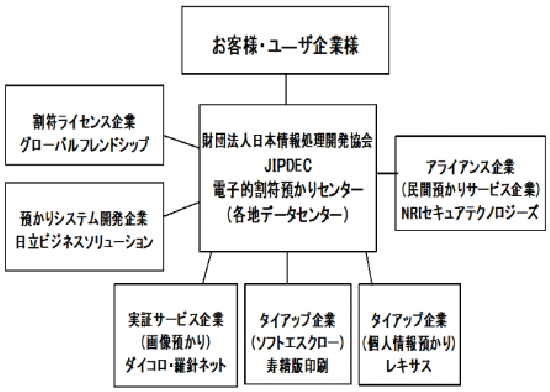
＊（財）日本情報処理開発協会(JIPDEC)が提供するサービス基盤

＊「ユーザサイドでの閾値秘密分散実施基盤」および「秘密分散により生成される1分割片の預かり基盤」から構成

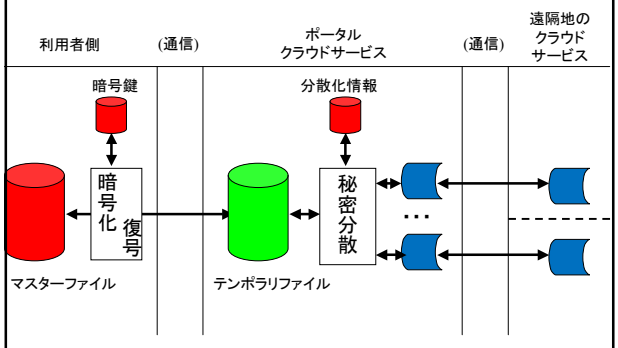
＊「ユーザサイドでの閾値秘密分散実施基盤」は、復元に必要な情報を原則、ユーザだけが知っている状況を作り出すためのサービス

＊「秘密分散により生成される1分割片の預かり基盤」は、復元に必要な分割片を容易に集められない状況を作り出すためのサービス

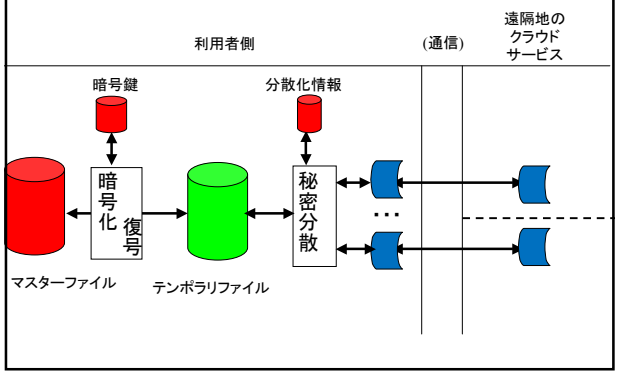
電子的割符預かり(J2ETエスクロー)サービス体制図



暗号技術と秘密分散技術を応用した安全なバックアップ/アーカイブ（1）



暗号技術と秘密分散技術を応用した安全なバックアップ/アーカイブ（2）

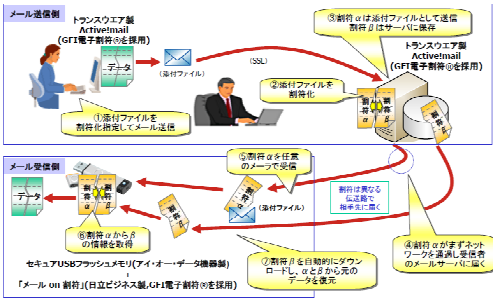


ウティマコとグローバルフレンドシップが暗号化＋秘密分散技術で協業

使用例

（1）割符メールソリューション

＊日立ビジネスソリューション（株）、（株）アイ・オー・データ機器、（株）トランスウエア、グローバルフレンドシップ（株）の協業による製品



Information Dispersal Algorithm（情報分散アルゴリズム）

Michael O. Robin氏が1989年に開発

サービス例

（1）Dispersed Storage Network

＊Cleversafe Inc.（米国）

＊『Cauchy Reed-Solomon Information Dispersal Algorithm (IDA)』として知られる数学公式を利用

（2）S*Plex3クラウド・ストレージサービス

＊スカパーJSAT（株）

＊スカパーJSATが開発した特許技術「 S*Plex3テクノロジー」は、Identity Based Encryption(IBE)とInformation Dispersal Algorithm(IDA)を採用

＊NTTPCコミュニケーションズがWebARENA Symphony バックアップサービスへ「 S*Plex3テクノロジー」を採用

“クラウドストレージを利用した秘匿分散のためのアプリケーション開発と検証”事業報告書（平成23年3月31日　IIJ）より

商用サービスとして利用されている秘密分散技術

サービス名	事業会社	秘密分散技術	複数DCへ分散I/F	対応プラットフォーム
SecureCube SecretShare	NRIセキュアテクノロジーズ	GFI電子割符 ・処理速度高速 ・シェアが1つなくなっても復号可能 ・シャミアの秘密分散法よりはシェアのサイズが小さくなる ・シェアサイズの可変分割可能	独自仕様	Windows
TRUSTAS	リアルシス	AONT方式 ・処理速度高速 ・シェアが1つでもなくなると復号できない。 ・シェアの合計サイズが元ファイルと同じ ・シェアサイズの可変分割可能	独自仕様	Windows
TAS	SBI Net Systems	(k,L,n)しきい値秘密分散法 ・元ファイルが小さいサイズを想定 ・シェアが1つなくなっても復号可能 ・シャミアの秘密分散法よりはシェアのサイズが小さくなる ・シェアサイズの可変分割可能	秘密分散ライブラリのみであるため、分散I/Fはなし	Windows

“クラウドストレージを利用した秘匿分散のための
アプリケーション開発と検証”事業報告書（平成23年3月31日　IIJ）より

GFI割符技術への見解

ア　内閣官房情報セキュリティセンター（以下、NISC）より唯一の分散技術として認識
イ　秘密分散法ではないが、工学モデルとし同等のセキュリティ強度があるとの評価
　　（東京大学　山本教授）
ウ　処理速度が高速
エ　ファイルサイズ、種類に制限がない
オ　分割片のサイズを調整可能
カ　分割片が個人情報に該当しない（内閣府、経済産業省の見解あり）

リアルシス(株)の AONT秘密分散について

- 秘密分散法説明
- 災害対策リモート保管：
  TRUSTASサービスのご紹介
- 文書電子化・保管：
  TRUSTASフレームのご紹介

個人情報保護法の運用に関する検討状況について

平成23年6月15日
経済産業省・商務情報政策局・情報経済課

③ 個人情報の漏えいが生じた際の対策

経済産業分野を対象とするガイドラインでは、個人情報漏えいが生じた際に、事業者が高度な暗号化処理を施している場合、本人への通知や公表の省略を認めている。
この暗号化処理のように、本人への通知や公表の省略を認めてもよいと考えられる情報セキュリティ技術としては、

「存在してもアクセスさせない技術」（秘密分散など）、
「消去してしまう技術」（遠隔消去、時限消去など）
のような対策が有益との意見あり。

→ ただし、いずれも公的な認証制度がないため、法令で求めるレベルに十分な安全管理措置の判断基準はどのように確保するのかが課題

課題

（1）秘密分散アルゴリズムの整理
　　分類と体系化
　　情報分散アルゴリズムとの違い

（2）秘密分散アルゴリズムの客観的評価
　　情報分散アルゴリズムも含め

（3）セキュアクラウドストレージ利用方式の評価

（4）セキュアクラウドストレージサービスの
　　グローバル展開のための国際標準化