レグザクラウドサービス「TimeOn」を支える高信頼かつ高セキュアなクラウドストレージサービス基盤

Highly Reliable and Highly Secure Online Storage Platform Supporting "TimeOn" Regza Cloud Service

三木　正章　　林　　英史　　新貝　英己
■MIKI Masaaki　■HAYASHI Eiji　■SHINGAI Hideki

クラウドストレージサービスは利便性が高くユーザーは急速に増加しているが，共有時におけるデータ漏えいなどのセキュリティ面に加えて，データを長期間預けることができるかという信頼性の面で課題がある。

東芝は，これらの課題を解決するため，独自の再暗号化技術と，ユーザビリティを考慮した広域分散バックアップシステムとを導入した，クラウドストレージサービス基盤を開発した。再暗号化技術により利便性を犠牲にせずセキュリティを確保するとともに，広域分散バックアップシステムにより快適な応答時間とデータ高信頼性を実現している。当社はこの基盤を応用し，B2C（Business to Customer）サービスとしてレグザクラウドサービス「TimeOn」（以下，TimeOnと略記）の“クラウドアルバム”サービスやオンラインストレージサービス“デジタル貸金庫”を提供している。

Online cloud storage services are currently attracting an increasing number of users.　However, issues have been pointed out regarding the reliability of such services for long-term data storage and the security of data shared in or uploaded to the cloud.

To resolve these issues, Toshiba has developed a highly reliable and highly secure online storage platform incorporating its proprietary proxy re-encryption technology to ensure data security without sacrificing usability, and a wide-area distributed backup system to realize highly reliable data retention with a rapid response time.　We have applied this platform to cloud storage for business-to-customer (B2C) services, including the "Cloud Album" service of the "TimeOn" Regza cloud service that allows users to share data among TV products on the network, and the Digital Kashikinko online storage service for consumer PC products.

1　まえがき

クラウドシステム上のストレージサービスは，写真や動画など，増え続けるデジタルデータのバックアップや共有の場面で活用が進んでいる。例えば，ソーシャルメディア上で家族や友人に写真や動画を公開したり，個人で所持するパソコン（PC）やタブレット，スマートフォンなど複数のデバイス間でデータを共有したりするのにクラウドストレージは用いられる。また，家族の思い出が詰まったたいせつな写真の保管先をクラウドストレージにすれば，PC更新時の煩わしいバックアップ作業から解放される。

しかし，クラウドストレージを利用することに漠然とした不安を感じるユーザーも少なくない。操作が簡単な反面，ちょっとした操作ミスが思いがけないデータ漏えいに発展することがある。また，サービスプロバイダーの運用ミスによるデータの漏えい，ハードウェア障害によるデータの喪失や破壊などの可能性もある。

このような状況に対して，ユーザーからクラウドストレージに対する要求をまとめると，次のようになる。

(1)　複数ユーザー及び複数デバイス間で手間なく高セキュアにデータを共有したい

(2)　適切な応答時間でデータを保管することができ，長期間にわたり確実に預かってほしい

東芝は，これらの要求に応えるため，独自の再暗号化技術と，ユーザビリティを考慮した広域分散バックアップシステムとを導入した，クラウドストレージサービス基盤を開発した。

ここでは，この基盤の特長と，これを応用してB2Cサービスとして実現したTimeOnの“クラウドアルバム”サービスとオンラインストレージサービス“デジタル貸金庫”の二つのサービスの概要について述べる。

2　特長

クラウドストレージサービス基盤の特長は，再暗号化技術による共有データの暗号化とユーザビリティを考慮した広域分散バックアップシステムにある。

再暗号化技術により，データを共有する相手に鍵を配信する必要がなくなり，クラウドストレージ上で共有相手に合わせて鍵を付け替えてデータを配信できるようになった。クラウドストレージ上の鍵付替えは，データを復号することなく実施できるため第三者に見られないセキュアな状態が保たれる。

広域分散バックアップシステムは，データの信頼性を高めるために従来から用いられてきたが，今回これに，クライアントとデータセンター間のレイテンシ(注1)を抑えるようにシステム構

(注1)　データの要求から応答までの遅延時間。

成を工夫するとともに，サービス地域をスケーラブルに拡大できるようにしている。

以下に，それぞれの技術の特長について述べる。

2.1　再暗号化技術による簡便で安全なデータ共有

データを暗号化して共有する際のユーザー要件は，セキュリティと利便性の両立である。しかし，これらはトレードオフの関係にあり，以下に述べるように両方を同時に満足することは難しかった（**表1**）。

共通鍵暗号方式では，自分の鍵で暗号化してその鍵を共有相手にも教える。ユーザーは自分の鍵だけを管理すればよい（共有相手がN人いるとして，システム全体で鍵は最大N個）。暗号化後のファイルも一つであり余分なストレージ容量を消費しない（等倍）。一方で，一人の共有相手の不注意で鍵が漏れると，ユーザーのデータ全部が復号される可能性があり，セキュリティ面では脆弱（ぜいじゃく）である。また公開鍵暗号方式では，前述の共通鍵でのセキュリティ面の脆弱性は解消されるが，最大$N \times N$個の鍵ペアを管理する必要があり手間が煩雑になる。更に，同一のデータでも異なる暗号化を施して保管する必要があるため，ストレージ容量が最大N倍必要になる。

これら従来方式に対して再暗号化技術では，ユーザーが自分の鍵で暗号化したデータを，共有相手が復号できるように鍵を付け替えて配信できる[(1)]。この鍵の付替えはクラウドストレージ上で行われ，データ自体が復号されることはない。ユーザーは自分の鍵だけを管理すればよく（N個の鍵），ユーザー自身の鍵で暗号化したデータをストレージにアップロードするだけでよい（等倍）。共有相手に鍵を配信する必要もなく，万一共有相手又はデバイスから復号鍵が漏えいしたとしても，クラウドストレージ上の鍵付替え機能を無効化すれば，他の共有相手やデバイスには影響を及ぼすことなくセキュアな状態を保つことができる（**図1**）。

2.2　ユーザビリティを考慮した広域分散バックアップシステム

データ保管時に求められるユーザー要件に，長期間にわたって安心して預けられるかというデータの信頼性が挙げられる。また，クラウドストレージサービスでは，しばしば大容量のデータをやり取りするため，クライアントとデータセンター間のレイテンシを考慮しなければならない。

表1．再暗号化技術と従来の暗号方式との比較
Comparison of proxy re-encryption and other encryption schemes

共有における課題	再暗号化技術	共通鍵暗号方式	公開鍵暗号方式
セキュリティ	○ 影響範囲は限定的	× 鍵漏えい時に脆弱	○ 影響範囲は限定的
鍵の管理	○ 自分の鍵だけ （N個）	○ 自分の鍵だけ （N個）	× 自分＋相手の鍵 （$N \times N$個）
ストレージ容量	○ 容量等倍	○ 容量等倍	× 容量N倍

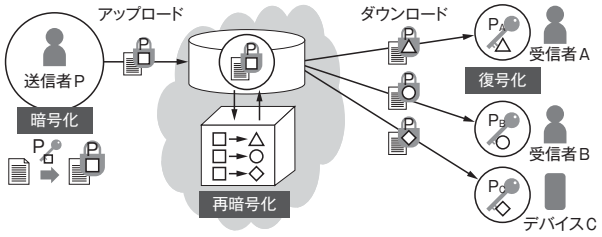

図1．再暗号化技術によるデータ共有 — データは復号せず，ユーザーやデバイスに応じて鍵を付け替える。
Data sharing using proxy re-encryption technology

今回開発したサービス基盤では，各地域のユーザーがアクセスするデータセンター，ユーザー最寄りのデータセンターを指示する管理用データセンター，及び各地域から独立したバックアップ専用のデータセンターを配置している（**図2**）。

サービス地域には複数のデータセンターを配置した。データは複数のデータセンターで相互にバックアップするようにしており，複数データセンター間で正しくデータをバックアップしたことを確認した後，ユーザーにデータ保管の応答を返すようにしている。更に，サービス地域のデータセンターからバックアップ専用のデータセンターに対して定期的なバックアップを行う。このデータセンターは，災害からの復旧などディザスタ リカバリの観点から，サービス地域とは地理的に離れた位置に立地している。それぞれのデータセンター内でハードウェアは冗長構成とし，ストレージはミラーリングされている。このようにして，データの完全性と信頼性を高めている。

ユーザーからデータ保管を直接受け付けるデータセンターは，応答時間の観点からサービス地域に配置する。複数のデータセンター間の相互バックアップは地域内で行われるため，比較的短い処理時間で済む。ユーザーの最寄りのデータ

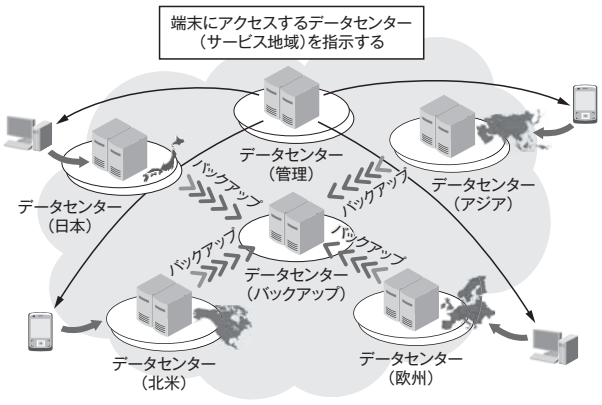

図2．広域分散バックアップシステムの概要 — 管理サーバからアクセス先を指示することでユーザビリティを損なわないサービス提供が可能である。サービス地域の追加も容易である。
Overview of wide-area distributed backup system

センターを指示する管理サーバは，全サービス地域からネットワーク的に等距離にあるデータセンターに配置される。これにより，各地域のユーザーは適切な応答時間でサービスを受けることができる。管理サーバと同様に各地域から等距離に配置したデータセンターへのバックアップは，リアルタイムには行わずユーザーの応答時間に直接影響が及ばないようにしている。

新たな地域でサービスを開始する際には，管理サーバにその地域の登録と，その地域向けのデータセンターを登録する。バックアップサーバにもバックアップ元を登録することで，その地域に対しても同様のサービスを提供できるようになる。

3　B2C応用事例

3.1　クラウドアルバム サービス

TimeOnのコンセプトの一つは，リビングにあるテレビを中心に据えて，PCやスマートフォンなど様々なデバイスを持つ家族や，友人，遠く離れた祖父母のテレビをつないで，クラウドストレージ上に写真やメッセージを保存し共有することである。

そこで当社は，TimeOnのストレージ部分にクラウドストレージサービス基盤を応用した。このサービス基盤が持つ再暗号化技術や広域分散バックアップシステムの仕組みが，ユーザーの居場所を越えたサービスであるクラウドアルバムにおいて，簡単で安全なデータ共有を実現している（**図3**）。

3.2　デジタル貸金庫[(2)]

ネット利用者を対象とした当社アンケート調査では，回答者のほぼ80％がデータの漏えいと消失のリスクを挙げている。そこで当社は，個人のたいせつなデジタルデータを強固なセキュリティで長期間保管することを目的としたクラウドストレージサービスのデジタル貸金庫を2012年11月から開始した。デジタル貸金庫の高セキュア・長期保管という特長は，クラウドストレージサービス基盤を適用することで実現している（**図4**）。

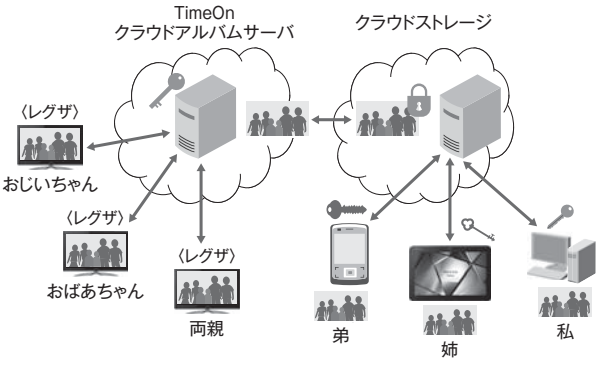

図3．クラウドアルバム サービスにおけるクラウドストレージ — クラウドストレージサービス基盤を応用することで，場所に依存しない複数ユーザー並びにデバイス間のデータ共有をサポートしている。

Cloud storage in Cloud Album service

＊画面はイメージで，予告なく画面や仕様が変更となる場合がある

図4．デジタル貸金庫のトップ画面 — Windows®(注2)8のモダンUI（ユーザーインタフェース）スタイルに対応した。

Top screen of Digital Kashikinko™

4　あとがき

再暗号化技術と広域分散バックアップシステムを適用した高信頼かつ高セキュアなクラウドストレージサービス基盤について述べた。このサービス基盤をB2Cのサービスに応用し，TimeOnのクラウドアルバムやオンラインストレージサービスのデジタル貸金庫に適用した。

今後，信頼性及び高セキュリティが要求されるB2B（Business to Business）市場にクラウドストレージサービス基盤の適用を展開していく。

文　献

(1)　吉田琢也 他．クラウドサービス上でより安全なデータ共有を実現する再暗号化技術．東芝レビュー．66，11，2011，p.18－22.
(2)　東芝．“デジタル貸金庫”．<http://tosafebox.com/>，(2013-03-29参照).


三木　正章　MIKI Masaaki
デジタルプロダクツ&サービス社 プラットフォーム&ソリューション開発センター プラットフォーム・ソリューション開発第五部主務。クラウドサービスの開発に従事。
Platform & Solution Development Center


林　　英史　HAYASHI Eiji
デジタルプロダクツ&サービス社 プラットフォーム&ソリューション開発センター プラットフォーム・ソリューション開発第五部主務。クラウドサービスの開発に従事。
Platform & Solution Development Center


新貝　英己　SHINGAI Hideki
クラウド&ソリューション事業統括部 クラウド・ソリューション第三部参事。クラウドサービスのマーケティング・企画業務に従事。
Cloud & Solutions Div.

(注2)　Windowsは，Microsoft Corporationの米国及びその他の国における商標。