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

Proxy Re-encryption Scheme for Secure Data Sharing in Cloud Services

吉田　琢也　　松下　達之
■YOSHIDA Takuya　■MATSUSHITA Tatsuyuki

“再暗号化技術”とは，あるユーザー向けに暗号化されたデータを復号することなく別のユーザーの鍵に付け替え可能な公開鍵暗号技術である。暗号化しても利便性を下げることなく，クラウドサービス上でより安全にデータを共有できる技術として，クラウドコンピューティングの普及とともに注目を集めている。

東芝ソリューション（株）と東芝は，再暗号化鍵の偽造防止技術により既存方式にない高い安全性を実現する新しい再暗号化方式を開発した。また，実際に想定されるサービス提供形態を検討してシステムを試作した。試作したシステムの機能を評価した結果，商用化に際して実現性や実用性に問題がないことを確認できた。

A proxy re-encryption (PRE) scheme is a type of public-key cryptography that allows a proxy to convert a ciphertext encrypted for a user (delegator) into that for another user (delegatee) without revealing any information to the proxy by using a re-encryption key generated by the delegator.　With the wide dissemination of cloud computing in recent years, the PRE scheme is attracting increasing attention as a key security component for the realization of secure data sharing in cloud services.

Toshiba Solutions Corporation and Toshiba Corporation have developed a new PRE scheme with higher security compared with previous schemes. Experiments on a prototype PRE system have confirmed that its performance is sufficient for practical application.

1　まえがき

近年，クラウドコンピューティングが大きな注目を集め，コストや利便性に優れていることを主な理由として急速に普及しつつある。

その一方で既存のクラウドサービスのセキュリティは十分とは言えない。特にパブリッククラウドサービスのセキュリティに対する不安を感じている企業は多く，対策として暗号化を導入済み又は検討中の企業も多い[1]。しかし，従来の暗号化技術では利便性とセキュリティは二律背反の関係にあり，セキュリティを強化すると利便性が損なわれてしまう。

そこで東芝ソリューション（株）と東芝は，高い利便性を保ちながらセキュリティを大幅に強化するクラウドサービス向け暗号化技術の研究開発を行っている（**図1**）。

ここでは，その成果の一つとして，複数のメンバー間で暗号化したデータをクラウドサービス上で安全に共有できる“再暗号化技術”について述べる。

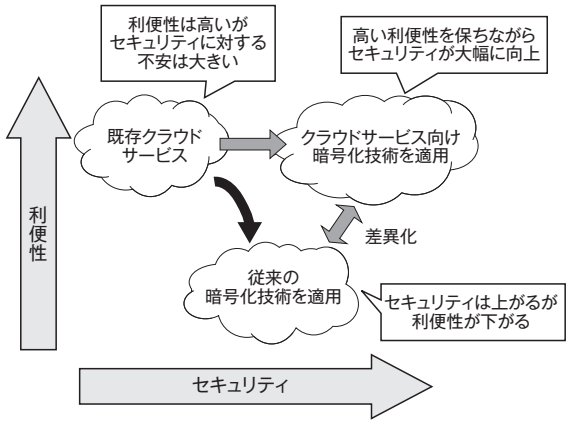


図1．クラウドサービス向け暗号化技術の狙い ― クラウドサービス向け暗号技術により，高い利便性を保ちながらセキュリティの向上を図る。
Aims of cloud service-oriented cryptography

2　現状のクラウドストレージにおけるセキュリティ対策技術

クラウドサービス上でデータを共有するニーズは非常に高く，クラウドサービスの用途として上位に挙げられる。以下では，新たに開発した再暗号化技術の有効性と特長について，クラウドサービス上でファイルを保存するクラウドストレージを利用して，取引先から重要データを受け取りプロジェクトグループのメンバー間で共有する場面を例にして述べる。

2.1　セキュリティの課題

従来のクラウドストレージのセキュリティ対策としては，SSL（Secure Socket Layer）やVPN（Virtual Private Network）といった通信路暗号化による盗聴対策，ファイアウォールによる外部からの攻撃対策，ユーザー認証やアクセス制御による

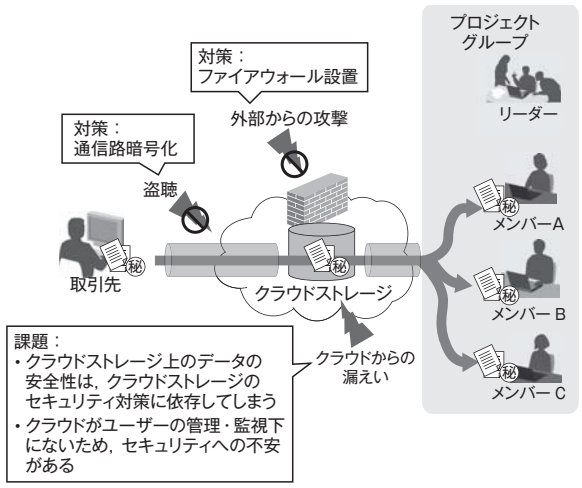


図2．既存のクラウドストレージにおけるセキュリティの課題 — データの安全性がクラウドストレージのセキュリティ対策に依存してしまい，ユーザーの管理・監視下にないことから課題が生じる。

Security problems in conventional cloud storage services

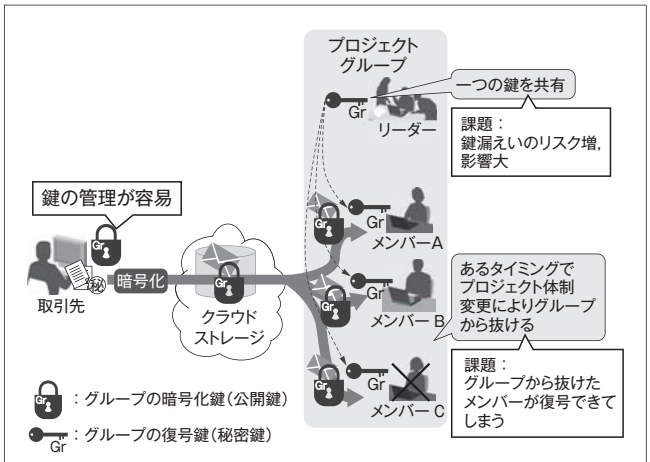


図3．グループの鍵を共有する場合の課題 — 秘密鍵を共有すると漏えいのリスクは増し，漏えい時の影響も大きい。

Problems in encrypting data with shared group keys

不正アクセス対策などが一般的である。

しかし，これらのクラウドストレージのセキュリティ対策はクラウドサービス側が行っており，ユーザーはこれらのセキュリティ対策が適切に行われているかを監視及び制御することができない。

そのため，サービス管理者による内部犯行や，設定ミス，アプリケーションのバグ，マルウェアなどによる脅威を排除できず，特にユーザーの管理・監視下にないパブリッククラウドサービスでは，セキュリティに対するユーザーの不安を払拭できない（**図2**）。

2.2　利便性とセキュリティのトレードオフ

クラウドストレージのセキュリティ対策に頼らずにデータの漏えいを防ぐには暗号化が有効であるが，利便性の低下がしばしば問題となる。従来の暗号化技術でデータを暗号化して共有しようとすると，以下に述べる二つの方法が考えられるが，どちらの方法にも一長一短があり，いずれの方法でも利便性とセキュリティのトレードオフがある。

2.2.1　グループの鍵を共有する場合　第1の方法は，グループで一組の公開鍵と秘密鍵を用意し，メンバー全員で共有するものである。

この方法では，暗号化のための公開鍵は一つであり，暗号化のための鍵管理は容易になる。

一方で，一つの秘密鍵を複数のメンバーが共有することになるため，誰かひとりでもずさんな鍵管理をしていれば鍵の漏えいにつながり，鍵が漏えいした場合には全てのメンバーが鍵を更新しなければならないなど，鍵漏えい時の影響が大きい。また，グループから抜けたメンバーが共有していた秘密鍵を持っているため，暗号化されたデータを復号し続けられることが問題となる（**図3**）。更に，共有する秘密鍵をリーダーからメンバーに安全に受け渡すこと自体が難しいという問題もある。これらは，パスワードの共有がセキュリティ上望ましくないことと同様の問題と言える。

2.2.2　メンバーそれぞれが鍵を持つ場合　第2の方法は，メンバーそれぞれが公開鍵と秘密鍵を持ち，暗号化する際にはメンバー全員それぞれの公開鍵でメッセージを暗号化するものである。

この場合，メンバー間では秘密鍵を共有せず，メンバーは自身の秘密鍵だけを管理すればよい。そのため，メンバーの秘密鍵管理は容易になり，セキュリティ上も好ましい。

一方で，暗号化する際にはグループ構成を把握し，全てのメ

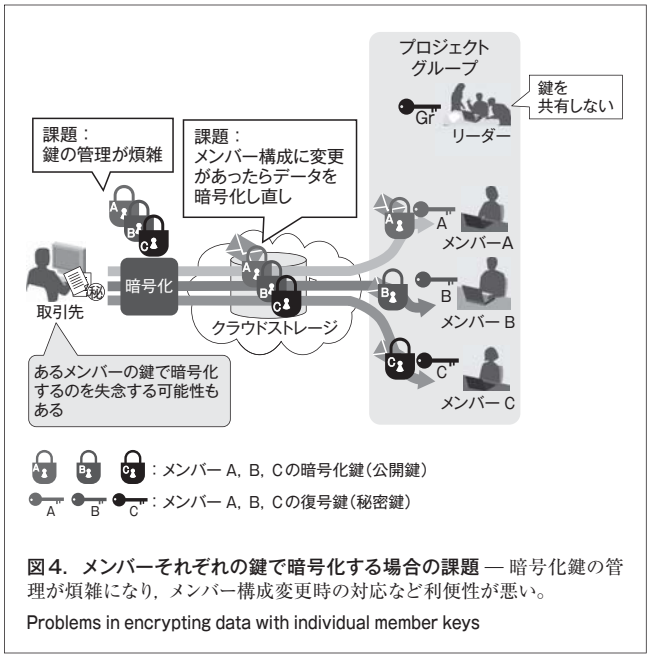


図4．メンバーそれぞれの鍵で暗号化する場合の課題 — 暗号化鍵の管理が煩雑になり，メンバー構成変更時の対応など利便性が悪い。

Problems in encrypting data with individual member keys

ンバーの公開鍵を使用して暗号化しなくてはならず，鍵管理が煩雑である。更に，グループのメンバー構成に変更があった場合，その変更に応じてクラウドストレージ上の重要データも暗号化し直さなければならない（**図4**）。例えば，新しいメンバーが追加されたときには，そのメンバーも復号できるように暗号化し直す必要がある。このため，利便性が大きく損なわれてしまう。

3　再暗号化技術

3.1　概要

再暗号化技術とは，暗号化されたデータを復号することなく別のユーザーの鍵に付け替え可能な暗号方式である[2]。

暗号化されたデータの鍵を付け替えるようすを**図5**に示す。これはユーザーAの鍵からユーザーBの鍵に付け替える場合の例である。従来の公開鍵暗号技術(a)では，秘密鍵を使って一度復号してから，新しい公開鍵で暗号化し直す必要がある。このとき秘密鍵が必要であり，一度暗号化が解かれるため，この処理はセキュリティホールになる可能性がある。

それに対し，再暗号化技術(b)を利用すれば，付け替え専用の“再暗号化鍵”を使うことで，暗号化されたデータを復号することなく別のユーザーの鍵に付け替えられる。データは常に暗号化されているため，万一クラウドストレージ上のデータが漏えいしても暗号化前のデータが流出することはない。

ここで，再暗号化鍵は，ユーザーAの秘密鍵とユーザーBの公開鍵から生成される。すなわち，ユーザーAが認めた場合にだけ鍵の付け替えが可能になる。これは，ユーザーBへのアクセス権付与をクラウドサービスに任せるのではなく，ユーザーA自身が暗号化によって行っていることと同等である。

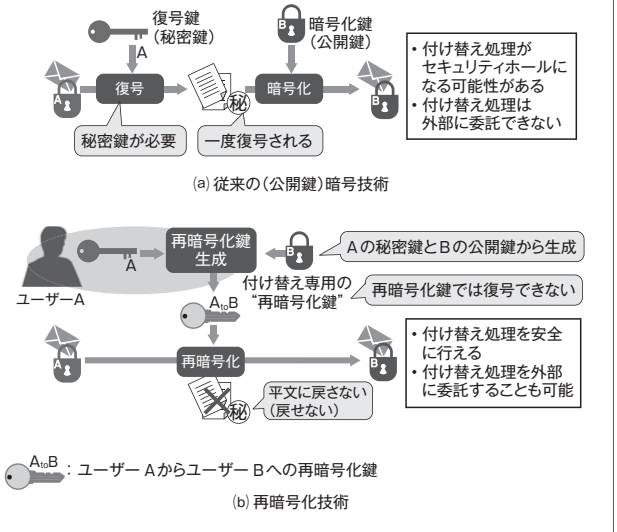
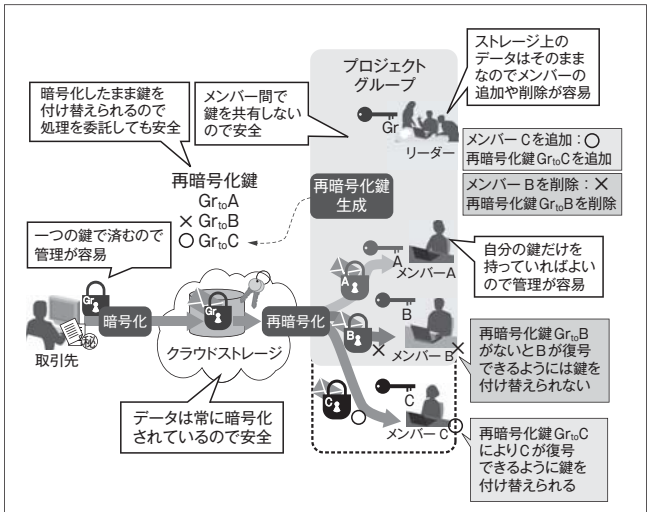


図5．従来の暗号技術と再暗号化技術の比較 — 従来の暗号技術では鍵の付け替えがセキュリティホールになる可能性があるのに対し，再暗号化技術では安全に鍵を付け替えられる。
Comparison of conventional public-key encryption and PRE



GrtoA，GrtoB，GrtoC：グループからメンバーA，B，Cへの再暗号化鍵

図6．再暗号化技術による利便性とセキュリティの両立 — 再暗号化技術を利用すると，利便性を下げることなく安全なデータ共有を実現できる。
Usability and security realized by PRE

また，再暗号化鍵では鍵の付け替えはできても復号はできないため，再暗号化処理を第三者に委託することも可能になる。

3.2　利便性とセキュリティの両立

この再暗号化技術をクラウドストレージへ適用すると，パブリッククラウド上でも利便性を損なうことなく安全に重要データの共有が可能になる（**図6**）。

取引先は，重要データをプロジェクトグループの公開鍵で暗号化してクラウドストレージに保存する。クラウドストレージ上には，グループから各メンバーへの再暗号化鍵が登録されており，重要データをダウンロードする際には，各メンバーが自分の秘密鍵で復号できるように再暗号化される。

取引先は暗号化の鍵が一つで済むため鍵管理が容易である。また，クラウドストレージ上では重要データは常に暗号化されているため，万一，クラウドストレージ上のデータが流出しても重要データが漏えいすることはない。更に，プロジェクトグループでは，メンバー間で鍵を共有する必要がなく，秘密鍵は自分のものだけを持っていればよい。メンバー構成に変更がある場合にも，ストレージ上のデータはそのままで，メンバーの追加や削除に応じてクラウドストレージ上の再暗号化鍵を登録したり削除したりするだけで，データ共有の許可や拒否を設定できる。

4　新たな研究開発成果

4.1　再暗号化鍵の偽造防止技術

再暗号化技術は，このように利便性とセキュリティを両立す

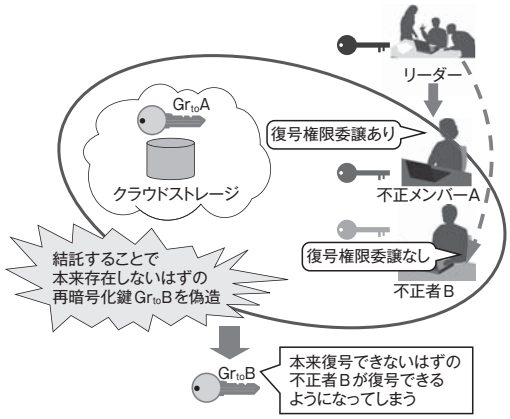


図7. サービス管理者と不正な利用者の結託 — 既存の再暗号化方式では，結託により本来存在しないはずの再暗号化鍵を偽造できてしまう。
Collusion attack by server administrator and malicious users

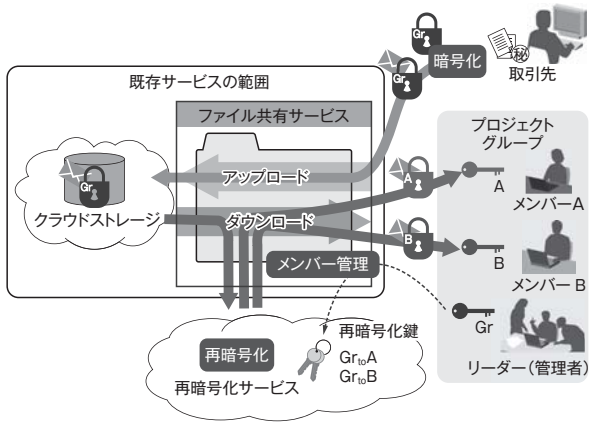


図8. 再暗号化技術のサービス提供例 — 再暗号化サービスをクラウドサービスとして提供することで再暗号化機能を容易に適用できる。
Example of provision of re-encryption service

る暗号化技術として注目されて盛んに研究が行われており，これまでに多くの方式が提案されている。しかし既存の方式では，サービス管理者と不正な利用者が結託した場合，再暗号化鍵と秘密鍵から本来存在しないはずの再暗号化鍵を偽造できてしまうため，実用上十分な安全性を備えているとは言えなかった（**図7**）。

そこでわれわれは，サービス管理者と不正な利用者が結託しても再暗号化鍵を偽造できない新たな再暗号化方式を開発した[(3)]。従来の再暗号化方式では，鍵漏えいが起こってしまった場合，意図しないメンバー向けの再暗号化鍵を生成可能となり，不正なメンバーがデータ共有できてしまうという問題があった。新たに開発した方式は，再暗号化鍵の偽造防止技術によりこの問題を解決する。更に，この方式は再暗号化鍵に有効期限を指定できるように拡張可能である。

4.2 サービス提供形態の検討

再暗号化技術を既存のWebサービスに適用する場合，利用者にとっては導入の手間がかからず使い勝手も変わらないこと，Webサービス開発者にとっては既存サービスへの機能追加が容易であることの二つの要件が重要になる。

一つ目の要件を満たすためには，Webブラウザのプラグインを利用する方法が考えられる。プラグインにより利用者のパソコンにクライアントソフトウェアをインストールする必要がなくなり，導入が容易なサービスとして提供できる。また，暗号化と復号や，再暗号化鍵生成の処理をプラグインに自動実行させることで，既存のWebサービスの使い勝手を変えずに再暗号化機能を提供できる。更に，鍵生成をプラグインで実行させることで，暗号化機能をシステムへ導入する際に問題となりがちな鍵生成と配付の問題も解決できる。

二つ目の要件を満たすためには，**図8**に示すように再暗号化サービスを一つのクラウドサービスとして提供する方法が考えられる。このサービスをREST（Representational State Transfer）などの汎用的なAPI（Application Programming Interface）として提供すれば，既存のWebサービスと連携して再暗号化機能を追加することが容易になる。

4.3 システムの試作結果と評価

これまでの検討を踏まえ，東芝ソリューション（株）は，4.1節で述べた新たな再暗号化方式[(3)]のライブラリ，Java™（注1）アプレットのプラグイン，REST APIを持つ再暗号化サービス，及びクラウドストレージとしてAmazon S3を利用するファイル共有サービスを試作した。

その結果，この構成でシステム構築が可能であり，処理時間も実用的と言えることを確認した。ライブラリの処理時間を**表1**に示す。データのアップロードとダウンロード処理時間のオーバヘッド（注2）はそれぞれ約0.12 sと0.35 sである。この処理時間は，データ本体をAES（Advanced Encryption Stan-

表1. 試作した再暗号化方式ライブラリの処理時間
Processing times of prototype using PRE

処　理		処理主体	処理時間（ms）
アップロード	暗号化	クライアント	117
ダウンロード	再暗号化	再暗号化サービス	175
	復号	クライアント	173

開発環境　言語　：C
　　ビルド：Visual Studio®（注3）2010
実行環境　OS（基本ソフトウェア）：Windows®（注4）XP SP3
　　CPU：Intel® Core™（注5）2　2.40 GHz
　　RAM：2 Gバイト

（注1）　Javaは，Oracle又は関連会社の米国及びその他の国における商標又は登録商標。
（注2）　暗号化しない場合に比べて余分に掛かる時間。
（注3），（注4）　Visual Studio，Windowsは，米国Microsoft Corporation の米国及びその他の国における商標又は登録商標。
（注5）　Intel，Intel Core は，米国及びその他の国におけるIntel Corporationの商標。

dard）などの高速な暗号化方式で暗号化してその鍵を再暗号化方式で暗号化するという，ハイブリッド暗号化と呼ばれる手法を利用すれば，データサイズには依存しない。

例えば，メール添付が困難なファイルをクラウドストレージ上で共有するなど，数十から数百Mバイトといったサイズの大容量ファイルを共有する場合には，データ送受信自体に数秒から数十秒かかる。前記の処理時間のオーバヘッドはこれに比べて十分に小さく，したがって今回試作したシステムは実用的であると言える。また，再暗号化サービスに処理能力の高いサーバを利用することで処理時間の短縮が可能であり，ライブラリのチューンアップによる高速化も見込める。このため，サイズが小さくデータの送受信時間が短いファイルを扱う場合でも，実用的なサービスとして提供可能になると考える。

5　あとがき

再暗号化技術について，既存方式の技術的課題を解決する新しい方式を開発した。更に，クラウドサービス上でのデータ共有への適用の検討，運用上の課題抽出とその解決，サービス提供形態の検討，及び開発した方式のライブラリとシステムの試作実装による実現性と実用性の検証を行った。これにより，再暗号化技術の実用化に向けた課題を解決した。

今後は，再暗号化技術の具体的な適用先について詳細な検討を進めていく。ここでは，典型的な適用例としてクラウドストレージを取り上げて述べたが，コンテンツ保護や暗号化メールなど，それ以外の適用先についても幅広く視野に入れて考えている。クラウドサービス利用に伴うセキュリティの見直しを行っている企業は多く，その対策として暗号化を導入済み，又は検討中の企業も多い。それらの企業に向け，広く再暗号化技術の展開を図っていく。

文　献

(1) アイティメディア(株). “企業クラウド活用に伴うセキュリティ意識の変化に関するアンケート調査”. Tech Target ジャパンホームページ. <http://techtarget.itmedia.co.jp/tt/news/1011/26/news02.html>, (2011-10-26参照).
(2) Blaze, M. et al. Divertible protocols and atomic proxy cryptography. Advances in Cryptology - EUROCRYPT '98. Lecture notes in computer science(LNCS). **1403**, 1998, p.127－144.
(3) Hayashi, R. et al. Unforgeability of Re-Encryption Key against Collusion Attack in Proxy Re-Encryption. the 6th International Workshop on Security. LNCS. **7038**, 2011, p.210－229.

吉田　琢也　YOSHIDA Takuya, D.Eng.
東芝ソリューション（株）技術統括部 商品・技術推進部シリコンバレー事務所長，工博。情報セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Toshiba Solutions Corp.

松下　達之　MATSUSHITA Tatsuyuki, Ph.D.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー，博士（情報理工学）。情報セキュリティ技術の研究・開発に従事。IEEE，電子情報通信学会会員。
Computer Architecture & Security Systems Lab.