NTT持株会社ニュースリリース

（ニュースリリース）

2012年2月10日

オンライン環境でのデータ保護の課題を抜本的に解決する「クラウド鍵管理型暗号方式」を開発
～NTTが考案した独自技術で暗号の安全な仮想化が可能に～

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：三浦　惺、以下「NTT」）は、オンライン環境でのデータ保護におけるセキュリティ上の課題を解決する新しい暗号方式「クラウド鍵管理型暗号方式」（以下、「クラウド暗号方式」）を開発しました。

このクラウド暗号方式は、暗号化されたデータを復号するための鍵（パスワードや秘密鍵等、以下「復号鍵」）をクラウドで管理する新しい暗号方式であり、NTTが考案した「自己訂正技術」を組み合わせることで、オンライン環境における新しい情報流通のカタチを実現しました。

開発の背景

近年、プライバシー情報や機密性の高いデータを、クラウドをはじめとするオンライン環境でサーバ側に渡して処理するサービスが広く一般に普及し始めています。それとともに、データの漏えいや不正利用に対する不安が高まり、新たなセキュリティ上の課題が生じてきました。

このような中、これまでにもデータを暗号化して保護することで情報漏えいを防止する様々な暗号技術の導入が試みられてきましたが、従来の暗号技術を有効に用いるためには、利用者自らが煩雑な復号鍵の管理（保管・配布）を行う必要がありました。また、復号鍵を、利用者自らが自分の端末やICカードなどに保管して管理する必要があり、管理の過程で事故が起こると情報漏えいのリスクが高まる問題がありました。

そこでNTTの情報流通プラットフォーム研究所（以下、NTTの研究所）では、長年の暗号技術の基礎研究により培った知見に基づき、誤りや偽りなどを訂正できる自己訂正技術を考案し、オンライン環境で安全に利用できるクラウド暗号方式を開発しました。このクラウド暗号方式によって利用者は簡便に暗号を利用することができるとともに、暗号化データの不正利用を防止することもできます。

クラウド暗号方式の仕組みと特長

クラウド暗号方式は、復号鍵をクラウドにとどめたまま管理し、暗号の復号をクラウドに安全に委託する暗号方式です（図1）。利用者が端末にインストールしたソフトウエアと、復号鍵を管理するクラウドが連携して、暗号化されたデータを端末上で復号できる仕組みです。

（1）クラウドで安全かつ柔軟な管理を実現

従来の暗号方式では利用者の端末に復号鍵を読み込んで暗号を復号していたので、すべての利用者が復号鍵を管理する必要がありました。クラウド暗号方式では、復号鍵はクラウドの内部で管理され、端末に復号鍵を読み込みません。利用者は復号鍵管理の煩雑さから解放されるとともに、暗号化データの利用をいつでも簡単・確実に制御できるようになります。

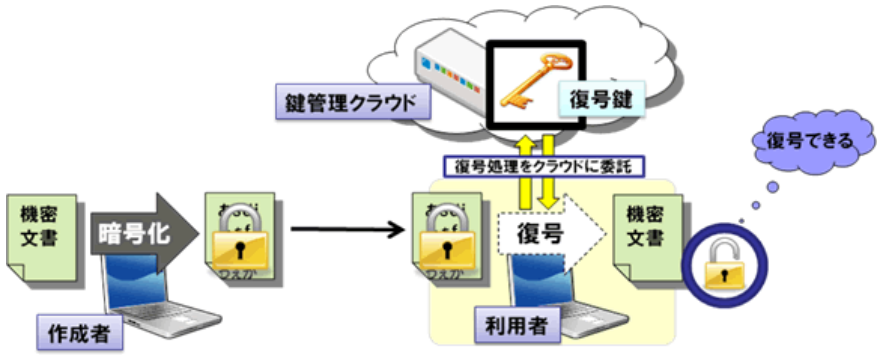

図1　クラウド暗号方式の仕組み

たとえば、暗号化データをA、B、Cの三人に渡して、後からAとBだけが読めるように設定したり、一度読めるように設定したAが読めなくなるように再設定したりすることが可能です（図2）。暗号化データを作成した後でデータの復号を許可する相手を制御することも可能であるため、暗号化されたデータが流出しても、データを不正に利用される被害をくいとめることができます。

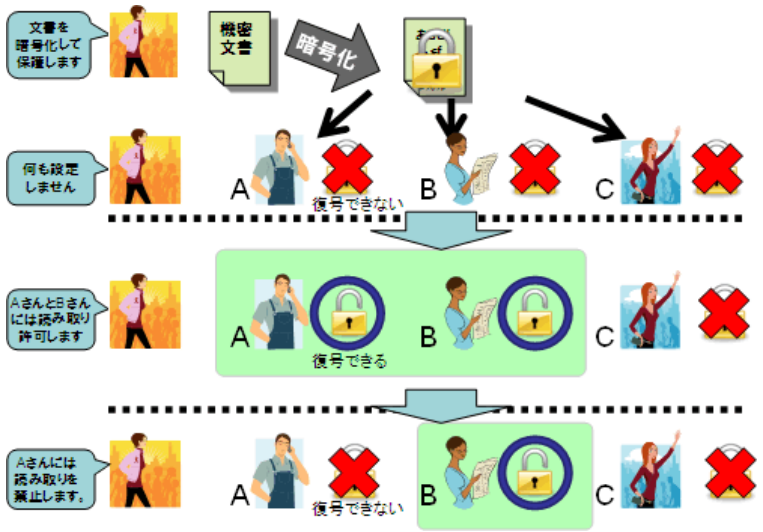

図2　暗号化データの安全で柔軟な利用

（2）どのような誤りにも対応できる自己訂正が可能

クラウド暗号方式が実現した背景には、自己訂正技術があります。一般に、自己訂正技術は、暗号化データの復号処理を他のコンピュータに委託するときなどに、他のコンピュータに要求した演算の結果に誤りがあったり、第三者に演算結果を偽装されたりしても、正しい演算結果だけを抽出して正常な処理を行うことができる技術です。自己訂正技術は、他のコンピュータに演算を何回か要求し、演算結果の整合性を見ることにより実現できます。また、他のコンピュータに演算を要求するときに、演算の対象となるデータは委託したい処理に関する情報を一切含まず、処理の内容を秘密に保ちます。ところが、従来の自己訂正技術では、演算結果に含まれる誤りや偽りといった不正の性質や頻度によっては、正しい演算結果だけを抽出することができなくなる限界がありました。

今回NTTの研究所が考案した新しい自己訂正技術（図3）は、他のコンピュータに複数回の演算を要求するときに、対象データ（図3中「身代わり1・2」）の間に他者から予測不能な関係を持たせることで不正検知を可能としており、事実上どのような不正があっても正しい演算結果だけを抽出し、正常な処理が可能です。また、復号などの委託した処理の結果は、委託を受けたコンピュータの運用者にさえ秘密に保たれます。このため、現実のオンライン環境で安全性を保ちながらクラウドに暗号化データの復号処理を委託する「暗号の仮想化」が可能になり、クラウドで鍵を管理する安全な方式が実現しました。

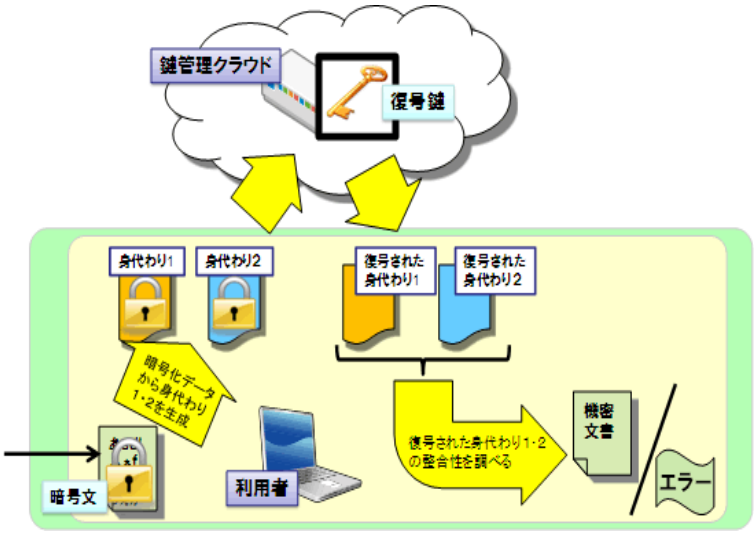

図3　NTTの研究所が考案した自己訂正技術

今後の展望

今後はクラウド暗号方式をビジネスユースとして一般の人に気軽に使っていただける実用的な技術にするために、プロトタイプシステムの改良、ならびに実用化研究を進めていきます。具体的には、クラウド暗号方式を実際に使う場合を想定して、システムの設計や運用面での安全性の確保、ならびに技術の社会的役割についても検討を重ねて、2～3年以内の実用化に向けて研究を進めていきます。

本件に関するお問い合わせ先

NTT情報流通基盤総合研究所
企画部　広報担当
TEL：0422-59-3663
E-mail：islg-koho@lab.ntt.co.jp

NTT持株会社ニュースリリース インデックスへ

NTT持株会社
ニュースリリース

▸ 最新ニュースリリース

▸ バックナンバー

▸ English is Here

NTT持株会社
ニュースリリース内検索

1997 年 04 月 ～

2021 年 11 月

検索

NTTグループの情報は
こちらからもご覧いただけます。

▲このページの先頭へ