株式会社 KDDI 研究所
2012 年 10 月 24 日

情報漏えいを防ぎ高速な暗号処理が可能なクラウド向け暗号方式を開発
従来の 30 倍の速度を達成、スマートフォンでも利用可能に

株式会社 KDDI 研究所（本社：埼玉県ふじみ野市、代表取締役所長：中島　康之）は、クラウドサーバ上でユーザの属性情報を用いてアクセス制御と暗号化を同時に行う新暗号方式「ポリバレント暗号」を開発しました。本方式は、クライアントが、クラウドサーバに一切の情報を漏らすことなく連携することにより、安全性を保ちつつ、モバイル端末でも瞬時に属性ベース暗号*1を処理できるようになりました。

【背景】

クラウドサービスの利用は、社内の情報システムインフラ構築を軽減させることに貢献し、管理コストを大幅に削減することが可能となります。しかし、機密情報をそのままクラウドサーバに保管すると情報漏えいの可能性があるため、暗号化とアクセス制御を組み合わせて重要なデータを保護する必要があります。従来の暗号化アルゴリズムを用いてアクセス制御と暗号化を行うと、鍵の配布の処理や暗号処理が煩雑になるため、実用的ではありませんでした。また、従来のアクセス制御方式では、利用者の情報やアクセスポリシーが内部の不正者に対して漏洩するという問題がありました。そこで近年、暗号処理とアクセス制御を組み合わせた方式(属性ベース暗号)が研究されてきましたが、いずれも膨大な処理時間を要するという問題がありました。さらに、上記の暗号処理をクラウドサーバに代行させた場合、データのみならず、データへのアクセス権の基となる利用者の属性情報までも漏洩する可能性がありました。

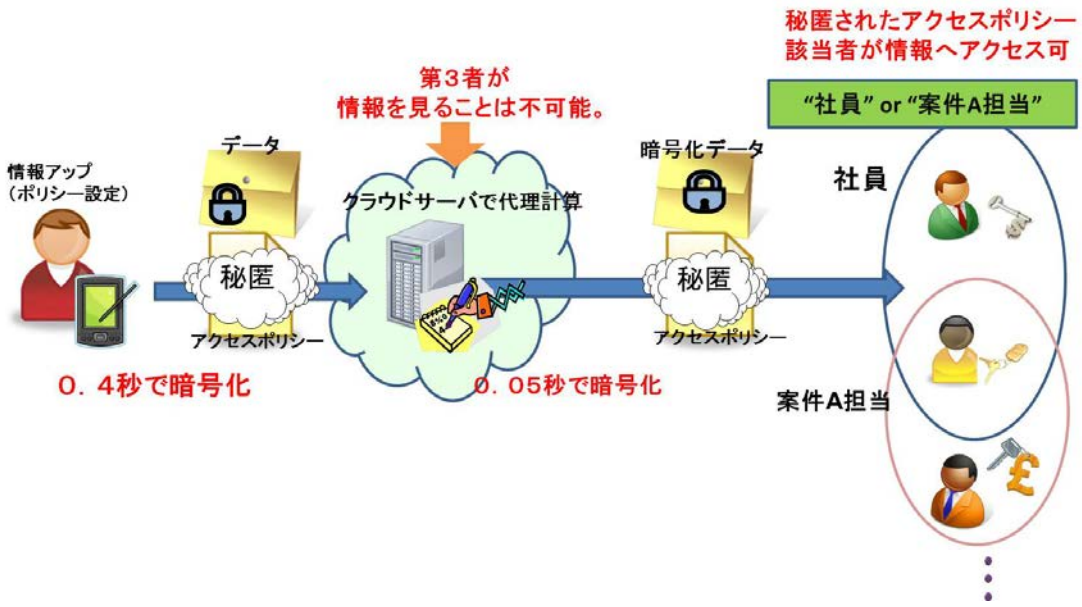
【今回の成果】

この問題を解決するために、クラウドサーバに対し暗号化・復号の処理をあらゆる情報を漏らすことなく代行させる新暗号方式「ポリバレント暗号」を開発しました。この技術では、安全性を保ちつつ処理の大部分をクラウドサーバで安全に実行させることが可能であり、クライアントは一部の処理だけを実行します。本暗号によって、クライアントの暗号化・復号処理が大幅に削減されるため、モバイル端末でも瞬時に処理できるようになりました。具体的には、クライアントがすべての処理を実行する場合と比較して、クラウドサーバを活用することにより約 30 倍の高速化を達成しています。また、利用者の属性情報を含むクラウドサーバ上に保存した一切の情報が漏洩しません。

【今後の展望】
今後はクラウド環境におけるソリューションビジネスなどを検討していきます。

［用語解説］
(*1) 属性ベース暗号
属性の関係式によってアクセスポリシーを規定し、条件を満たすユーザのみが復号できるようにデータを暗号化する方式。クラウドに適した方式として研究されている。
http:// www.cryptrec.go.jp/report/c08_idb2008.pdf

［参考画像］
ポリバレント暗号概要図



・処理の分割技術によりクラウドサーバが大部分の処理を代行できる＝端末の処理が高速
・一切の情報がクラウドサーバに漏えいしない