（報道発表資料）

2024.9.26

日本電信電話株式会社

世界初、登録型属性ベース暗号における実用上不都合な条件式制限を解消

～安全性と機能性を両立した革新的な暗号方式の実用性を向上～

発表のポイント：

- ◆ 複雑な登録型属性ベース暗号を解析が容易な部品的技術から組み立て式に作成
- ◆ セキュリティ上の懸念点である「マスター秘密鍵」の流出問題を解消
- ◆ NOT（否定）使用可、条件式で同じ属性を何度でも使え、「システム開始時に使用する属性を指定する必要なし」などアクセス制御の条件式に制約がない

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：島田明、以下「NTT」）は、登録型属性ベース暗号（Registered Attribute-Based Encryption）において従来方式では実現できなかった実用的なアクセス制御を可能にする暗号方式を開発しました。登録型属性ベース暗号は、アクセス制御が可能な公開鍵暗号技術である属性ベース暗号（Attribute-Based Encryption）の安全性上の懸念を解決した新しいタイプの属性ベース暗号です。今回の研究成果により、安全性と実用的なアクセス制御を両立した属性ベース暗号が世界で初めて実現可能になりました。

なお、本成果は暗号理論における最高峰国際会議である the 44th Annual International Cryptology Conference (CRYPTO 2024) (※1)において発表しました。

1. 背景

属性ベース暗号（Attribute-Based Encryption)は、データを暗号化する際の暗号文に、「（人事部 AND 課長）OR 経理部」というような「AND/OR/NOT」による復号条件式を組み込み、暗号文を復号するための秘密鍵に「経理部、部長」というような属性情報を付与することで、条件式に見合った鍵でのみの復号を実現する公開鍵暗号方式です（図1）。属性ベース暗号において暗号化を行う際には、暗号化するデータと復号条件式に加えてマスター公開鍵と呼ばれる公開情報を使用します。属性ベース暗号は、社内データのアクセス制御やコンテンツ配信サービスなどへの応用が期待されていますが、各ユーザの秘密鍵は全ての暗号文を復号可能な強大な権限をもつ鍵生成局（Key Generation Center）が生成するシステムになっています。この鍵生成局が持つ「マスター秘密鍵」と呼ばれる秘密情報が流出するとシステム内の全てのデータが復号されてしまうという課題がありました（図2）。すなわち、鍵生成局がセキュリティ上の単一障害点(Single Point of Failure)となり、安全性面での懸念点になっていました。

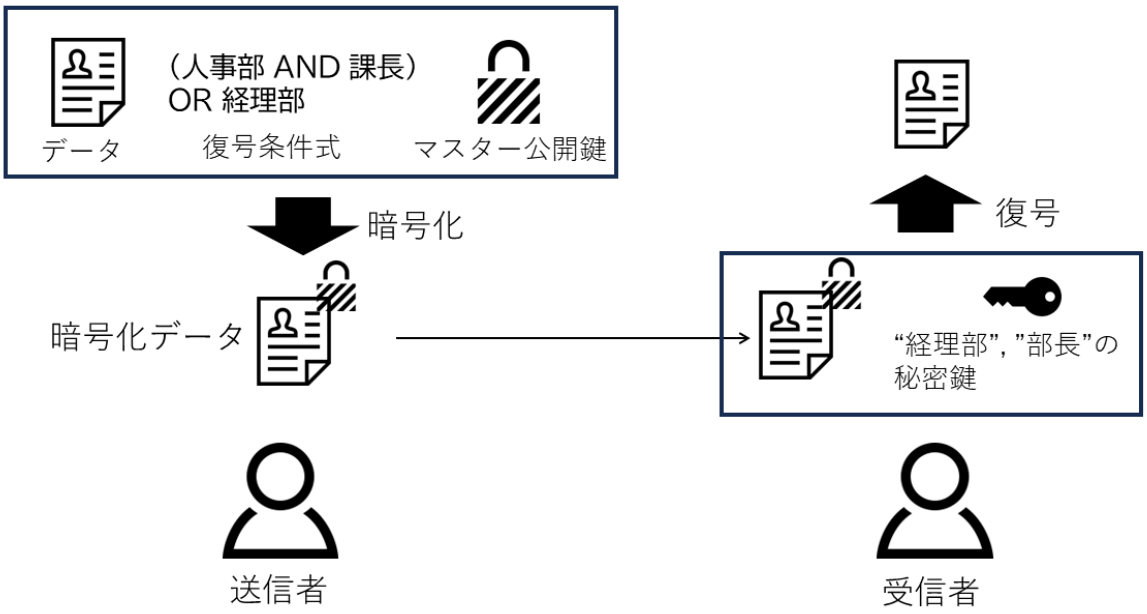

図 1 属性ベース暗号の使用例

近年、この課題を解決するために、登録型属性ベース暗号と呼ばれる鍵生成局を持たない属性ベース暗号が提唱されました。登録型属性ベース暗号においては、各ユーザが自身の公開鍵と秘密鍵を自分で生成し、公開鍵と自身の属性情報を登録サーバに登録します（図3）。登録サーバの役割は、各ユーザによって登録された公開鍵を圧縮して暗号化に必要なマスター公開鍵を生成するだけで秘密の情報は持っていないため、攻撃を受けたとしてもシステムの安全性に影響はありません。暗号文は各ユーザの秘密鍵によって復号条件を満たしたときのみ復号されます。しかし、従来の登録型属性ベース暗号では、NOT を含む条件式を使うことができない、復号条件式の中で同じ属性を複数回使えないなどの実用上不都合な制限が複数ありました。

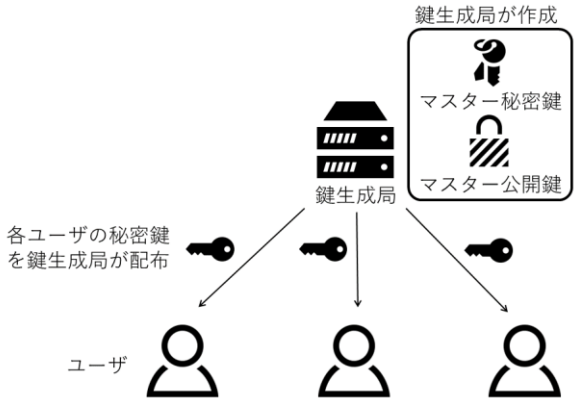

図 2 属性ベース暗号の鍵生成モデル

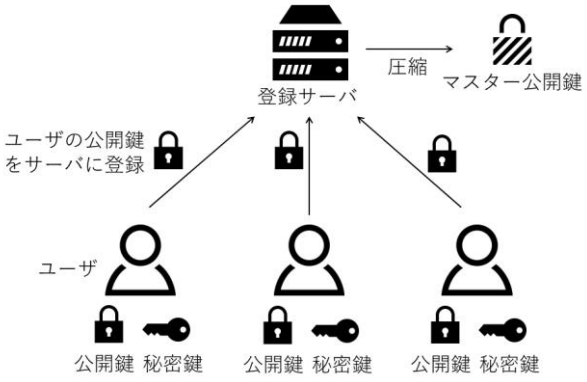

図 3 登録型属性ベース暗号の鍵生成モデル

2. 研究の成果および技術のポイント

NTT は、産業技術総合研究所と共著で投稿した論文(※2)において、復号条件式に関する制約がある登録型属性ベース暗号から、より制約がない登録型属性ベース暗号に変換する一連の変換技術を考案しました。既存の登録型属性ベース暗号にそれらの変換を繰り返し適用することで、属性数やアクセス制御に用いる条件式の大きさなどに制限がなく、さらに NOT を含む条件式を扱うことが可能な登録型属性ベース暗号に変換できることを示しました。このような制約のない登録型属性ベース暗号を直接的に考案するアプローチも考えられましたが、複雑な暗号方式の安全性の証明、実現は困難でした。そこで、複雑な登録型属性ベース暗号を単純な属性ベース暗号及び一連の変換というより解析が容易な要素技術から組み立て式に作るという技法に着目することで、登録型属性ベース暗号が構成可能なことを世界で初めて示しました（図 4）。

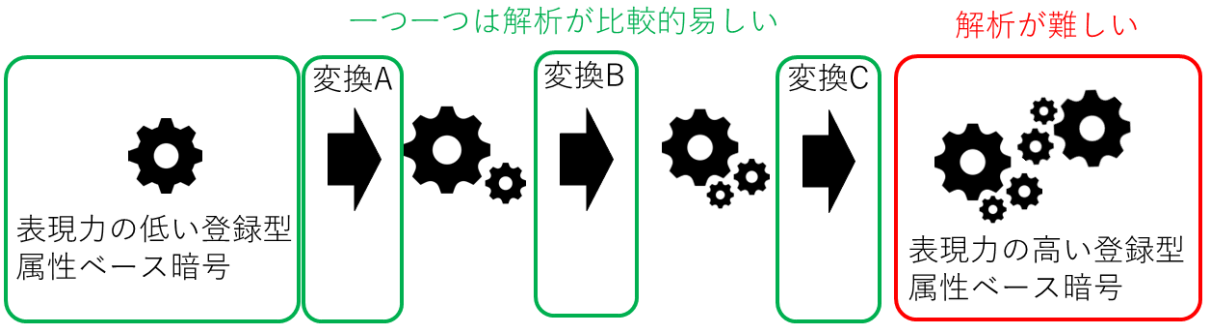

図 4 登録型属性ベース暗号の変換イメージ

★本技術の既存技術に対する優位性は表1に示した通りです。（1）データの暗号化にかかる時間が復号対象者数に依存しない、（2）システム内にマスター秘密鍵が存在しない、（3）復号条件式の制限がない、の3点を世界で初めて実現しました。

技術	暗号化時間と復号対象者数	マスター秘密鍵	復号条件式の制限
公開鍵暗号	依存	なし	なし
属性ベース暗号	非依存	あり	なし
登録型属性ベース暗号（既存）	非依存	なし	あり
登録型属性ベース暗号（本研究）	非依存	なし	なし

表１ 従来技術との比較

3. 今後の展開

本技術により、実用的な復号条件式を扱うことが可能な登録型属性ベース暗号が実現可能となることで、動画や音楽などのコンテンツ配信サービスにおけるコンテンツデータ・企業などが持つ組

織のデータなど、複数が利用するシステムのセキュリティが向上し、不正アクセスなどによるデータ流出のリスクを大きく低下させることが期待されます。

　引き続き、変換を繰り返すことで最終的に得られる登録型属性ベース暗号の効率が悪くなってしまう課題などの解決に向け、より一層実用的な登録型属性ベース暗号の研究開発に取り組んでいきます。

【用語解説】

※1. CRYPTO2024 https://crypto.iacr.org/2024/

※2. A Modular Approach to Registered ABE for Unbounded Predicates. Nuttapong Attrapadung (AIST), Junichi Tomida (NTT Social Informatics Laboratories)

■本件に関する報道機関からのお問い合わせ先
日本電信電話株式会社
サービスイノベーション総合研究所
企画部　広報担当
nttrd-pr@ml.ntt.com