現代暗号の発展形…次世代の「高機能暗号」

西出 隆志

本稿では，暗号の機能面の進化に着目し，より高度な用途を可能にする暗号技術を取り上げます．従来の暗号技術は，「データを暗号化し，必要なときに復号して利用する」というシンプルな使い方が主流でした．しかし，例えば，暗号化したままデータを処理できる秘密計算技術のように，従来の枠を超えた暗号技術が存在しており，これらの先進的な暗号技術は総称して，高機能暗号と呼ばれることがあります．

最近では，こうした高機能暗号の中でも実用性の高い技術が増えてきており，標準化，ソフトウェア・ライブラリの整備，商用サービス化も進んでいます．このような動きにより，産業，医療，金融，行政など，さまざまな分野での活用が今後加速していくことが期待されています．本稿ではそうした高機能暗号の一端を紹介します(3)注1．

公開鍵暗号の発展形…属性ベース暗号／関数型暗号

公開鍵暗号の機能の観点からの発展形である属性ベース暗号と関数型暗号について説明します(4)(5)．

● 属性ベース暗号

公開鍵暗号では，例えば受信者のアリスの公開鍵で暗号化された暗号文は，対応する秘密鍵を持つアリスのみが復号できます．この仕組みは，暗号文に対するアクセス制御とみなすことができ，「アリスのみが復号可能」という条件が暗号文に設定されていると解釈できます．この考え方を一般化した技術が「属性ベース暗号（Attribute-Based-Encryption）」です．属性ベース暗号では暗号文作成時に「復号可能条件」を指定でき，この条件は復号者の属性に関する条件式として表現されます．これにより，暗号技術そのものに基づく柔軟なアクセス制御が可能になります．

例えばある企業で，「部署Aかつ職位が課長」または「職位が部長」である人のみが復号可能な暗号文を作成し，企業内ファイル・サーバに保管する場合，次のような復号可能条件を設定できます．

復号可能条件：
（部署＝A AND 職位＝課長）OR（職位＝部長）……(1)

この条件は属性ベース暗号の暗号化処理で指定されます．また暗号文を生成するために必要な公開鍵（マスタ公開鍵と呼ばれる）は，通常の公開鍵暗号と同様に，誰でも参照できる形で公開されます．

▶鍵生成の仕組みと管理

属性ベース暗号は通常の公開鍵暗号技術の発展形ではありますが，鍵生成の仕組みには大きな違いがあります．通常の公開鍵暗号ではアリスは自身の公開鍵と秘密鍵を自ら生成します．一方，属性ベース暗号では各ユーザが自身で鍵を生成するのではなく，「鍵生成局」（例えば企業内の鍵管理部門）が存在し，この鍵生成局が各ユーザに対して復号に必要な鍵を生成・配布します注2．各ユーザは，鍵生成局のみが保持する「マスタ秘密鍵」という秘密情報を知らないため，独自に鍵を生成することはできません．復号可能条件［式(1)］の例では，次のように鍵が鍵生成局から各ユーザへ配布されます．

- 部署Aに所属するユーザ：部署Aに対応する鍵を取得
- 職位が課長のユーザ：課長に対応する鍵を取得
- 職位が部長のユーザ：部長に対応する鍵を取得

また，鍵生成局はマスタ公開鍵の生成と公開を行う役割も担います．

▶属性ベース暗号の「結託耐性」

重要な特徴として「結託耐性」が挙げられます．もし単純に複数の公開鍵暗号を組み合わせて属性ベース暗号を実現しようとすると，次のような問題が発生します．例えば，部署Aに所属するユーザと，部署Bに所属しつつ職位が課長であるユーザが，それぞれの鍵

注1：GMOサイバーセキュリティ byイエラエの酒見氏による高機能暗号に関する解説動画「データ利活用を促進させるプライバシー強化技術PETsの紹介」．https://www.youtube.com/watch?v=t56qGCaGSW8が参考になる．

注2：最新の研究動向ではマスタ秘密鍵を保持する鍵生成局を必要としない「登録型属性ベース暗号」と呼ばれる方式が提案される(1)．

◆参考文献◆
(1) Nuttapong Attrapadung and Junichi Tomida：A modular approach to registered ABE for unbounded predicates. In CRYPTO，pp.280–316，Springer，2024. 13.
(2) 安永 憲司：暗号理論入門，2024. 15，森北出版．