（報道発表資料）

2010年7月28日
日本電信電話株式会社
三菱電機株式会社

クラウド時代の高度なセキュリティー対策を実現する新世代暗号方式を開発

～最も先進的なインテリジェント暗号を世界で初めて実現～

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」）と三菱電機株式会社（本社：東京都千代田区、執行役社長：山西 健一郎、以下「三菱電機」）は、クラウドコンピューティング（以下「クラウド」）普及の課題と言われてきたセキュリティー上の問題解決の切り札となることが期待される新しい暗号方式を開発しました。

この暗号方式は、暗号-復号のメカニズムの中に高度なロジック（論理）を組み込むことが可能であり、暗号機能によりきめ細かいデータ送受信制御を行うことができる、全く新しいインテリジェント暗号（「賢い」暗号）です。

この暗号方式を用いることで、機密性の高い情報を暗号化したままクラウドで利用することができ、従来は困難とされていた多くの分野でのクラウドの利用が期待できます。

この暗号方式の詳細は、2010年8月に米国で開催される国際暗号学会「CRYPTO 2010」※1で発表する予定です。

＜開発の背景＞

ICT社会の進展は目覚ましく、近年では、クラウドをはじめとするネットワークの新しい高度な利用形態が普及してきました。しかし、そのような利用形態では、プライバシー情報や機密性の高いデータをサーバー側に渡して処理を行うため、新たなセキュリティー上の課題が生じます。

ネットワークのセキュリティーを保証するために現在では共通鍵暗号※2と公開鍵暗号※3が広く利用されていますが、上記のような新しいネットワーク利用形態でのセキュリティー課題を解決するためには、より先進的な暗号が必要とされるようになりました。

NTTと三菱電機は、共通鍵暗号や公開鍵暗号をさらに発展させた先進的な暗号として、暗号-復号のメカニズムの中に高度なロジック（論理）を組み込むことができるインテリジェント暗号の開発に取り組んできました。このたび、双線型写像ベクトル空間※4という数学的手法を開拓することで、暗号-復号メカニズムの中のロジックとして現時点で考え得る最も一般的な機能をもつインテリジェント暗号である「新世代暗号方式」の開発に世界で初めて成功しまし

た（図1）。

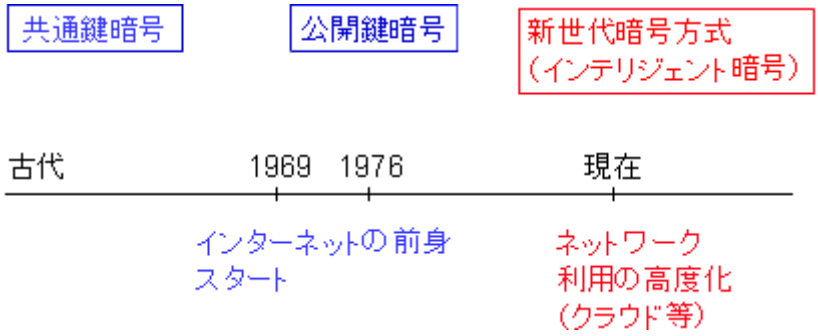

図1　暗号の技術的な進展と背景

＜新世代暗号方式の特長＞

（1）最も一般的なロジックを実現

数年前より世界中でインテリジェント暗号を目指した研究が活発に行われてきましたが、このたび開発した新世代暗号方式では、従来開発されてきたそれら暗号方式の機能をすべて特殊例として包含する最も一般的な機能を実現できます。これは、AND、OR、NOT、閾値ゲートにより構成される関係式をすべて含む理論上最も広いクラスになっています。

中でも特筆すべきことは、従来の方式の機能には含まれていなかったNOTゲートが使えるようになったことです。これにより、属性情報の変更などにも柔軟かつ簡便に対応可能なデータベース管理をクラウド上で実現することができます。

（2）多様な利用形態に対応

インテリジェント暗号においては、暗号文と復号鍵にさまざまなパラメータを導入することで暗号-復号のロジックを規定しますが、そこでは、属性情報とそれに対する条件式が、それぞれ暗号文、又は復号鍵のパラメータとなります。このたびの新世代暗号方式では、<1>「復号鍵に属性情報、暗号文に条件式」の形態も、<2>「暗号文に属性情報、復号鍵に条件式」の形態も可能であり、さまざまな利用形態に対応することが可能となりました。

<1>前者の形態を利用することで、各データごとにきめ細かくアクセス条件（開示範囲）が設定された暗号データをクラウド上で管理して、そこで設定されたアクセス条件を満足する属性情報をもつ利用者のみがそのデータを復号・閲覧できるような機能提供が可能になります。企業における機密情報管理システムや公的機関による個人情報データベース管理などの応用があります。図2は、企業における機密情報管理システムでの利用イメージを表しています。管理する機密文書ごとに誰に復号を許すかを属性情報の条件式で表し、その文書をその条件式とともに暗号化してクラウド上で管理します。その条件式を満足する属性情報をもつ社員がその文書を復号する際には、その社員の（属性情報に応じた）復号鍵を用いて復号し閲覧します。この図では、人事部第一課の課

長が、その属性情報に応じた復号鍵を用いて、クラウド上にある暗号化機密情報を入手、復号して閲覧可能となる状況を表しています。

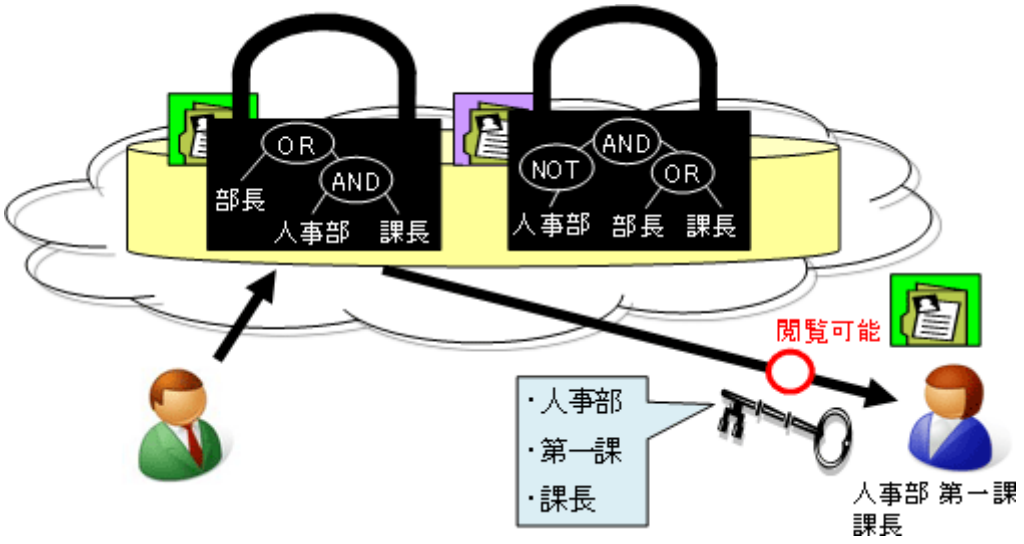

図2　企業における機密情報管理システムでの利用イメージ

<2>また、後者の形態を利用することで、属性情報がついたデータを暗号化したままクラウド上で管理して、各利用者は自分に設定されたアクセス条件を満足する属性情報のデータのみを復号・閲覧できるような機能提供が可能になります。コンテンツ配信、金融や医療の分野でのデータベース管理への応用などがあります。図3は、コンテンツ配信での利用イメージを表しています。コンテンツ提供業者がアニメ、洋画などのコンテンツをその属性情報とともに暗号化してクラウド上に置き、視聴者はその属性情報に関する条件式をパラメータとする復号鍵を用いてコンテンツを復号し視聴します。この図では、アニメ又は教育に関する500円相当のコンテンツならば復号可能という条件式をもつ復号鍵を使って、視聴者がその条件式を満たす暗号化されたコンテンツを入手、復号して視聴可能となる状況を表しています。

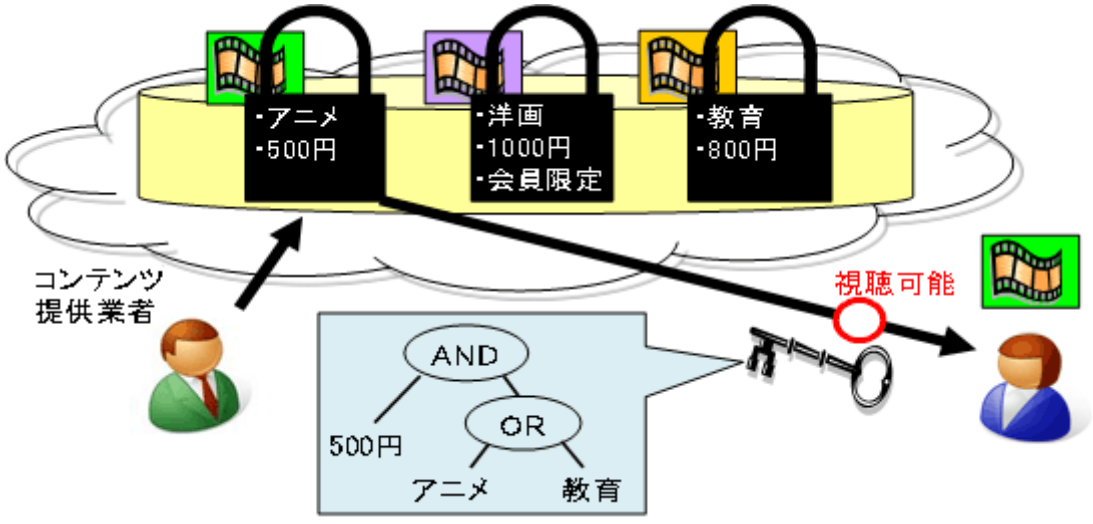

図3　コンテンツ配信での利用イメージ

＜今後の展望＞

　このたび開発した新世代暗号方式は、クラウドのような高度なネットワークサービスの安心・安全な利用を実現するうえで大変重要な役割を果たすことが期待されるため、今後はさまざまなアプリケーションに対応した利用形態や実現方法など実用化に向けた検討を進めていく予定です。

＜用語解説＞

※1　CRYPTO 2010

　暗号分野における最も代表的な国際会議。正式名称は、The 30th International Cryptology Conference。2010年8月15日～19日に、米国カリフォルニア州サンタバーバラで開催される。

※2　共通鍵暗号

　データの暗号化と復号に同じ秘密鍵を用いる暗号方式。高速な処理ができるため、大量のデータを扱う通信メッセージやファイルの高速暗号化や携帯端末の認証などに多く使われている。代表的なものに、AES暗号や、三菱電機が開発した64ビットブロック暗号「MISTY（ミスティ）」、NTTと三菱電機が2000年に共同開発した128ビットブロック暗号「Camellia（カメリア）」がある。

※3　公開鍵暗号

　1976年にDiffieとHellmanにより提案された概念。暗号化と復号で異なる鍵を用いる暗号方式であり、暗号化鍵を公開できるため、不特定多数の人々が情報をやりとりするネットワーク上での暗号通信に適している。現在は、共通鍵暗号で利用する秘密鍵を共有するための鍵配送方式として主に利用されている。代表的なものに、RSA暗号やNTTが開発した「PSEC-KEM」などがある。

※4　双線型写像ベクトル空間

　最近、暗号分野では楕円曲線上の「双線型写像群」がIDベース暗号やインテリジェント暗号などさまざまな応用において使われている。その双線型写像群を多重に用いることで、双線型写像群そのものよりも数学的に豊かな代数構造をもつ「双線型写像ベクトル空間」を構成することができる。そして、その空間の性質を利用することで、豊富な暗号学的「仕掛け」（トラップドア）が実現可能である。今回の新世代暗号方式を開発したNTTと三菱電機の研究者は、2009年に双線型写像ベクトル空間の概念を世界で初めて導入しており、今回の新世代暗号方式は、この双線型写像ベクトル空間を用いて構成されている。

＜商標関連＞

Camelliaは、NTTと三菱電機の登録商標です。
MISTYは、三菱電機の登録商標です。
RSAは、RSA Security Inc.の登録商標です。
その他のすべての商標は、それぞれ各所有者に帰属します。

【本件に関するお問い合わせ】
日本電信電話株式会社
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

三菱電機株式会社
広報部
TEL： 03-3218-2346
E-mail：prd.prdesk@ny.MitsubishiElectric.co.jp

NTT ニュースリリース