鍵の無効化を考慮に入れた ID に基づく鍵配送方式の研究

岡本 健

北陸先端科学技術大学院大学 情報科学研究科

1999 年 2 月 15 日

キーワード： ID-KDS, Diffie-Hellman, RSA, 帰着可能性.

暗号技術は古来から軍事目的で考案されており、4000 年以上の歴史を持つが、最近まで一般の人にその技術内容が知られることはあまりなかった。

このような状況に変化がおとずれたのは、1976 年に W.Diffie と M.E.Hellman が発表した有名な論文「New Directions in Cryptography」によるところが大きい。ここで彼らは従来の暗号技術とは異なる「公開鍵暗号系（public-key cryptosystem）」という新しい概念を提唱している。これは、暗号化するための鍵「公開鍵」と復号するための鍵「秘密鍵」が異なり、暗号化の鍵である公開鍵は公開し、復号化の鍵である秘密鍵を秘密にしておくというものである。また、1978 年に R.L.Rivest、A.Shamir、L.Adleman が発表した論文「A method for obtaining digital signatures and public key cryptosystems」において RSA 暗号系が提案された。これは最も現実的な公開暗号系の１つであり、素因分解の困難さを安全性の根拠にしているのが特徴である。

1990 年代中頃になると世界的規模のネットワークであるインターネットの急速な普及ならびに商用化の進展にともない、暗号技術が広く使われるようになった。これは、コンピュータとネットワークの融合による情報化の進展が必然的にもたらした大きな変化といえる。しかし一方で悪意をもったユーザによる情報の盗聴、改ざん、なりすましといった不正行為が以前にもまして表面化し、大きな社会問題になってきている。安全な情報化社会を実現するため、暗号技術の活用は必要不可欠であり、情報インフラの構築を進めるためにもユーザの負担が少なく、かつ安全性の高い通信システムが求められている。

これらの問題点を解決するための一手法として、「ID に基づく暗号系」（Identity-based cryptosystem）を用いる方式がある。これは、A.Shamir が 1984 年に発表された論文「Identity-based Cryptosystem and Signature Schemes」の中で提案されたもので、大きく分けて認証系（ディジタル署名、相手認証）の方式と鍵配送（暗号系）の方式があり、後

者については特に ID-KDS （Identity-Based Key Distribution）と呼ばれることが多い。この場合、ID （Identification）というのは、他人と区別できるユーザの名前を意味する。

ID-KDS は、公開鍵の登録簿（登録センター）のかわりに、鍵配送センターを設定する方式であり、また、システムで共通の公開鍵を定めた上で、ユーザの名前（ID）に対応した秘密鍵を生成し、それを各ユーザに配布する必要がある。ID-KDS については、現在までに多くの方式が提案されており、これらはいずれも大変有益な方式といえるが、実用化にあたってはいくつか考慮すべき点がある。大きな問題点の一つに「鍵の無効化問題」がある。これは、従来の方式ではユーザの秘密情報が何らかの理由で第三者に知られてしまった場合、センタはユーザの秘密情報を無効化し、新たな秘密情報を再交付しなければならないが、この時一つの ID に対し一つの秘密情報しか生成できないため、センターはユーザの ID 情報を破棄し、新たに別の ID を使用しなければならなかった。

また、実社会において ID に基づく鍵配送方式を構築する際、管理者はユーザの ID として、その人の名前や e-mail アドレス、住所など、ある特定の属性を選択しそれ以外の属性は使用しないというポリシーを用いることが望ましい。しかし、従来の方式では鍵の無効の際に新たな属性をもつ ID が要求され、その選択をどのような手法で行なうかという問題がでてくる。また、このような方式で運営を行なうと各利用者は他のユーザに対し複数の属性を持った ID を管理しなければならない。しかしながらこれらの事柄は ID に基づく暗号系の利点を損なうことになり好ましくない。

本論文では以上のような問題点を解決するために新たな概念を提案している。これはユーザと ID 情報を１対１対応にするというもので、これを実現するためには一つの ID に対し複数の秘密情報を生成しなければならない。本研究では、1989 年に発表された岡本-田中方式を拡張することによって具体的な方式を提案している。

本論文では、次のようなテーマについて研究を行なった。

1. ID に基づく鍵配送方式について新しい概念の提唱。
2. 岡本-田中方式を拡張することにより、提案方式の概念に対する具体化な方式の提案。
3. 提案方式の安全性について関数における帰着を用いた、数学的に厳密な考察。
4. 提案方式の概念を他のキーマネジメントに応用についての考察及び具体的な方式の提案。

以下、本論文の構成について述べる。

第２章では、まず公開鍵暗号系について概略を述べ、暗号/復号化、及び 電子署名について具体的な例を用いて説明する。

第３章では、鍵配送、鍵共有について、分散型、管理分散（認証付加）型という基本的なモデルを説明する。また、ID に基づく暗号系についての概念を述べ、提案方式の基になった岡本-田中方式を説明する。

第４章では、まずチューリングマシンについて説明し、関数の複雑さのクラス、帰着可能性について数学的に厳密な定義をする。また各種のプロトコルを破ること難しさについて考察し、関数の複雑さの順序付けを行なう。

第５章では、ID に基づく鍵配送方式について新しい概念の提唱を行ない、具体的な方式を提案する。また、提案方式の安全性について関数における帰着を用いる。そして提案方式の概念を他のキーマネジメントへ応用する方法として、具体的な方式を提案する。