IDベース暗号アルゴリズムと暗号メールシステム

高島克幸*
坂上　勉*

Identity-Based Encryption Algorithm and Mail System

Katsuyuki Takashima, Tsutomu Sakagami

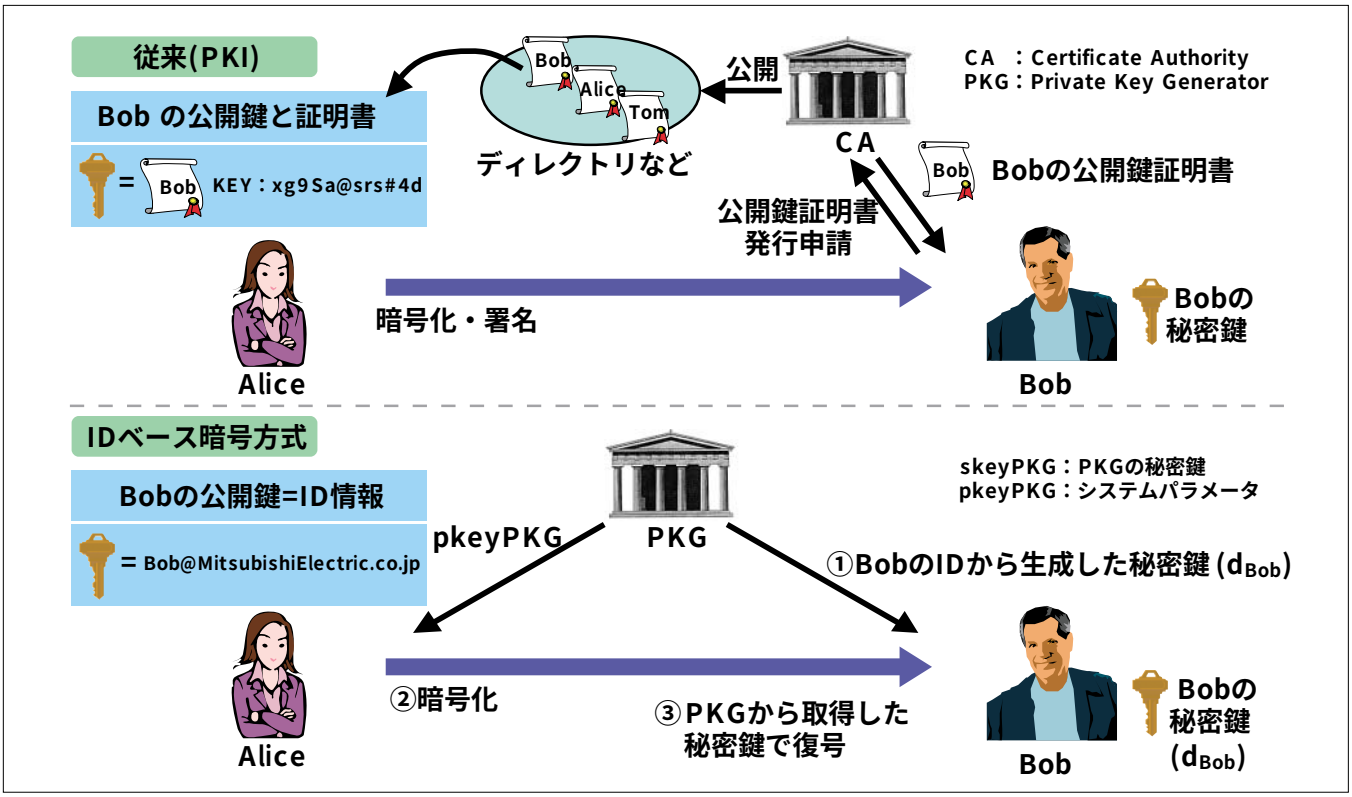
要　旨

情報漏洩(ろうえい)防止のために，暗号機能／機器を導入するのが有効であることは周知であるが，その簡便な導入を可能にする技術がIDベース暗号と呼ばれる暗号技術であり，三菱電機でも積極的に，その研究開発を行っている。IDベース暗号は，ID情報を公開鍵(かぎ)にすることができる公開鍵暗号技術であり，実用的な方式が最近になって初めて提案されたにもかかわらず，その有用性のために，それ以後，IETF(Internet Engineering Task Force)，IEEE(Institute of Electrical and Electronics Engineers)，ISO(International Organization for Standardization)といった各種団体での標準化が急速に進められている。

通常，公開鍵暗号では，暗号化の際に用いる公開鍵の正当性保証のために，公開鍵証明書というデータを用いる。これは，公開鍵と利用者を結び付けるための署名付きのデータである。IDベース暗号では，IDを公開鍵にできるため公開鍵証明書を用いる必要がなく，便利な方式であり，今後，PKI(Public Key Infrastructure)との共存を図りながら，多様なセキュリティニーズに対応できる方式として注目されている。

現在の情報通信技術は，およそ考えられるすべてのものに番号(ID)を割り振り，管理することを可能としたが，その番号体系を利用し，機器認証／管理を行う手段をIDベース暗号は与える。それによって，今後一層複雑化する情報空間での安全性を確保するとともに，従来人手で管理されてきた物／情報を，現在よりはるかに大きいスケールで安全に管理することが可能になる。

本稿では，そのように近年注目されているIDベース暗号技術について，我々が取り組んでいる基盤技術である暗号アルゴリズム改良提案と，それを用いた暗号メールシステムの試作について述べる。



IDベース暗号を適用した暗号メールシステム

IDベース暗号を適用した暗号メールシステムでは，AliceからBobへ暗号通信を行う場合，①BobはBobのIDから生成した秘密鍵をIDベース鍵生成サーバ(PKG)から取得し，② AliceはシステムパラメータとBobのIDを使ってメッセージを暗号化し送信し，③それを受け取ったBobは，PKGから取得した秘密鍵でメッセージを復号する。AliceはBobのIDを公開鍵にして暗号メール通信を行うことができ，公開鍵証明書を必要としない。

*情報技術総合研究所