PKI構築技術

坂上　勉*
佐伯正夫*

要　旨

三菱電機PKI(Public Key Infrastructure：公開かぎ(鍵)基盤)システムは，多様なPKIアプリケーション構築のための基盤とするために，基本構成要素層，認証構成要素層，セキュアプロトコル層，及びシステム構成部品層からなるレイヤ アーキテクチャを採用している。また，本格的実用とPKIアプリケーションの効率的な運用・保守のために重要な種々のPKI構築技術の研究開発を進めている。ここでは，特に中核的な認証構成要素層に関して，重要性が高く最近注目されている次のPKI構築技術について，開発成果や効果などを紹介する。

⑴　CAシステム構成技術(IA／RA分散)

IA(Issuing Authority：発行局)とRA(Registration Authority：登録局)を分散させるなど，CA(Certification Authority：認証局)システムを必要に応じて構成可能とする。CAの運用効率が向上する。

⑵　ICカードプリンタ利用技術

ICカードへの証明書発行を表面印刷しながら複数枚一括処理可能とする。証明書発行の運用効率と信頼性が向上する。

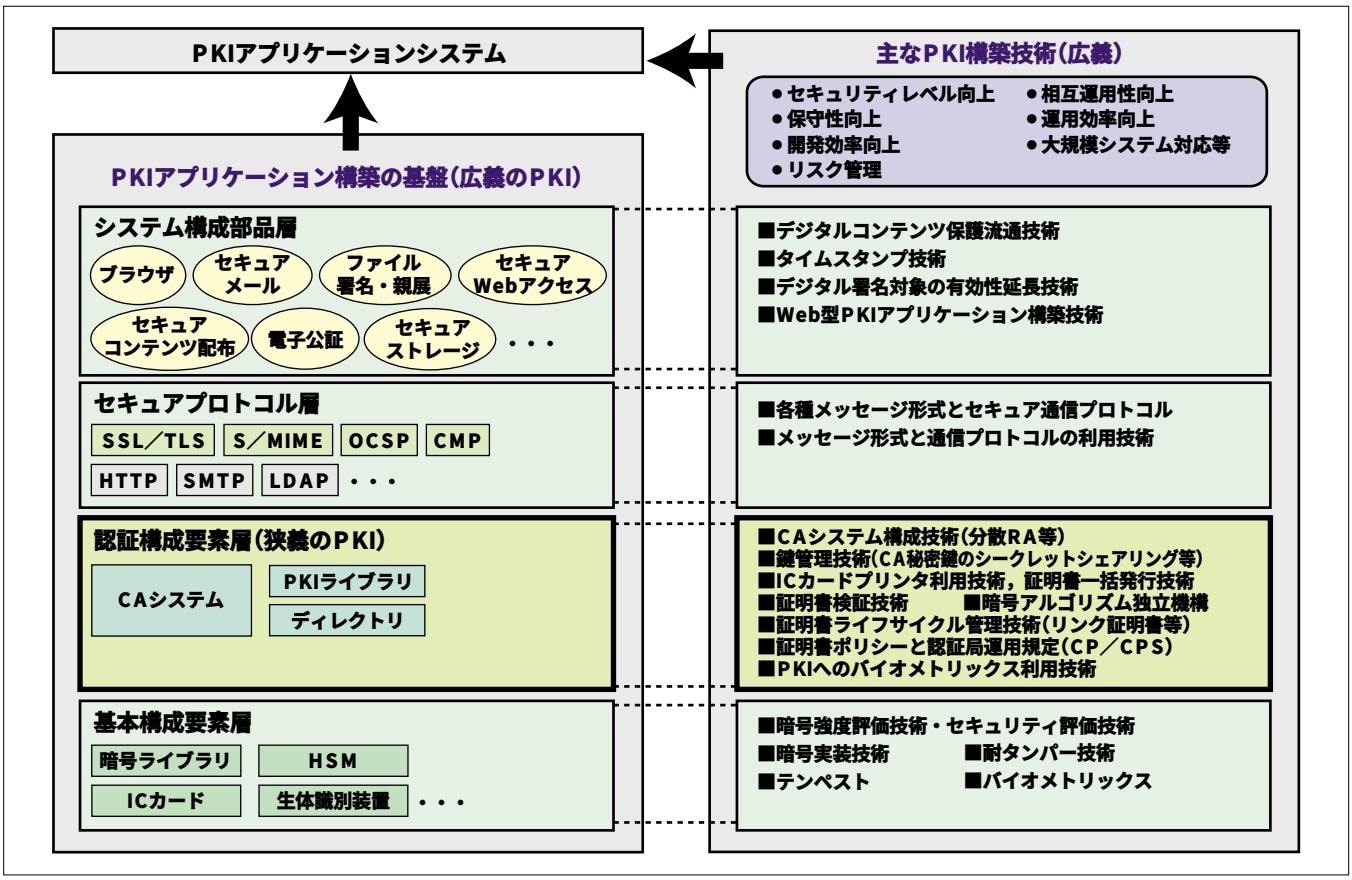
⑶　リンク証明書

世代の異なるCAから証明書を発行された利用者間での証明書検証を可能とする。利用者側の運用効率が向上する。

⑷　暗号アルゴリズム独立機構

PKIアプリケーションが用いる暗号アルゴリズムを容易に切換え可能とする。保守性が向上し，リスク管理にも有用である。

最後に，三菱電機PKIシステムの特長を簡単に紹介する。



PKI構成要素と構築技術

三菱電機PKIシステムは，多様なPKIアプリケーションの構築基盤とするために，基本構成要素層，認証構成要素層，セキュアプロトコル層，及びシステム構成部品層からなっている。本格的な実用に供するPKIアプリケーションを効率良く開発・運用し将来にわたって維持／改良していくために，この各層に対応した種々のPKI構築技術が重要となる。

*情報技術総合研究所