

保健医療福祉分野の情報化を安全と標準で支える ヘルスケアPKI対応ICカードミドルウェア

齋藤和美* 角野章之†
米田 健**
茗原秀幸***

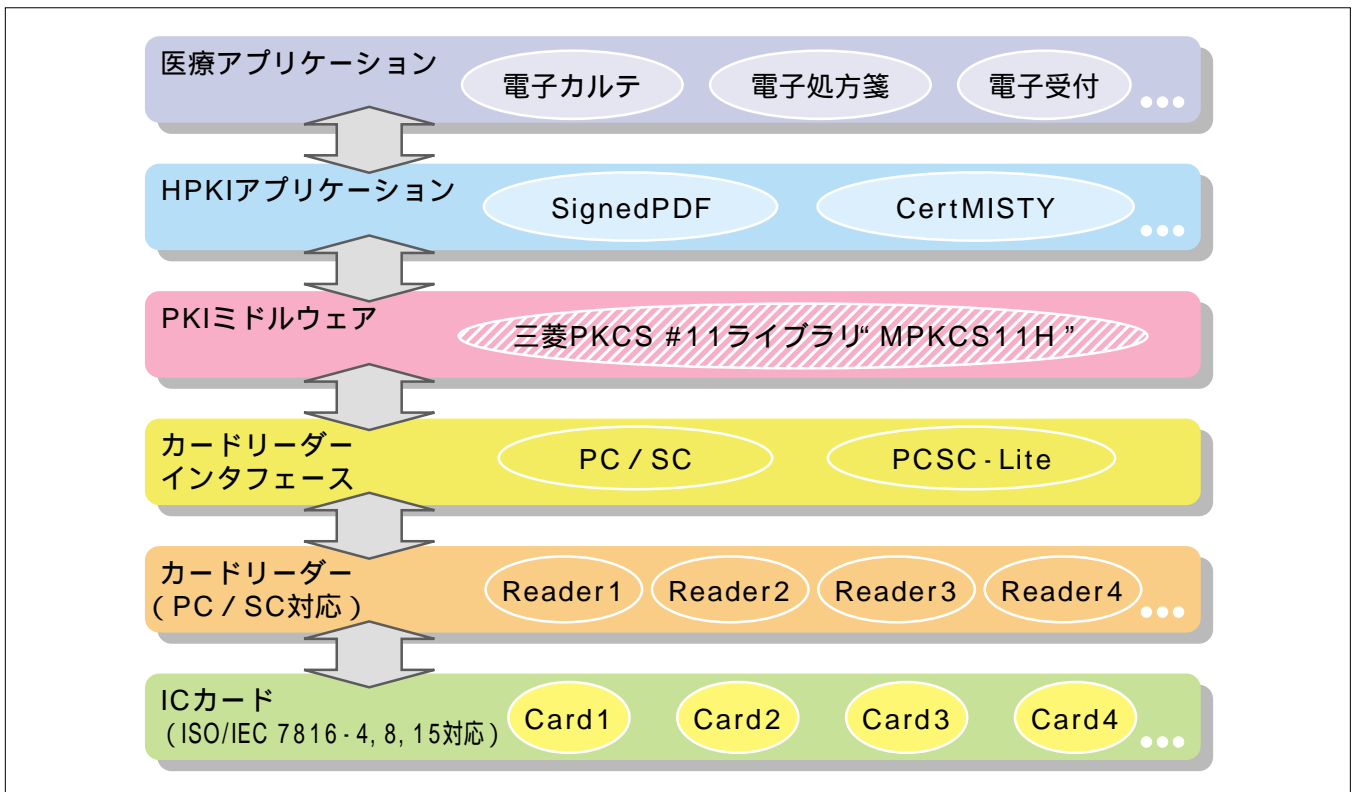
Smart Card Middleware for Healthcare PKI

Kazumi Saito, Takeshi Yoneda, Hideyuki Miyohara, Akiyuki Sumino

要 旨

近年、保健医療福祉分野では電子カルテに代表される情報システム化に伴い、ICカードを利用したヘルスケアPKI (Healthcare Public Key Infrastructure : HPKI)による電子署名の利用が普及しつつある。保健医療福祉分野は公的な分野であるため、特定のベンダーに依存しない標準的なICカードが求められる。ICカードの国際標準規格として、ISO/IEC 7816-4, 8, 15が制定されている。これら標準規格に準拠することで、カードインタフェース(I/F)やデータ構造がベンダーに依存しない。保健医療福祉情報システム工業会(JAHIS)は、医療従事者を対象とした“HPKI対応ICカードガイドライン”を2008年中に標準ガイドラインとして制定予定である。この仕様は標準的なICカードを採用し今後国内のヘルスケア分野への適用が見込まれる。我々は、この仕様に準拠する三菱ICカードミドルウェア

アとしてPKCS #11ライブラリ“MPKCS11H”を国内で初めて開発した。PKCS #11は、ICカードのような暗号トークンにアクセスするためのAPI(Application Program Interface)を定めた業界標準であり、ブラウザや公的個人認証サービス等多数のアプリケーションに利用されている。MPKCS11Hは、通信及びカードI/FにPC/SC(Personal Computer/Smart Card), ISO/IEC 7816-4, 8, 15を採用した。JAHISガイドライン準拠のICカードを用いて、秘密鍵(かぎ)による署名生成や証明書の取得が可能である。署名時のユーザー認証に関してISO/IEC 7816-15とPKCS #11の間で仕様の対応付けが困難な箇所が見られたが、安全性を保持しつつ解決した。今後は、ヘルスケアほか汎用用途に向けた機能拡張を実施していく。



三菱PKCS #11ライブラリ“MPKCS11H”の位置付け

MPKCS11HはJAHISガイドライン準拠ICカードを用いて、秘密鍵による電子署名生成やエンドエンティティ等の証明書取得機能を持つ。PC/SC, ISO/IEC 7816-4, 8, 15等の標準I/Fを使用し、カードやカードリーダーはベンダーに依存しない。三菱電子署名ソフトウェア“MistyGuard(注1)<SignedPDF(注2)>”や三菱認証ライブラリ“CertMISTY(注1)”等を介して医療従事者による電子カルテや電子処方箋等の電子署名をサポートする。

(注1) MistyGuard, CertMISTYは、三菱電機㈱の登録商標である。

(注2) SignedPDFは、三菱電機インフォメーションシステムズ㈱の登録商標である。