セキュリティライブラリ

辻　宏郷*
齋藤和美*

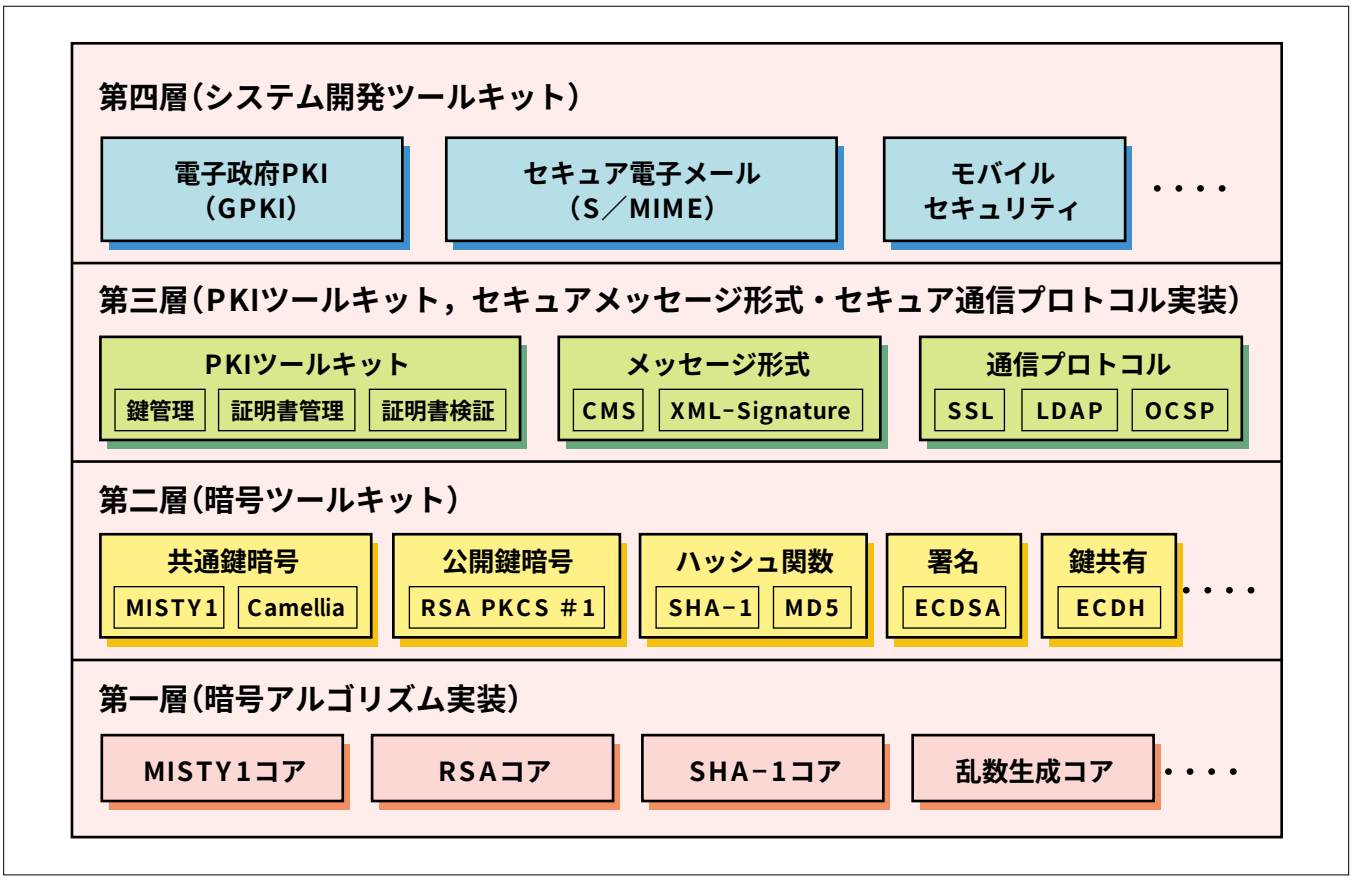
要　旨

セキュリティライブラリは，暗号技術を用いた情報セキュリティシステム開発に必要となる基盤技術（暗号アルゴリズム及び関連技術）を実装したミドルウェアである。情報セキュリティシステム構築には各種暗号アルゴリズム，かぎ（鍵）及び証明書の管理機能，セキュアメッセージのフォーマット機能，セキュア通信プロトコル等の実装が必要であり，必要となる暗号アルゴリズムやセキュリティ機能は，システムごとに異なっている。

三菱セキュリティライブラリでは，様々なシステム要件に対応するために，４階層モデルからなるアーキテクチャを設計した。このアーキテクチャでは，第一層：暗号アルゴリズム実装，第二層：暗号ツールキット，第三層：PKI（Public Key Infrastructure）ツールキット，セキュアメッセージ形式・セキュア通信プロトコルの実装，第四層：システム開発ツールキットと定義し，各層の構成要素となるライブラリ，コンポーネントを実装した。

PKI暗号ライブラリ“ MCrypto ”は，第二層及び第三層に対応する構成要素で，暗号アルゴリズム独立，鍵管理・証明書管理機能，証明書検証機能，生体識別情報を用いた認証機能等の特長を持っている。組み込み機器向け暗号ライブラリ“ MC ”は，第一層に対応する構成要素で，省資源での動作，可搬性といった組み込み機器での要件を満たすために，必要メモリ容量を制御・削減可能なメモリ管理方式，必要機能に応じたモジュールの再構成，プラットフォームごとに最適化したアルゴリズム・コア採用等の特長を持っている。

今後は，サポートするプラットフォームの拡大や最新標準規格への対応を行っていく予定である。



三菱セキュリティライブラリのアーキテクチャ（４階層モデル）

セキュリティライブラリの実装において，４階層モデルからなるアーキテクチャを設計し，各層において提供すべき機能を定義した。第一層は，暗号アルゴリズム（共通鍵暗号，公開鍵暗号，ハッシュ関数等）の実装である。第二層は，暗号ツールキットである。第三層は，PKIに対応する鍵管理機能・証明書管理機能等を実装したPKIツールキット，セキュアメッセージのフォーマット機能とセキュア通信プロトコルの実装である。第四層は，アプリケーションごとに特化したインタフェースを提供するシステム開発ツールキットである。

*情報技術総合研究所