公開鍵インフラストラクチャ構築技術

佐伯正夫*　坂上　勉**
吉武　淳*
辻　宏郷*

要　旨

公開かぎ(鍵)インフラストラクチャ(Public Key Infrastructure：PKI)は，盗聴，改ざん，成り済まし等の脅威を防ぐための，“公開鍵暗号技術に基づくセキュリティサービスを提供する，鍵及び認証書の管理を行う構成要素・機能・手続きの集合”であり，多様な情報システムにわたって，認証，アクセス制御，改ざん防止，秘匿及び否認防止を効率的に実現するための共通基盤技術である。業界標準に基づき，三菱電機情報セキュリティアーキテクチャに沿って三菱電機PKIを構築した。

その構築技術を，主要構成要素と主な特長を中心にして紹介する。

⑴　各種業界標準に準拠し多様な応用システムに適用可能

WWW(World Wide Web)で使用するSSL(Secure Socket Layer)対応認証書，S／MIME(Secure／Multipurpose Internet Mail Extensions)メーラ対応認証書など，用途に応じた認証書を選択・定義できる認証サーバシステムと，移行性・相互運用性・拡張性を付与する応用システム構築用ライブラリを提供する。

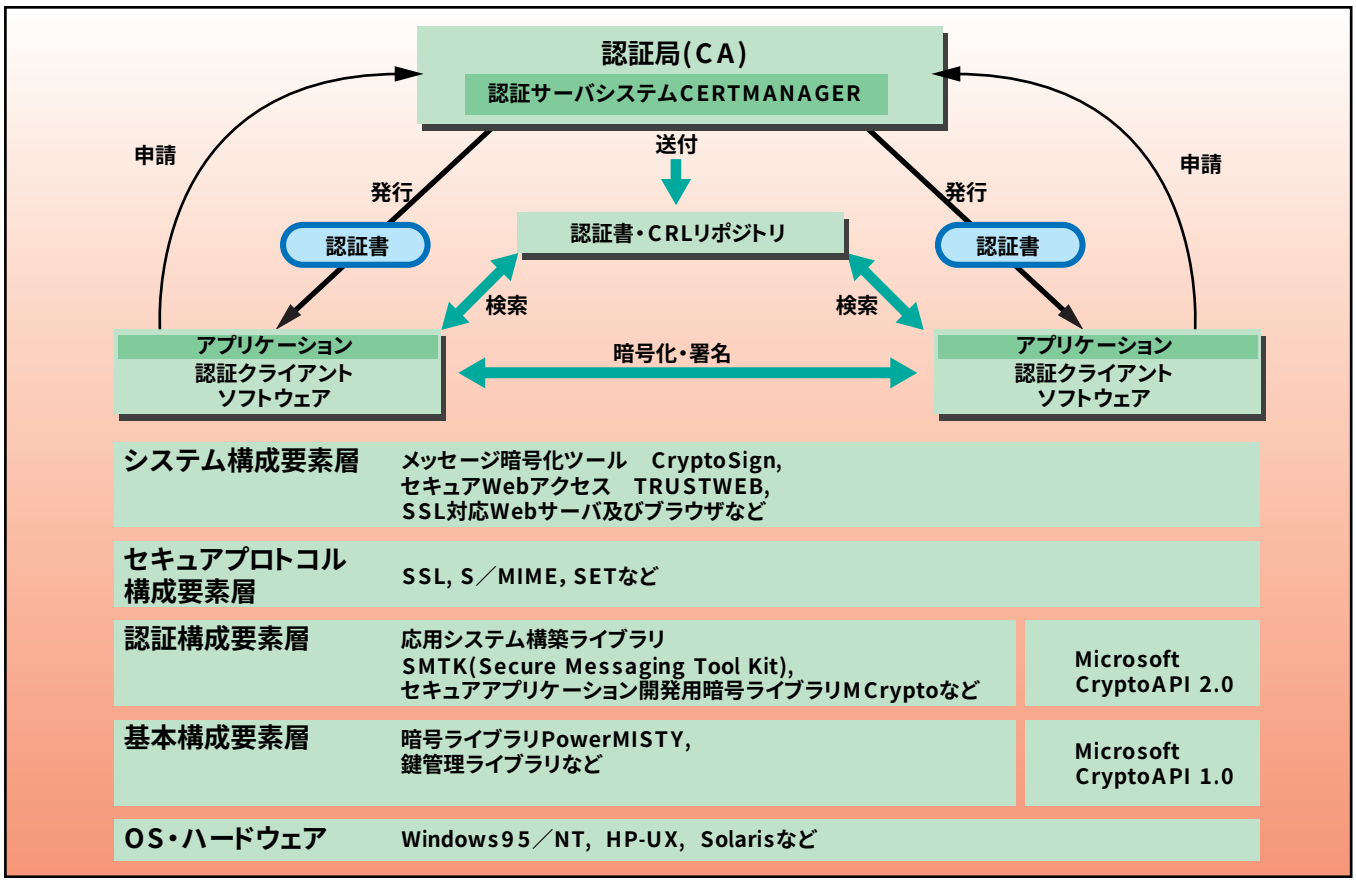
⑵　企業向け機能を豊富に用意

社員の手間をかけずに管理部門が一括代行して鍵と認証書を発行・管理するための一括代行申請機能，社員の鍵紛失，パスワード忘れ，退職等に対してリカバリーを可能とするキーアーカイブ・認証書再発行機能等を提供する。

⑶　世界最高水準の強度を誇るMISTY鍵による暗号化

⑷　応用システム構築を簡便化するメッセージ暗号化ツール，Webサーバアクセス等のシステム構成要素群を提供

最後に，PKIの新しい構成要素である“キーリカバリーシステム”を紹介する。



PKI構成概念図

PKIは，多様な応用システムにわたって，“公開鍵暗号技術に基づくセキュリティサービスを提供する，鍵及び認証書の管理を行う構成要素・機能・手続きの集合”であり，認証局(Certification Authority：CA)，認証書及び認証取消リスト(Certification Revocation List：CRL)のリポジトリ，認証クライアントソフトウェア，及びそれらを構築するための各種構成要素からなる共通基盤システムである。

*情報技術総合研究所　**情報システム製作所