

# 三菱電機情報セキュリティアーキテクチャ

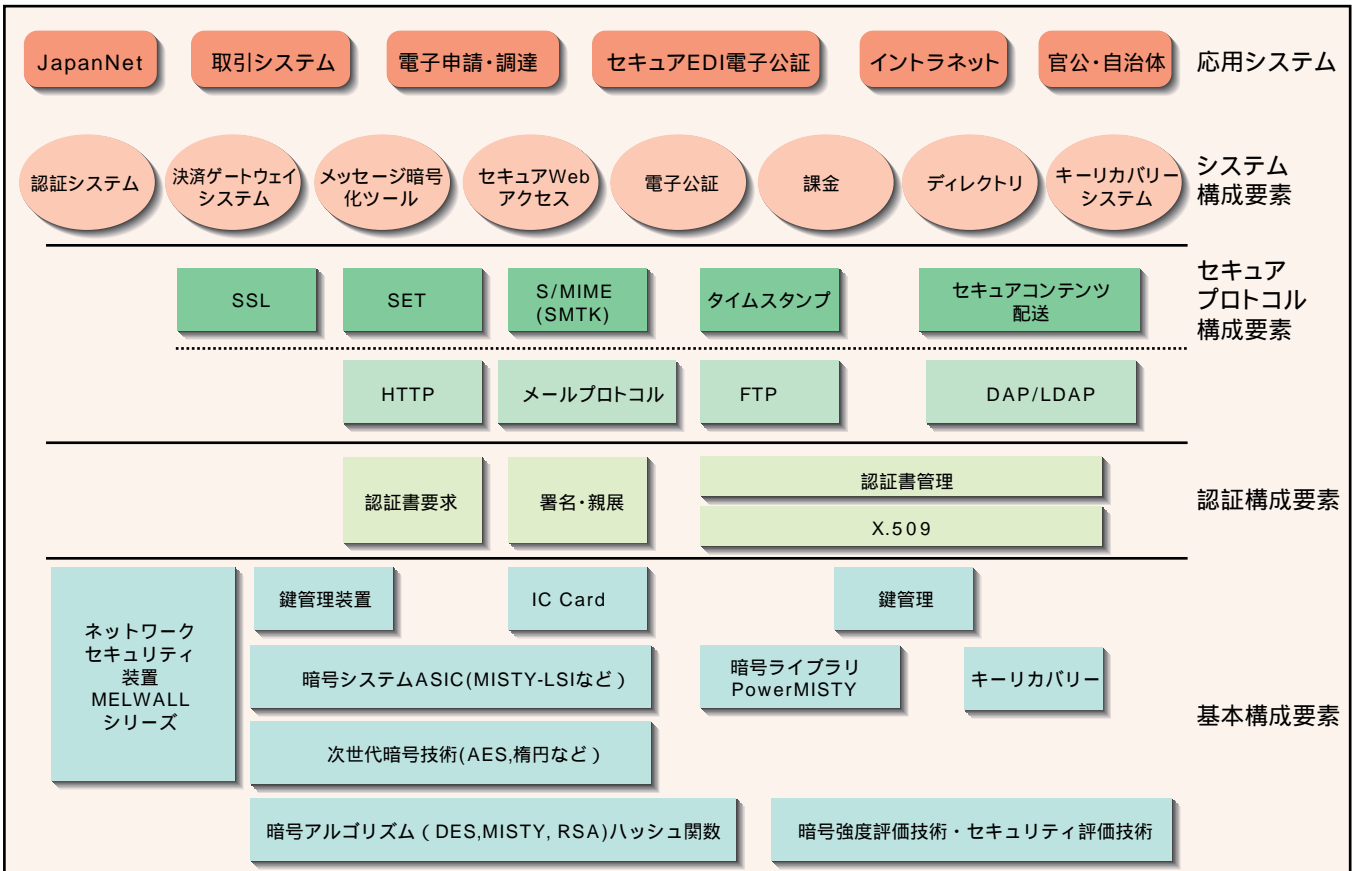
勝山光太郎\* 米田 健\*  
藤井誠司\*\*  
鈴木 博\*\*\*

## 要 旨

インターネットの爆発的普及により、盗聴、改ざん、成り済ましといった脅威から情報システムを安全に守ることが、これまで以上に大きな課題となっている。これまで、情報の秘匿に重点のあった情報セキュリティ技術も、公開かぎ(鍵)のインフラ構築により、認証や否認防止といった面での応用が展開されるようになってきた。

情報セキュリティの適用分野を特定秘匿型、協調交流型、参加閲覧型、大規模不特定認証型の四つに大別し、これらに適用するセキュリティソリューションとして、セキュア通信ソリューション、セキュアメールソリューション、セキュアWebアクセスソリューション、セキュア認証システムソリューション、セキュアEDIソリューション、セキュアECソリューションを実現する。

これらのソリューションを提供するための構成要素を定義したものが、情報セキュリティアーキテクチャである。基本構成要素、認証構成要素、セキュアプロトコル構成要素、システム構成要素の4階層からなる。基本構成要素は、暗号アルゴリズム、暗号強度評価技術を基盤とし、暗号ASICや暗号ライブラリで構成される。認証構成要素は、認証書を扱うライブラリ群からなる。セキュアプロトコル構成要素は、SSL(Secure Socket Layer)やS/MIME(Multimedia Internet Mail Extension)といったプロトコルの規格に準拠したライブラリ群からなる。システム構成要素は、認証システムや電子公証システムといった要素からなる。これらを利用して様々な応用システムが構築される。



## 三菱電機情報セキュリティアーキテクチャ

情報セキュリティアーキテクチャは階層構造をとり、基本構成要素、認証構成要素、セキュアプロトコル構成要素、システム構成要素からなる。これらを組み合わせて応用システムを構築する。