巻頭論文

暗号・情報セキュリティの動向


小野修一*


小松田敏二**


竹田栄作***

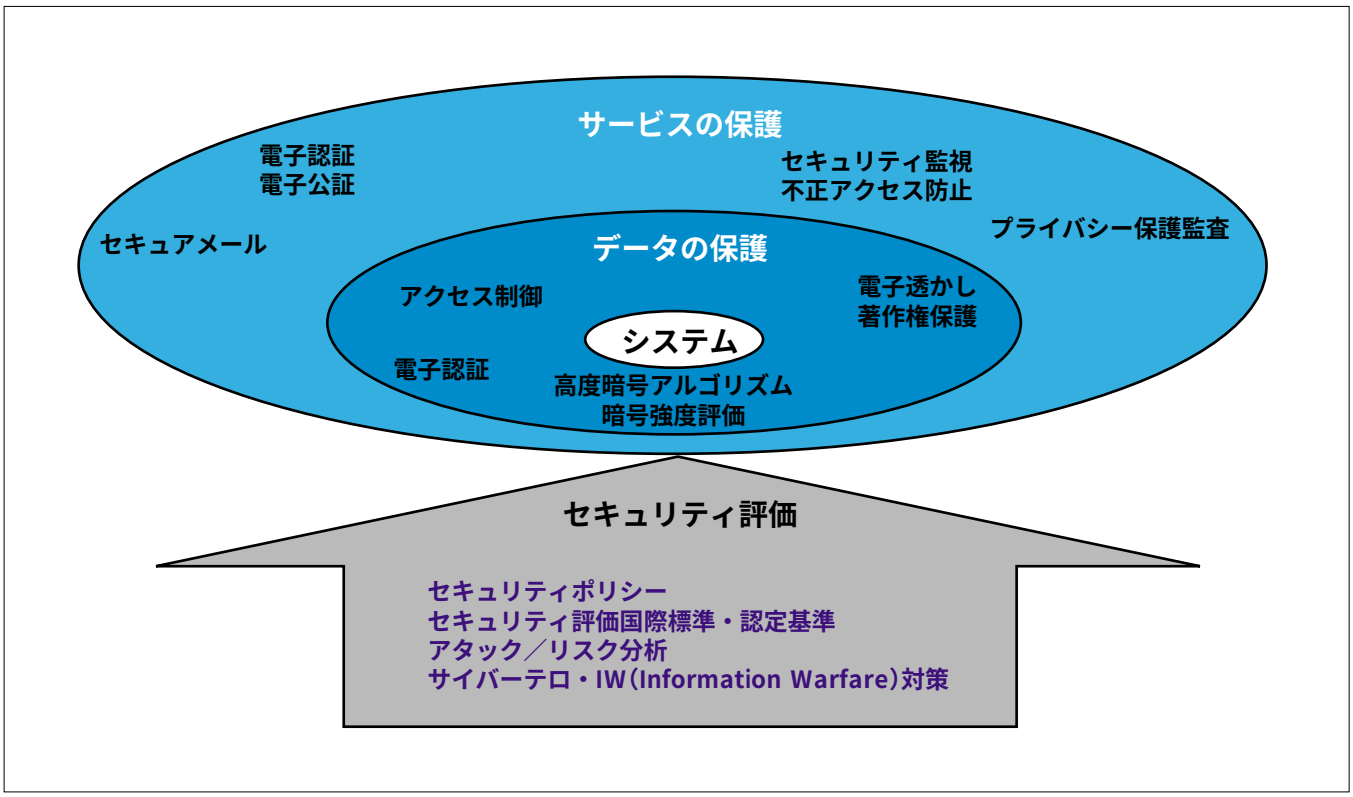
要　旨

インターネットに代表されるネットワークと携帯電話が結び付いて文字どおり地球規模のデジタル社会が出現し，社会制度や公共の情報基盤も，それを反映した形態に変化しつつある。今後のデジタル社会をいかに安全なものにしていくかは，国家・社会の基盤にとってその存続にかかわる重大問題であり，企業にとっては死命を制するビジネス課題になっている。それらを支える情報基盤の核となるものが，暗号を中心とする情報セキュリティである。

現代において，なぜ　暗号・情報セキュリティが必要であるか，その役割と意味は何か，どのような応用分野，課題があるかを展望する。さらに，暗号とは何か，その安全性の意味とは何か，コンピュータや通信のデジタル技術とどのような関連にあるのかを，歴史的背景と近年の動向を踏まえて言及し，現代暗号の成り立ち，情報セキュリティの適用形態，三菱電機における技術的活動について触れる。

今後の動向として次に，二つの特徴的な話題を取り上げる。携帯電話の世界的普及，インターネット接続機能の装備により，現在のインターネットのユーザー規模をはる(遥)かにりょうが(凌駕)した音声交信可能なモバイルインターネットの出現が予測される。モバイルインターネットが潜在的に持つ安全上のぜい(脆)弱性を克服するためには，暗号・情報セキュリティの技術はより高度なものが求められる。

また，将来的な量子コンピュータの出現等，分子レベルに迫る半導体・光素子・通信の技術の先に，現在のデジタル暗号によるセキュリティ基盤の安全性の限界が論じられている。デジタル社会の安全性の確保には将来を見据えた技術の追求が要請されており，その代表的なものとして，量子力学の原理，光技術，デジタル技術を統合した量子暗号がある。三菱電機は，2000年９月に国内初の量子暗号の実証実験に成功し，早期の実用化を目指している。



デジタル社会に向けた暗号・情報セキュリティ技術

暗号・情報セキュリティ技術をユーザーの視点から見ると，データを保護するためのもの，サービス機能を保護するためのもの，これら保護機能・仕組みを評価し保証するためのものに大別される。

*情報技術総合研究所長　**インフォメーションシステム事業推進本部情報セキュリティ推進センター長　***情報技術総合研究所 情報セキュリティ技術部長