ユビキタスセキュリティ技術

松井　充*　山田敬喜*
反町　亨*　時田俊雄**
佐伯　稔*

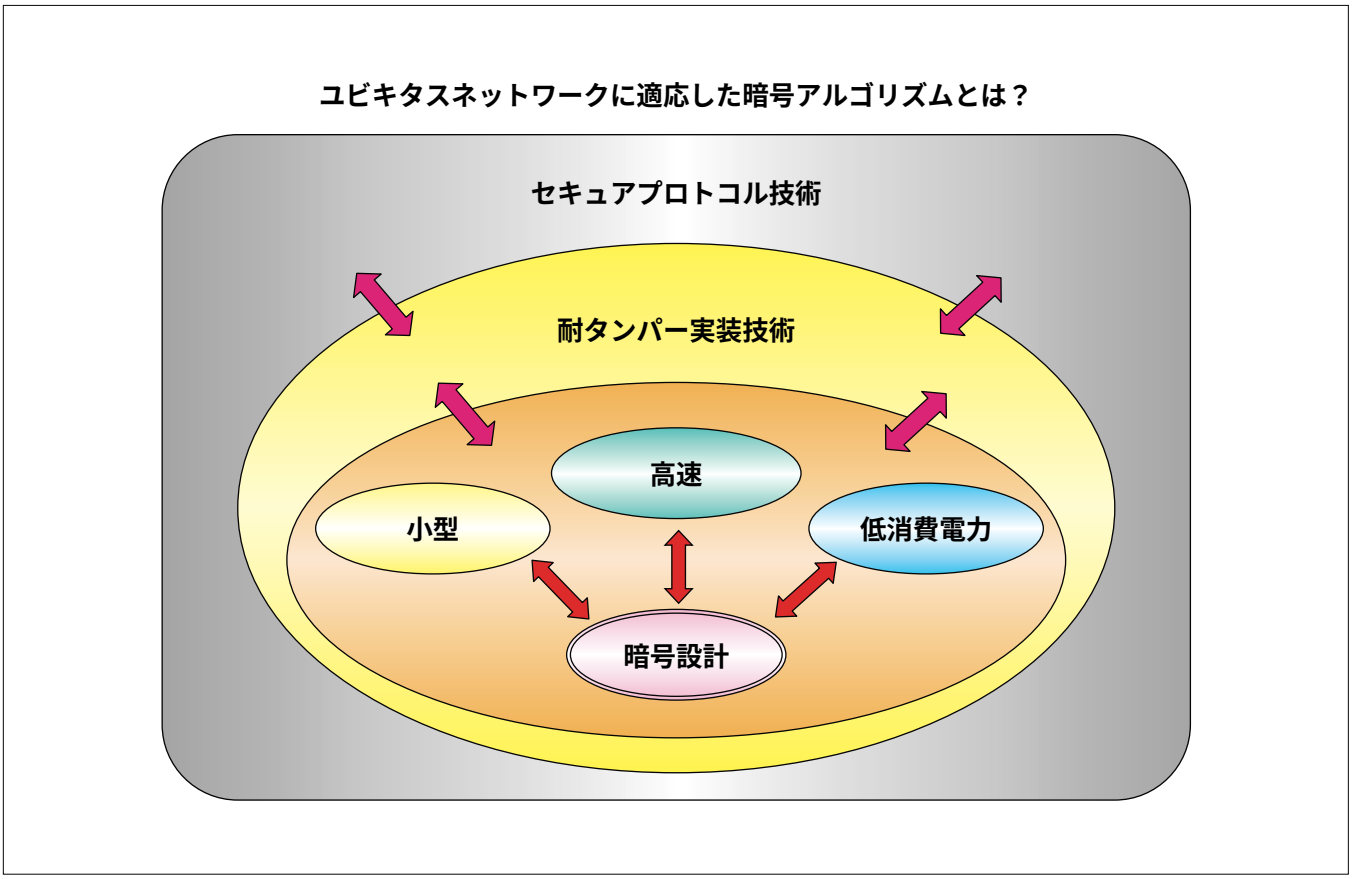
Security Technology for Ubiquitous Network

Mitsuru Matsui, Tohru Sorimachi, Minoru Saeki, Keiki Yamada, Toshio Tokita

要　旨

ユビキタスネットワークの進展に伴い，データの盗聴・偽造・改ざんなどの防止又は検出などを実現する情報セキュリティ技術の重要性は更に増していくものと思われる。その中でも暗号技術は，情報セキュリティ技術の最重要な基盤技術の一つとして今後とも不可欠であろう。本稿では，ユビキタスネットワークに望まれる暗号技術について述べる。三菱電機は，これまで，“MISTY”やNTT㈱との共同開発の“Camellia”など安全性と実用性の両面に優れた暗号アルゴリズムを開発してきた。これらは，安全であるとともに，ハードウェアやソフトウェアのいずれにおいても，小型・高速実装可能なマルチプラットフォーム対応を特長としてきた。ユビキタスネットワークにおいてもこれらの暗号アルゴリズムで大部分の領域をカバーできる。しかし，あらゆる機器やセンサに通信機能を持たせることを前提とするユビキタスネットワークにおいては，更に省実装（小型・低消費電力）で高速な暗号が必要となるケースが発生すると予測される。

本稿では，ユビキタスネットワークで必要とされる暗号アルゴリズムの性能要件について整理し，当社がユビキタスネットワークへの適用をターゲットとする暗号アルゴリズムの性能仕様を示す。また，それら暗号アルゴリズムを実装する上で考慮する必要のある耐タンパー実装技術やセキュアプロトコル技術についても，最新の研究開発動向を中心に述べる。



暗号アルゴリズムの設計と実装への要求（イメージ）

今後ユビキタスネットワークの進展に伴い，暗号アルゴリズムの設計と実装への要求はますます拡大していくものと思われる。

*情報技術総合研究所　**同研究所（工博）