次世代ネットワークにおける セキュリティ技術

近澤　武*
後沢　忍*

Security Technologies for Next Generation Network

Takeshi Chikazawa, Shinobu Ushirozawa

要　旨

NGN（Next Generation Network）と呼ばれる次世代ネットワークは，インターネットとは異なり，通信品質やセキュリティが確保されることに特長がある。

NGNのセキュリティについて，いろいろと検討され，多くの課題が挙げられているが，これらの課題のうち，“通信の盗聴等”に対しての“通信の秘密を確保する対策”として有効な“暗号技術”は重要な技術の一つである。

三菱電機とNTTが共同開発した暗号アルゴリズム“Camellia(注1)（カメリア）”は，安全性と性能に優れており，NGNの暗号としても提案されている。またCamelliaは，NGNとそこにつながる企業間で使用可能な当社製超高速VPN（Virtual Private Network）装置にも搭載されている。さらに当社は，NGNのネットワーク高速化に対応可能な高速暗号アルゴリズム“BROUILLARD(注2)（ブルイヤール）”や，NGNに接続される様々な機器に実装される暗号に適した小型暗号アルゴリズム“BRUME(注2)（ブリュム）”を開発済みである。

（注１）　Camelliaは，日本電信電話㈱と三菱電機㈱の登録商標である。
（注２）　BROUILLARD，BRUME，MISTYは，三菱電機㈱の登録商標である。

NGNで提案されている暗号アルゴリズム“Camellia”を搭載した超高速VPN装置の外観

当社では，ネットワークの高速化と暗号アルゴリズムの進化に柔軟に対応できる暗号処理アーキテクチャとして，階層型並列処理方式を確立した。この方式をネットワーク上でデータの暗号化を行うIPsec（Security Architecture for Internet Protocol）VPN装置に適用し，世界で初めて10Gビットイーサネット上でのワイヤスピード（ネットワークの持つ最大通信速度）を達成した。実装している暗号アルゴリズムは，NGNで提案されているCamelliaのほか，MISTY(注2)，AES，Triple-DESである。

*情報技術総合研究所