M-042

暗号・ハッシュアルゴリズムの処理性能から導かれる，低コストネットワーク機器としての 16 ビット CPU の可能性

16-bit CPUs' potential for low-cost network appliances supporting cryptographic and hash algorithms

田中 康之† 土野 春菜† 米山 清二郎† 神明 達哉†
Yasuyuki TANAKA Wakana TSUCHINO Seijiro YONEYAMA Tatuya JINMEI

1 はじめに

TCP/IP ネットワーク機能の適用範囲は組み込み機器にまで拡大してきた．また，インターネット上ではデータの暗号化や通信相手認証を行うことが一般化してきている．そのため，今後は組み込み機器に対しても，データを暗号化する機能や通信相手認証の機能（これら 2 つの機能をまとめて「セキュリティ機能」と呼ぶ）が要求されると考えられ，組み込み機器に広く用いられている，8 ビット CPU や 16 ビット CPU のセキュリティ機能の処理性能を把握することが重要になる．

8 ビット CPU については，岡部らが共有鍵暗号アルゴリズムやハッシュアルゴリズム，そして IPsec の処理性能を示している [1]．岡部らの成果から，8 ビット CPU のセキュリティ機能の処理性能をある程度把握できる．16 ビット CPU については，個別のアルゴリズムの性能評価はあるものの [2]，暗号アルゴリズムとハッシュアルゴリズム，ネットワーク処理の性能評価をまとめた報告は無い．そのため，セキュリティ機能を備えたネットワーク機器としての，16 ビット CPU の処理性能を見積もることが難しい．組み込み機器の多機能化・高機能化はますます進むと思われるため，8 ビット CPU よりも処理能力が高く，扱えるメモリ空間が広い 16 ビット CPU のセキュリティ機能の処理性能が把握できないことは問題である．

そこで，本発表では 16 ビット CPU のセキュリティ機能について性能評価を行い，センサノードや音声通信に対する 16 ビット CPU の利用可能性について議論する．そして，データの暗号化や通信相手認証が可能なネットワーク機器としての 16 ビット CPU の可能性について検討する．測定対象のアルゴリズムは，共有鍵暗号アルゴリズムの 3DES と AES，そして，ハッシュアルゴリズムの MD5 と SHA-1 である．その他に，Diffie-Hellman 鍵交換方式 (以下，DH) と公開鍵暗号アルゴリズムの RSA の処理時間も測定した．さらに，暗号やハッシュアルゴリズムの処理性能とネットワークの処理性能を比較するため，16 ビット CPU における UDP の性能測定を行った．ネットワークの処理性能測定では，インターネットプロトコルとして今後の普及が見込まれる IPv6 を使用した．

† 株式会社東芝 研究開発センター 通信プラットホームラボラトリー

表 1 共有鍵暗号アルゴリズムおよびハッシュアルゴリズムの処理性能

アルゴリズム	鍵長 bit	初期ベクトル	処理	性能 (KB/s)
3DES (CBC)	192	8 byte	暗号化	3.5
			復号化	3.5
AES (CBC)	128	16 byte	暗号化	18.8
			復号化	18.7
MD5	128	N/A	N/A	127
SHA-1	160	N/A	N/A	36

2 評価環境

測定対象となる 16 ビット CPU は東芝製の TLCS-900/L1(TMP91C824)[3] である．測定ではシステムクロックを 16.5MHz とした．コンパイラは東芝製 TLCS-900 ファミリ用コンパイラを使用している．暗号アルゴリズムやハッシュアルゴリズムの測定はリアルタイムエミュレータを用いて行い，各アルゴリズムの処理時間計測は CPU カウンタを利用した．

暗号やハッシュアルゴリズムの性能測定に使用したソフトウェアは OpenSSL(バージョン 0.9.8a) と rsaref(バージョン 2.0p3) である．OpenSSL からは 3DES，AES，MD5，SHA-1 の実装を，rsaref からは DH と RSA の実装を抽出し，TLCS-900 用に改変して使用した．

ネットワーク処理の性能測定には我々の TCP/IPv6 スタックを使用した．ネットワークインタフェースは Realtek RTL8019AS(10Base-T) である．ネットワークの処理性能測定では，16 ビット CPU を搭載したボードと測定用 PC をクロスケーブルで直接接続した．ここで，測定用 PC は 16 ビット CPU に比べて十分高性能であるため，16 ビット CPU の性能測定結果において測定用 PC の処理オーバヘッドは無視できると考えられる．また，クロスケーブル上の伝搬遅延も無視できるほど十分小さいと考えられる．

3 結果

3.1 暗号・ハッシュアルゴリズム

16 ビット CPU における 3DES と AES，そして MD5 と SHA-1 の処理性能は表 1 のようになった．

DH の性能測定では．素数長が 1024 bit の場合，DH の公開鍵と共有鍵の計算におよそ 5 分かかった．RSA では，鍵長が 1024

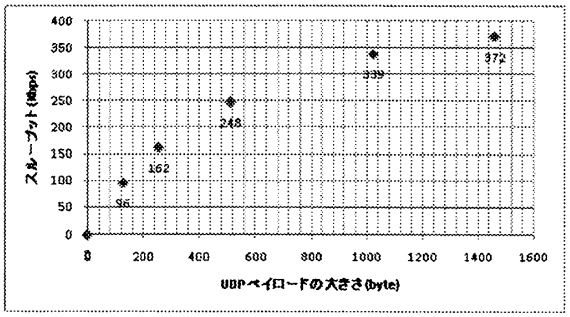

図 1　UDP の送受信処理性能

バイトで入力データが 32 バイトのとき，公開鍵による暗号化に 2.4 秒，秘密鍵による復号化に 45.6 秒要した．

3.2　ネットワーク処理

ネットワーク処理の性能測定は，UDP のエコーサーバプログラムを 16 ビット CPU 上で実行させて行った．図 1 に測定結果を示す．測定用 PC からエコーサーバに対して送信した UDP データグラムが測定用 PC で受信されるまでの時間を測定することで，16 ビット CPU における UDP の送受信性能が求められる．ただし，ここで得られる結果にはエコーサーバプログラム自体のオーバヘッドが含まれる．測定用 PC から送信するデータグラムのサイズは 128，256，512，1024，1452[*1] バイトの 5 パターンで変えて測定を行った．MTU サイズは 1500 バイトであり，本測定ではいずれのパターンでもフラグメンテーションは発生していない．

TCP についても UDP と同様の性能測定を実施した結果，TCP と UDP の処理性能にオーダレベルの差は見られなかった (ただし，詳細は省略)．

4　考察

以上の結果から，共有鍵暗号アルゴリズムとハッシュアルゴリズム，そしてネットワーク処理の性能を比較すると，共有鍵暗号アルゴリズムの処理負荷が一番大きく，共有鍵暗号アルゴリズムの処理がボトルネックになることがわかった．そこで，共有鍵暗号アルゴリズムの処理性能測定結果を元に，セキュリティ機能を持つネットワーク機器としての 16 ビット CPU の可能性を考察する．

はじめに，組み込みネットワーク機器で実装されることが多いセンサノードにおいてデータの暗号化や通信相手認証を実施することを考える．センサノードでは取得したデータの送信間隔が数分から数十分と長いことが多く，データの暗号化に数秒程度の時間がかかっても問題ない．ここでは具体的に，環境データを扱うセンサノードを 16 ビット CPU で実装した想定で，データの暗号化に必要な時間の見積りを行う．環境データの場合，センサノードが 1 つのセンサから取得する情報は数バイトで表現できる．センサで得られた情報の他に過去の履歴やセンサノード自体の情報をリモートホストへ提供するとしても，一度の転送量は数 KB であろう[*2]．16 ビット CPU でも，数 KB 程度のデータであれば AES なら 1 秒以内，3DES なら 2,3 秒のうちに暗号化を完了することが出来る．よって，このようなセンサノードに対しては，16 ビット CPU を用いてデータの暗号化や通信相手認証を行うことができると言える．

次に，センサノードよりもリアルタイム性が求められる通信として，音声通信を 16 ビット CPU で暗号化することを考える．表 1 より，16 ビット CPU における AES の暗号化と復号化の処理性能はそれぞれ約 144kbps であるため，コーデックの処理負荷が小さければ，リアルタイム通信の暗号化を 16 ビット CPU で実現できる可能性がある．スピーカーやマイク，ネットワークインタフェースカードの制御オーバヘッドを考慮する必要があるが，16kbps や 32kbps 程度の音声通信ならば 16 ビット CPU で実現できるであろう．

以上から，センサノードのようにある程度の遅延が許される通信や音声データのような低ビットレートのリアルタイム通信であれば，16 ビット CPU を用いてデータの暗号化や通信相手認証が行えると結論づける．

しかし，データ暗号化や通信相手認証を行うための鍵交換をどのように実施するかは問題である．性能測定結果からわかるように，16 ビット CPU による DH や RSA の処理は非常に負荷が大きく，DH や RSA の使用を前提とした鍵交換方式を 16 ビット CPU に適用するのは非現実的である．そのため，暗号鍵の共有は手動設定とするか，KINK[5] など，DH や RSA を使用しない鍵交換方式を考える必要がある．

5　まとめ

16 ビット CPU における暗号アルゴリズムやハッシュアルゴリズム，そしてネットワーク処理の性能測定結果から，ある程度の遅延が許容される通信や低ビットレートのリアルタイム通信ならば，16 ビット CPU を用いてデータの暗号化や通信相手認証が実施できることがわかった．ただし，鍵交換方式については，事前の手動設定とするか，KINK[5] など，DH や RSA を使用しない鍵交換方式を考える必要がある．

参考文献

[1] N. Okabe, S. Sakane, K. Miyazawa, K. Kamada, A. Inoue, and M. Ishiyama. Security Architecture for Control Networks using IPsec and KINK. *SAINT2005, The 2005 International Symposium on Applications and the Internet*, 2005.

[2] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu. Analyzing and modeling encryption overhead for sensor network nodes. *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pages 151–159, 2003.

[3] TLCS-900/L1. http://www.semicon.toshiba.co.jp/product/micro/900family/900l1/index.html.

[4] Live E! http://www.live-e.org/.

[5] S. Sakane, K. Kamada, M. Thomas, and J. Vilhuder. Kerberized Internet Negotiation of Keys (KINK). RFC 4430, Mar. 2006.

*1 MTU サイズから IPv6 ヘッダと UDP ヘッダの 48 バイトを差し引いた 1452 バイトがフラグメントを起こさない最大の UDP ペイロードサイズ．

*2 Live E![4] の Sensor Data Upload Interface Specification には，約 4KB 程度のアップロードデータの例が示されている．