様式 C-19

科学研究費補助金研究成果報告書

平成２４年　６月　１日現在

機関番号：11101
研究種目：若手研究（B）
研究期間：2009　～　2010
課題番号：21700064
研究課題名（和文）　高速低電力動作再構成可能ロジックを有する高精度ホストベース IPS プロセッサの開発
研究課題名（英文）　Development of a Host-Based IPS Processor with a Reconfigurable Logic for High-Speed and Low-Power Operations
研究代表者
佐藤　友暁　　（SATO TOMOAKI）
弘前大学・総合情報処理センター・准教授
研究者番号：00336992

研究成果の概要（和文）：
本研究はモバイルコンピュータに搭載可能なホストベースの IPS (Intrusion Prevention System)プロセッサの開発である。本プロセッサは，ファイアウォールロジックユニットと再構成可能なロジックセルで構成される。ファイアウォールロジックユニットはロジックレベルのシグネチャでファイアウォール機能を実現する。その機能は通常のファイウォール機能に加え,低消費電力化およびシグネチャの削減のために不可欠である。再構成可能なロジックセルは，通常のロジックセルと遅延調整向けロジックセルで構成される。高速化・低消費電力化設計を施した８ビットの加算回路による比較を行った結果，遅延調整向けロジックセルを使用した回路は，通常のロジックセルを使用したものに比べ28.5%の面積で実現することが明らかになった。

研究成果の概要（英文）：
In this study, an IPS (Intrusion Prevention System) processor which is used on mobile computers is developed. The processor is composed of Firewall Logic Unit and reconfigurable logic cells. The firewall function of Firewall Logic Unit is executed by hardware logic. The unit is useful for low-power operations and reduction in number of signatures. The reconfigurable logic cells are composed of conventional logic cells and logic cells for the timing adjustment. Two 8-bit adder circuits are designed by design method for high-speed and low-power operations. One is the use of conventional logic cells and the other is the use of conventional logic cells and logic cells for the timing adjustment. The results of comparing areas of these circuits are the area of the circuit using logic cells for the timing adjustment is reduced to 28.5%.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,400,000	420,000	1,820,000
2010 年度	1,900,000	570,000	2,470,000
年度			
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：IDS，IPS，セキュアネットワーク，ファイアウォール，低消費電力，無線 LAN，再構成可能ロジック，ウェーブパイプライン

１．研究開始当初の背景

不正アクセスやコンピュータウイルスによる情報漏えいや情報改ざんは今日の重要な問題になっています。特に個人の PC (Personal Computer)環境においては，以下の理由により不正アクセスの被害，踏み台に利用された被害，情報漏えいの被害が深刻になっております。

・PC の管理が徹底されていない
・常時接続・ブロードバンド化の一般化および公衆無線 LAN アクセスポイント (AP)の普及
・Winny 等の P2P (Peer to Peer)ファイル交換ソフトウェアの普及

これらの問題に対し，IDS (Intrusion Detection System)や IPS による監視と被害防止が不可欠です。現在の IDS と IPS の問題点を設置場所による分類で整理すると問題点は次の通りです。

ホストベース IDS/IPS
・検知処理において CPU を使用するため,CPU リソースやバッテリ電力を消費する
・CPU 負荷の高いパケットレベルでの詳細な解析は不可能
・CPU 負荷が高くなる高精度のアノマリ検知が不可能

ネットワークベース IDS/IPS
・LAN 内部のクライアント間で発生する検知が不可能
・ネットワークを流れるパケット量によっては，すべてのパケットを解析不可能
・IDS/IPS 処理専用の高性能計算機が必要(ソフトウェアを含め非常に高価です)
・設置形態によっては，通信の秘密を侵害する解析方法が不可能

２．研究の目的

本研究は，不特定多数がバッテリで駆動するモバイル機器を使用する無線 LAN 環境下やモバイル WiMAX 環境下においても，不正アクセス，踏み台利用，情報漏えいから情報やコンピュータシステムを完全に保護できることを目的とし，そのために必要なプロセッサの開発を行うことが研究の目的です。

３．研究の方法

研究目的を達成するために，ウェーブパイプライン設計向けロジックセルの開発およびファイアウォールロジックユニットの開発を行う。これらの評価を行うことで，IPS プロセッサの優位性を明らかにすることが本研究の主な方法です。

FPGA は容易に回路の書き換えが可能なため、常に新しい不正アクセス検知回路を追加することができます。このためホストベース IPS プロセッサは FPGA と同等の機能が必要です。しかし、既存の FPGA はウェーブパイプライン設計を考慮していません。

FPGA を使用してウェーブパイプライン化設計を行うと遅延調整のために大量の LUT を消費します。本研究では，この問題を解消するために，ウェーブパイプライン設計の際に必要となる遅延調整が容易で大量のバッファを消費しないロジックセルを開発します。

ファイアウォールロジックユニットを，最適設計します。さらにこのロジックユニットから不正アクセス検知回路のクロックを制御することで，電力消費の削減につなげます。

図１にホストベース IPS プロセッサを示します。このプロセッサ上にウェーブパイプライン設計向けロジックセルおよびファイアウォールユニットを搭載します。

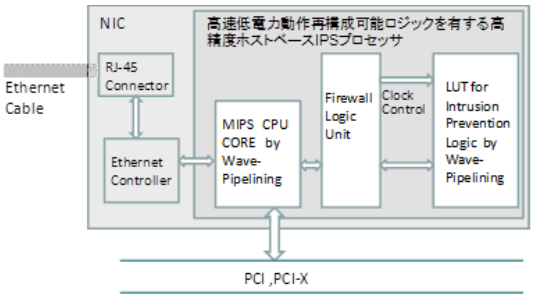

図１　ホストベース IPS プロセッサ

４．研究成果

本研究の成果は，第一にネットワークベース IPS の機能をロジックベースで実現する際に不可欠である，ウェーブパイプライン方式に最適化させたロジックセルの開発を行った。東京大学 VDEC (VLSI Design and Education Center)を通じて提供される 0.18um テクノロジを使用し開発が完了した。また遅延時間の調整手法として，配線方式とロジックセル内部の制御による方式を明らかにした。

図１にここで設計を行ったロジックセル，表１に各ロジックセルの遅延時間，表２に各ロジックセルの面積を示します。表２より遅延調整向けロジックセルの面積は，従来のロジックセルの約 15%の面積で実現可能であることが明らかになりました。

図２のロジックを使用して通常の加算回路，ウェーブパイプライン化加算回路を作成する。図３は，ウェーブパイプライン化加算回路である。白色の部分は図２のロジックセルを２個使用による全加算器です。ウェーブパイプライン化は，通常の全加算器による処理時間と比較して大幅な処理時間の向上

を図ることができます。しかし，図３に示すように多数のロジックセルが必要となります。

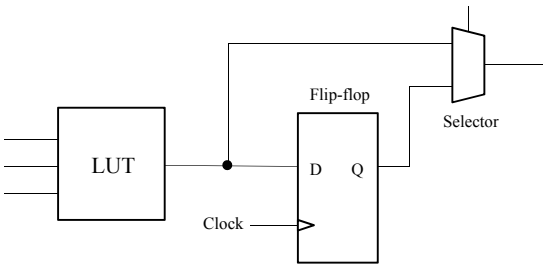

図２　ロジックセル

表１　ロジックセルの遅延時間

ロジックセルの遅延時間	0.84 ns
遅延調整向けロジックセルの遅延時間	0.85 ns

表２　ロジックセルの面積

ロジックセルの面積	997.4 μm^2
遅延調整向けロジックセルの遅延時間	148.5 μm^2

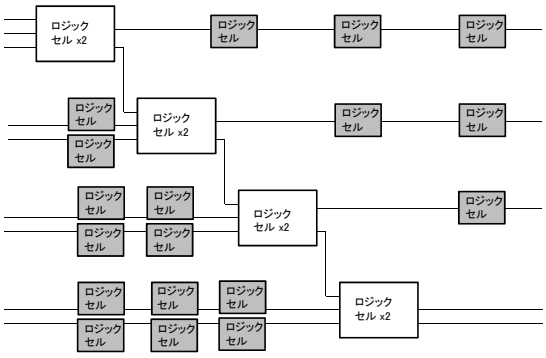

図３　４ビットウェーブパイプライン化加算回路

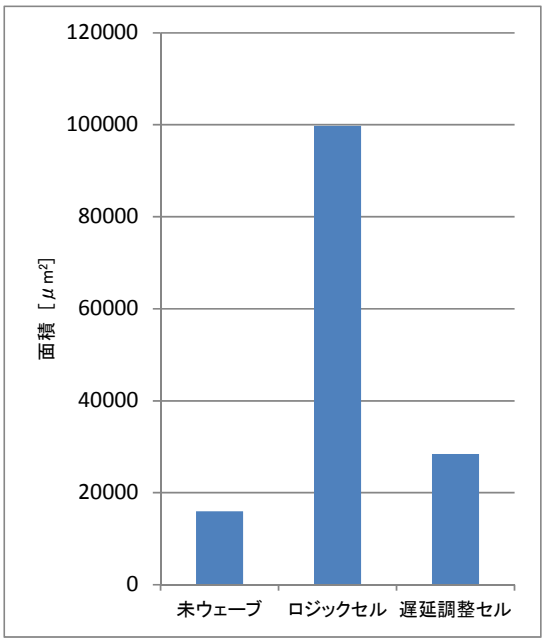

図４　８ビット加算回路の比較

図４は，８ビットの加算回路の面積の比較を行った結果です。ウェーブ化を実施しない８ビットの加算回路に比べてウェーブ化を実施した８ビットの加算回路は約６．２５倍の面積が増加します。そこで本件研究の手法である遅延調整向けロジックセルを使用したところ，約1.78倍の増加で済みました。

第二に消費電力を削減させるためのファイアウォールユニットの開発を行った。ファイアウォールユニットは多数のシフトレジスタを必要とします，本研究ではこのシフトレジスタをウェーブパイプライン手法によって，シフトレジスタを使用せずに実現した。また，ウェーブパイプライン手法の特徴を生かし，多重化に成功した。

第三に実装が必要な通信システムとモバイルプロセッサの調査および必要な回路の開発を行いました。

第四に出張先において，HSPA (High Speed Packet Access)等によるモバイル通信システムの調査を行い，データを収集しました。これらのデータはIPSのシグネチャを開発する際に生かすことができます。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計21件）

① Tomoaki Sato, Phichet Moungnoul and Masa-aki Fukase, "Compatible WEP Algorithm for Improved Cipher

Strength and High-Speed Processing," Proc. of ECTI-CON 2011, pp. 401-404, 2011. 査読有

② Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, Naomichi Mimura, Kazuki Narita, Tatsuya Takaki, and Tomoaki Sato, "Double Cipher Implementation in a Ubiquitous Processor Chip," Proc. of ECTI-CON 2011, pp.125-128, 2011. 査読有

③ Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, and Tomoaki Sato, "Impact of Using a Double Cipher Scheme on the Implementation of a Particular Ubiquitous Processor," Proc. of ISCIT 2010, pp. 821-826, 2010. 査読有

④ Tomoaki Sato, Kei Ito, Keisuke Saito, Phichet Moungnoul and Masa-aki Fukase, "Development of a shift register for Firewall Circuits by Wave-Pipelined Operations," Proc. of 2010 International Workshop on Information Communication Technology, pp. w4c-1-1-w4c-1-4, 2010. 査読有

⑤ Tomoaki Sato, Phichet Moungnoul and Masa-aki Fukase, "Power Control Scheme for H-HIPS in Mobile Communications," Proc. of 2010 International Workshop on Information Communication Technology, pp. s3-3-1-s3-3-4, 2010. 査読有

⑥ Phichet Moungnoul, Anan Sopin and Tomoaki Sato, "Performance of IR-UWB PSM and BPM over S-V Channel Model," Proc. of 2010 International Workshop on Information Communication Technology (ICT2010), pp. W2A-1-1-W2A-1-4, 2010. 査読有

⑦ Masa-aki Fukase and Tomoaki Sato, "H/S Collaborative Development of a Ubiquitous Processor Free from Instruction Scheduling and Pipeline Disturbance," Proc. of 9the IEEE/ACIS International Conference on Computer and Information Science (ICIS 2010) pp. 57-62, 2010. 査読有

⑧ Tomoaki Sato, Phichet Moungnoul, keisuke Saito, Masa-aki Fukase, "Development of a WiMAX Processor by Using a CPLD," Proc. of IMETI2010, Vol. II, pp. 128-133, 2010. 査読有

⑨ Masa-aki Fukase, Atsuko Yokoyama, Takumi Ishihara, Harunobu Uchiumi, and Tomoaki Sato, "Wave Degree versus Dominant Characteristics of a Waved Multifunctional Unit," Proc. of IMETI2010, Vol. II, pp. 164-168, 2010. 査読有

⑩ Tomoaki Sato, Phichet Moungnoul, keisuke Saito, Masa-aki Fukase, "Wave-Pipelined CRC Circuits for Wireless Broadband Systems Based on W-CDMA," Proc. of ICESIT2010, pp. 100.1-100.4, 2010. 査読有

⑪ Natthawut Panitjaroen, Phichet Moungnoul, Tana On-In, Jirasak Chanwutitum and Tomoaki Sato, "Performance Improvement of Satellite Channel with Combine ionosphere scintillation and Small Scale fading using Adaptive Modulation," Proc. of ICESIT2010, pp. 90.1-90.4, 2010. 査読有

⑫ Phichet Moungnoul, Jaroonsak Jarassriwilai, Umaphorn Thongrak, Natthawut Panitjaroen and Tomoaki Sato, "MIMO Adaptive Modulation with Cross-Layer Model of Queuing over Nakagami Fading," Proc. of ICESIT2010, pp. 92.1-92.6, 2010. 査読有

⑬ Phichet Moungnoul Nipun Worawatjirakul Somyot Junnapiya Umaphorn Thongrak Jirasak Chanwutitum and Tomoaki Sato, "TCP Performance Improvement for Wireless Access using Cross-Layer MIMO Adaptive Modulation," Proc. of ICESIT2010, pp. 104.1-104.6, 2010. 査読有

⑭ Masa-aki Fukase, Ryosuke Murakami and Tomoaki Sato, "Design and Chip Implementation of an Instruction Scheduling Free Ubiquitous Processor," Proc. of ASP-DAC, pp.375-376, 2010. 査読有

⑮ Masa-aki Fukase and Tomoaki Sato, "A Ubiquitous Processor Built-in a Waved Multifunctional Unit," ECTI Transactions CIT, Vol. 4, No. 1, pp. 1-7, 2010. 査読有

⑯ Masa-aki Fukase and Tomoaki Sato, "Exploring the Optimum Buffer Size of an Emerging Stream Cipher Engine," ECTI Transactions EEC, Vol. 8, No. 1, pp. 53-58, 2010. 査読有

⑰ Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, “Verifying Firewall Circuits by Wave-Pipelined Operations,” Proc. of IEEE TENCON 2009, pp. WED3.P.14.1 -WED3.P.14.6, 2009. 査読有

⑱ Masa-aki FUKASE and Tomoaki SATO, “Performance Evaluation of an Emerging Stream Cipher Engine,” Proc.

of APSIPA ASC 2009, pp. 583-588, 2009. 査読有

⑲ Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, Yusuke Osumi, and Tomoaki Sato, "Cipher and Media Possibility of a Ubiquitous Processor," Proc. of ISCIT 2009, pp. 343-347, 2009. 査読有

⑳ Masa-aki FUKASE and Tomoaki SATO, "A Waved Multifunctional Unit on Account of Multimedia Mobile Computing," Proc. of WMSCI 2009, Vol. III, pp. 86-91, 2009. 査読有

㉑ Tomoaki SATO, Shuya IMARUOKA, and Masa-aki FUKASE, "Hardware-Based IPS for Embedded Systems," Proc. of WMSCI 2009, Vol. III, pp. 74-79, 2009. 査読有

〔学会発表〕(計 11 件)

① Tomoaki Sato, "Sustainable and Secured Computing Environment for ICT Education,"The 2nd National Conference on Applied Computer Technology and Information Systems (ACTIS 2011), Feb. 17, 2011.

② T. Sato, "Sustainable ICT Education Using a Student's Own PC," International Conference on Educational Research (ICER) 2010, Khon Kaen University, Thailand, Sept., 2010.

６．研究組織

(1)研究代表者

佐藤　友暁（SATO TOMOAKI）

弘前大学・総合情報処理センター・准教授

研究者番号：00336992

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：