2004－ＤＰＳ－117　(35)
2004－CSEC－　24　(35)
2004／3／5

機能と性能を取捨選択可能なIPsecハードウェア実装

山口 和哲*，楯岡 孝道*，阿部 公輝*

重要なデータをネットワーク上で扱うようになり，より統一的なセキュリティを実現するためにIPsecが提案されている．データ通信の目的が異なれば，セキュリティ強度や機能，性能を同じレベルで保つ必要はない．目的に応じたセキュリティ強度や性能は，多様なセキュリティ機能を持つIPsec機能，及び性能とコストのバランスが異なる実装をそれぞれ取捨選択することで得られると考えられる．本論文では，IPsecの機能や性能を取捨選択可能にするための枠組みとその接続部を提案，設計，及び実装を行い，その有用性と有効性に関する評価を行なう．また，各機能ごとにハードウェア実装を行い，その性能評価を行う．さらに，得られた性能とコストからIPsecハードウェア実装を行った際に，その性能の予測が可能であることを示す．

Customizable Hardware Implementation of IPsec With Respect to Its Function and Performance

Kazunori Yamaguchi*, Takamichi Tateoka*, Kôki Abe*

In this paper, we propose a method to customize the IPsec system, enabling to include/exclude each of the IPsec components and to predict the performance and area cost of the resulting entire hardware implementation. The customization is based on a design framework where IPsec functions are modularized and the interfaces between them are well defined. We illustrate the usefulness of our proposal by designing some of the hardware components satisfying the definitions and using them to customize the system for several specific applications. Evaluations of the effectiveness of the customizing in terms of making design tradeoffs among IPsec hardware realizations with respect to the performance and area costs are also given.

1　はじめに

インターネットの普及により，重要なデータをネットワーク上で扱うようになってきた．ネットワーク上で安全な通信を行うための通信経路を統一的に扱えるようにするためのシステムアーキテクチャーとして，IPレベルでセキュリティ機能を実現するIPsec（IP Security）[1]がある．本研究では，このIPsecに着目し，負荷の重いセキュリティ処理を高速化するために，そのハードウェア実装に焦点をおく．

データ通信の目的が異なれば，セキュリティ強度や機能，性能を同じレベルで保つ必要はない．目的に応じたセキュリティ強度は，多様なセキュリティ機能を持つIPsecの機能を取捨選択することで得られ，目的に応じた性能は，性能とコストのバランスが異なる実装を取捨選択することで得られる．

要求されるコストや性能の制約条件のもとで実装を行う場合，ソフトとハードの協調設計という手法も考えられる[2]．そのためには，それぞれの実装における各機能の性能とコストの評価が知られていなければならない．しかし，ソフトウェア実装による各機能の性能評価は行われているが[3]，ハードウェア実装における各機能の性能評価は行われていない．また，IPsec各機能の取捨選択も実現されていない．

本研究では，機能や性能の取捨選択を可能にするためのIPsecの枠組みとその接続部を提案し，設計する．また，各機能ごとにハードウェア実装を行い，性能評価を行う．そして，枠組みに各機能モジュールを組み込むことによってIPsecの実装を行い，その結果を評価する．

2　IPsecの構成

IPsecは，大きく以下の4種類の要素からなる．これらを制御を行うのがSAD（Security Association

* 電気通信大学 情報工学科
Dept.of Computer Science, The University of Electro-Communications

Database）である．

- カプセル化モード（Encapsulation mode:通信方式）
  2 種類のモードが存在する．
  - トランスポートモード
    パケットを生成したホスト自身が，自分のパケットを IPsec 化してネットワークに送り出すモード
  - トンネルモード
    他のホストが投げたパケットを転送する際にまとめて IPsec を適用するモード
- セキュリティプロトコル（Security Protocol）
  AH のみ，ESP のみ，または AH と ESP の両方（SA バンドル）を用いる 3 通りがある．
  - AH（Authentication Header）
    パケット全体に対する認証機能を提供
  - ESP（Encapsulationg Security Payload）
    パケットの暗号化とパケット一部に対する認証機能を提供
- 認証機能（Authentication algorithm）
  HMAC-MD5-96，HMAC-SHA-1-96 など
- 暗号化機能（Encryption algorithm）
  DES，3DES，AES など

この他に，SA の自動生成，及び管理を行うことのできる IKE （Internet Key Exchange）が存在する．

認証アルゴリズムや暗号化アルゴリズムは，IPsec という枠組みの中でさまざまなアルゴリズムを使用することができる．

3 IPsec のカスタマイズ

扱う情報や機器が異なる場合，そのセキュリティ強度や機能，性能は同じレベルで保つ必要はない．要求される性能やコストの制約条件をもとに，利用目的に応じて機能や性能の取捨選択を行うことによりカスタマイズを行うことが有効であると考える．また，コストの削減を行うことも可能である．機能の取捨選択を行うパーツとして大きく以下の４つに分けることができる．

- カプセル化モードの選択
- セキュリティプロトコルの選択
- 認証方式の選択
- 暗号化方式の選択

また各パーツにおいて，同じ機能をもった速度重視，面積重視の実装など利用形態に応じて最適化した実装を用いることが可能である．目的に応じて各パーツから用いる機能を選択し，カスタマイズを行う．鍵管理，及び鍵交換機能を持つ IKE については，利用頻度が少なくハードウェア化コストが非常に高いことが予想されるので，本研究ではソフトウェアで行うと想定し，扱わないこととする．

4 取捨選択可能な IPsec の枠組みとその接続部の提案

本論文では，同じアルゴリズムやモード，及びプロトコルをもったモジュールをそれぞれの機能モジュールと呼ぶ．取捨選択可能な IPsec の実装を行うにあたり，取捨選択を行って選んだ各機能モジュール同士を結びつけるための IPsec の枠組みとその接続部が重要である．本研究では，取捨選択可能な IPsec ハードウェア実装を実現するための IPsec の枠組みとその接続部を提案する．

4.1 取捨選択可能な IPsec の枠組みの設計方針

取捨選択可能な IPsec の枠組みの設計方針を示す．

1. 捨選択可能な機能を特定する．
2. 各機能モジュールを接続するための IPsec の枠組みを設計する．
3. 各機能モジュール同士の接続部の設計を行う．

上記の設計方針をもとに各機能モジュールを個別に作成し，その各機能モジュールの取捨選択を行うことにより，機能や性能，コストの異なる実装の実現を行う．そのためには，取捨選択を行うことのできる機能を特定し，各機能を接続するための IPsec の枠組みを設計することが重要である．また，各機能同士の接続部の設計が重要となる．

4.2 取捨選択可能を実現するための問題点と解決策

取捨選択を可能にするための問題点と解決策を以下にあげる．

IPsec の枠組みにおいて，取捨選択の単位となる各機能の機能モジュールへの分割方法，及び各モジュール間の接続部の設計が問題になる．本実験では，機能モジュール間の配線が複雑にならないことを重視し，第 3 節で提案した取捨選択を行うパーツをもとに，機能を分割した．その際，カプセル化モードの選択，及びセキュリティプロトコルの選択は関係が強いため，複雑になるのを避け単一の機能

モジュールとしてまとめた．また，すべての実装に必要なモジュールとしてSAを管理する機能を独立したモジュールとして設定した．

取捨選択を行うことによって，機能モジュールが複数の機能（アルゴリズム，またはプロトコル）を持つ場合と異なる機能を持つ場合に問題となる．各機能モジュールは，サポート信号を持ち，自己申告を行う設計になっており，さらに，サポートしていないとエラー信号を返す設計になっている．これにより，不適切な機能モジュールを選択した場合でも，誤動作を防ぐことができる．

また，ほかの各機能モジュールから不規則にデータが入力された場合，どの機能モジュールからのデータなのかがわからなくなってしまう．これは，データの入力時にデータに番号を付け，終了したデータの処理番号を参照することにより，どのデータに対する処理結果なのかを識別できる設計になっている．

4.3 機能モジュールへの分割

取捨選択可能なIPsecを実現するために必要な機能モジュールとその際に用いるアルゴリズム，モード，及びプロトコルを以下に示す．

- SAの管理を行う機能モジュール
  （SAの管理を行うことのできる機能）
- 認証値を計算する機能モジュール
  HMAC-MD5-96，HMAC-SHA-1-96など
- 暗号化，及び復号化を行う機能モジュール
  DES，3DES，AESなど
- 送受信を行う機能モジュール
  カプセル化モード，及びセキュリティプロトコル

SAの管理を行う機能は，どのような設計でも必要となる．認証値を計算する機能は，HMAC-MD5-96やHMAC-SHA-1-96などのSAに設定されている認証アルゴリズムを用いて認証値の計算を行う．暗号化と復号化を行う機能は，DESや3DES，AESなどのSAに設定されている暗号化アルゴリズムを用いて暗号化または復号化を行う．送受信を行う機能は，SAに設定されているカプセル化モードとセキュリティプロトコルの組み合わせを用いてデータの送受信を行う．

4.4 取捨選択可能な機能モジュールの特定

SAの管理を行う機能は，どのような仕様の設計でも必ず必要となるので本実装では取捨選択不可能とした．ただし，この機能をソフトウェアで処理するという選択を行うことは可能である．認証値の計算を行うアルゴリズム，暗号化または復号化を行うアルゴリズム，送受信を行うモードとプロトコル（カプセル化モードとセキュリティプロトコル）は，それぞれの設計仕様を満たせばよいので取捨選択可能とした．

4.5 IPsecに用いられる各機能モジュールとその枠組み，及び接続部

IPsecに必要な各機能モジュールを以下に示し，その枠組み，及び接続部を図1に示す．また，これらの各機能モジュールをサブモジュールとしたトップモジュールをIPsec_coverとする．

- SAD_control
  SADの管理を行うモジュール
- Authen_cover
  IPsecに用いる認証機能の管理を行うモジュール
- Encrypt_cover
  IPsecに用いる暗号化機能の管理を行うモジュール
- IPsec_send_receive
  送信データと受信データの制御を行うモジュール

この枠組みを基盤とし，その接続部を実現することにより，異なる機能や性能を持った各機能モジュールを組み込むことで機能と性能，コストの異なる実装を実現することができる．

5 取捨選択可能なIPsecハードウェア実装に関する評価

前節で提案したIPsecの枠組みとその接続部の設計にしたがって，IPsecの各機能モジュールを個別に作成し，取捨選択可能なIPsecの実装と評価を行う．

この実装の回路記述は，verilog-HDLを用いて行い，動作確認のシミュレーションは，CADENCE社のverilog-XL04.10.001-p（VDEC提供）を用いて行った．また，Synopsys社のDesign Compilerの論理合成結果をもとに性能評価を行った．使用したセルライブラリーは，ROHM社の作成した“ROHM035”（VDEC提供）である．

5.1 各機能モジュールの実装と性能評価

本論文ではSAD_controlモジュール，Authen_coverモジュール（HMAC-MD5-96），Encrypt_coverモ

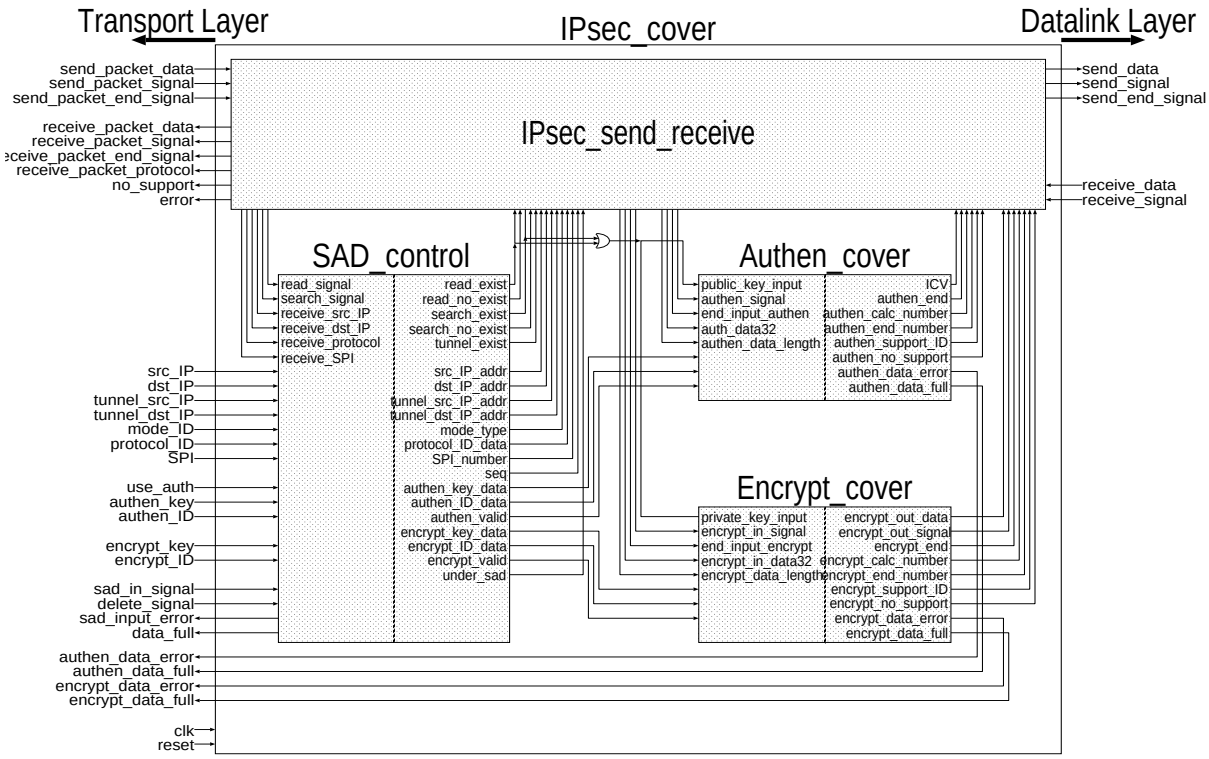

図 1: IPsec_cover の各機能モジュール間の接続部の設計

ジュール（使用アルゴリズムなし）を実装した．また，IPsec_send_receive モジュールには，トランスポートモードの AH，トンネルモードの AH，トランスポートモードとトンネルモード両方を利用できる AH の 3 種類の実装を行った．AH に着目したのは，IPsec をソフトウェアで処理した際に，IPsec を使用しない場合と AH を使用した場合では，約 0.40 倍のスループットになることが知られているからである [3].

本論文で実装した各機能モジュールと前節で提案した IPsec の枠組みでの位置付けと，その性能評価を表 1 に示す．枠組みの位置付けが同じ機能モジュールが取捨選択可能であり，その取捨選択方法により，全体の持つ機能や性能が異なる実装を行うことが可能である．

5.2 提案手法を用いた実装の例と評価

前節で示した提案手法に基づいて実装した 3 つの例を表 2 に示す．セキュリティプロトコルには AH を用い，認証機能には HMAC-MD5-96 を用いた．通信方式にトランスポートモードを用いたものを Example-A とし，トンネルモードを用いたものを Example-B，両方のモードを利用できるものを Example-C とした，また，この例で暗号化機能は利用されないので出力をすべて 0 とする回路を実装した．3 つの実装を比べた際に，通信方式以外の各機能モジュールは同じ機能を持っている．

まず，実装 A を作成する．次に実装 B を作成しようとすると，すでに実装 A が存在するので，実装 B の仕様を満たすためには，通信方式がトンネルモードの送受信機能モジュールを実装すればよい．作成した機能モジュールを実装 A の送受信機能モ

表 1: 実装した各機能モジュールの性能評価

枠組み	実装機能		周波数 (MHz)	面積 (mm^2)	使用する実装		
SA	SA の設定		144	10.35	A	B	C
認証	HMAC-MD5-96		83	13.92	A	B	C
暗号化	Not-used		—	0.00	A	B	C
送受信	trans, AH	送	109	32.65	A		
		受	120	27.95	A		
	tunnel, AH	送	97	38.15		B	
		受	122	28.05		B	
	mode, AH	送	98	38.21			C
		受	123	28.02			C

周波数:クロック周波数，面積:回路面積
trans:トランスポートモード,tunnel:トンネルモード,
mode:両モード選択可

表 2: 設計例

Ex.	SP	通信方式	認証機能	暗号化機能
A	AH	trans	HMAC-MD5-96	Not-used
B	AH	tunnel	HMAC-MD5-96	Not-used
C	AH	mode	HMAC-MD5-96	Not-used

Ex.:Example，SP:セキュリティプロトコル，
trans:トランスポートモード，tunnel:トンネルモード，
mode:両モード選択可

ジュールと交換すれば実装 B を実現することができる．同様の方法で，実装 C も実装できる．それぞれの実装は，シミュレーションよって正しく動くことを確認した．

IPsec ハードウェア実装 Example-A，B，C それぞれの性能を表 3 に示す。論理合成で得られたクロック周波数とデータの処理にかかるクロック数からスループットを算出した．本論文では 8192 バイトのデータを送信した．

表 3: IPsec のハードウェア実装の性能

IPsec 実装	スループット（Mbits/s）		周波数（MHz）	面積（mm^2）
Example-A	(a)	155.17	63	85.49
	(b)	229.72		
Example-B	(a)	174.61	71	89.92
	(b)	258.54		
Example-C	(a)	149.38	60	91.37
	(b)	221.18		

周波数:クロック周波数，面積:回路面積，
(a):IPsec を利用した場合,(b):IPsec を利用しなかった場合

表 3 の Example-A，B，C の回路面積は，表 1 で示したそれぞれに用いられている各機能モジュールの面積の和とほぼ一致している．これより，各機能モジュールの回路面積より取捨選択を行った際の全体の回路面積が予測できることがわかる．同様に，表 3 の Example-A，B，C の周波数は表 1 で示したそれぞれに用いられている各機能モジュールの中で，周波数が一番小さく，ボトルネックと考えられる機能モジュールに依存している．これよりクロック周波数よりボトルネックとなる機能モジュールを推測でき，全体のクロック周波数を予測することが可能である．これより，各機能の性能が即知であれば，実際に実装を行わなくても，取捨選択を行った際の目安となる性能を得ることが可能である．

ハードウェア実装との性能比較を行うために，ソフトウェアで IPsec による通信を行い性能評価を行う．表 4 に用いた機器を示す．

ソフトウェアでの性能の測定は，nttcp[4] を用いて 8192 バイトのデータを送信することにより計測した．性能評価を表 5 に示す．

表 4: ソフトウェア通信実験に用いた機器

	送信に用いた機器	受信に用いた機器
OS	FreeBSD 4.8R	FreeBSD 4.8R
CPU	Pentium 133MHz	K6 400Mhz

表 5: IPsec のソフトウェア実装における性能

利用した IPsec 機能	スループット（Mbits/s）
トランスポートモード，AH	35.26
トンネルモード，AH	36.34
IPsec を使用しない場合	92.27

表 3 と表 5 を比較した結果を以下に示す．トランスポートモードの AH を用いた場合，ハードウェア実装することによって IPsec を利用した場合に約 4.5 倍になり, 利用しなかった場合は，約 2.5 倍になった．同様にトンネルモードの AH を用いた場合，ハードウェア実装することによって IPsec を利用した場合に約 4.8 倍になり，利用しなかった場合は，約 2.8 倍になった．また，両方のカプセル化モードと AH を用いた場合，ハードウェア実装することによって IPsec を利用した場合に約 4.1 倍になり，利用しなかった場合は，約 2.4 倍になった．

5.3 性能の取捨選択

同じ機能を持つ異なる性能の機能モジュールに関する取捨選択を考える．表 6 にその例を示す．これは，仮に認証機能に動作周波数 Freq1，回路面積 Area1 の認証機能 A と，動作周波数 Freq2，回路面積 Area2 の認証機能 B が存在するとした場合に，その 2 つの実装を取捨選択することにより，性能の取捨選択を行う例である．ここで，Freq1 <98 <Freq2, Area1 <Area2 とする．

表 6: 性能の取捨選択の例

枠組み		実装機能		周波数 (MHz)	回路面積 (mm^2)
SA		SA の設定		144	10.33
認証機能	A	HMAC-MD5-96		Freq1	Area1
	B			Freq2	Area2
暗号化機能		Not used		—	0.00
送受信		trans,	送	98	38.21
		tunnel，AH	受	123	28.02

Freq1 <98 <Freq2，Area1 <Area2
周波数:クロック周波数，
trans:トランスポートモード，tunnel:トンネルモード

表 6 より認証機能 A を用いて実装を行った場合，ボトルネックは認証機能部の Freq1(MHz) になり，

回路面積は 76.56+Area1 になることがわかる．同様に B を用いた場合，ボトルネックは送受信部の 98(MHz) になり，回路面積は 76.56+Area2 になることがわかる．これより，A は面積重視の実装になり，B は速度重視の実装になるので，例えば，A はリモートコントロールを受ける情報家電への通信などに有効であり，B は監視カメラなどの通信に有効であると考えられる．以上より，性能の異なる機能モジュールを用いることで，同じ機能を持つ異なる性能の実装を行うことが可能である．

なお，この性能の取捨選択に関する初期的結果は文献 [5] に述べられている．

6 考察

前節で述べた評価結果より，IPsec の枠組みとその接続部の設計を用い，機能と性能を取捨選択可能にすることの利点は，以下の通りと考えられる．

- すでに存在する各機能モジュールを用いることにより，新しく作成しなくても異なる機能，及び性能を持った実装を行うことができる．
- 性能の異なる機能モジュールを組み込むことにより，全体として同一機能を持つ，異なる性能の実装を行うことができる．
- 新しいアルゴリズムへの対応が容易に行うことができる．
- 各機能モジュールの性能から，取捨選択を行った実装の性能を推測することができる．
- 実装にかかる作業の削減ができる．

欠点としては，機能モジュールにまたがって最適化が行えないことと，現状では，ソフトととの協調設計が行えていないことがあげられる．

本論文における実装では，取捨選択可能な IPsec 実装の動作実現を第一目的としたため，各機能モジュールにおいて，十分な最適化を行ったとは言えない．さらに最適化することで性能の向上が可能であると推測する．

今回行った実装にバッファの役目を行うために用いた FIFO が全体の約 67%であった．これにより，FIFO の最適化を行うことで回路面積の削減が可能であると考える．

ソフトとハードの協調設計を考えるにあたって，それぞれの実装は，同一のテクノロジーで実現されることになる．本実験の性能比較は同一のテクノロジーを用いて行っていないのであくまで参考値である．

7 おわりに

本研究では，機能や性能の取捨選択可能な IPsec の枠組みとその接続部の提案，各機能ごとのハードウェア実装及びその性能評価を行い，提案手法の有効性を示すために，手法に基づいた IPsec の実装とその動作確認及び性能評価を行った．また，異なる機能の取捨選択が可能であることを示すために，異なる機能モジュールを IPsec の枠組みに組み込み動作確認及び性能評価を行った．以上より，異なる機能や性能を持つ機能モジュールの取捨選択を行うことにより，利用目的に応じた IPsec ハードウェアを容易に実装できることを示した．

今後ソフトウェアとハードウェアの協調設計を考えるにあたっては，今回ハードウェア実装を行っていない機能モジュールに関する性能評価を行うことが必要である．また，ソフトとハードの接続部を確立すれば，ソフトとハードの取捨選択も容易に実現できると考える．さらに，ソフトウェア実装とハードウェア実装の機能モジュールが充実し，それらの性能評価が示されれば，要求さるコストや性能の制約条件のもとで，IPsec のよりよい実装を実現することが可能であると考える．

参考文献

[1] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Nov. 1998.

[2] 佐藤伸広，ダハナヤカゲ・ディネーシュ，清水雅一，楯岡孝道，阿部公輝, “インターネットプロトコルスタックのハードウェア/ソフトウェア協調設計”, 電子情報通信学会 2004 年総合大会講演論文集，Mar. 2004. 掲載予定

[3] 有賀征爾，南政樹，江崎浩, “IP Security ソフトウェア処理の性能評価”，インターネットコンファレンス’99 論文集, pp.61-66，Dec，1999.

[4] E. Bartel, “New TTCP program”, `http://www.leo.org/~elmar/nttcp/`,

[5] 山口和哲，楯岡孝道，阿部公輝, “機能と性能を取捨選択可能な IPsec ハードウェア実装の検討”, インターネットコンファレンス 2003 論文集，p.119，Oct. 2003.