社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（36）
2005－CSEC－28（36）
2005／3／23

実用暗号通信 PCCOM の実装と評価

増田 真也† 渡邊 晃†
†名城大学大学院理工学研究科

ネットワークセキュリティ技術の重要度が高まっているが，導入するシステムは既存の環境に影響を与えないようなものであることが望まれる．我々はこれまでに，オリジナルパケットのフォーマットを変えないまま，本人性確認（正当な相手であることの保証）とパケットの完全性保証（パケットが改竄されていないことの保証）を行うことができる暗号通信プロトコル PCCOM（Practical Cipher COMmunication）を提案し，検討を行ってきた．PCCOM は既存の環境にほとんど影響を与えず，NA(P)T やファイアウォールとの共存が可能である．本稿では PCCOM の実装を行ったので報告する．PCCOM の機能検証の結果およびスループットの測定結果を述べる．

Implementation and Evaluation of Practical Cipher Communication

Shinya MASUDA† and Akira WATANABE†
†Postgraduate Course in Science and Technology, Meijo University

Network security technologies have become a major concern, and it is desired that the system is compatible with the conventional systems. We have proposed the cipher communication protocol, called *PCCOM (Practical Cipher COMmunication)*, giving no influences to existing systems. It can authenticate both terminals, and guarantee the integrity of packets, not changing the packet format. In this paper, we describe the implementation of PCCOM. The evaluation results show that PCCOM has enough flexibility and throughput in the practical use.

1. はじめに

ネットワークにおけるセキュリティ上の脅威は年々深刻な問題となっており，セキュリティ技術の重要性が高まっている．その中でも，IP 層でパケットの暗号化などを行うことによりネットワーク自体のセキュリティを確保するネットワークセキュリティ技術は，利用するアプリケーションを意識することなく安全を確保できることから，ネットワークの根本的なセキュリティ対策として有効な手段とされている．しかし実際には，Gateway-to-Gateway の安全を確保する手段は確立されているものの，End-to-End や Host-to-Gateway で通信間に NA(P)T やファイアウォールを挟むような環境では使用条件に制約があり，普及が進んでいないのが現状である．このことから，既存システムや新たな技術の出現に柔軟に対応できる技術が求められている．しかし，セキュリティ強度と柔軟性・利便性といった実用度は相反する要素であり，ひとつの技術であらゆる要求に対応するのは困難である．従って今後のセキュリティ技術は，セキュリティ強度と実用度を想定する利用形態に応じて幾つかのレベルに分け，それぞれに適した方式を検討することが重要になると考えられる．

既存のネットワークセキュリティ技術の代表として IPsec が挙げられる[1)~4)]．IPsec の中でも暗号通信方式について規定しているのが ESP で，盗聴を防止する暗号化の他に，なりすましを防止する本人性確認（正当な相手であることの保証）や改竄を防止するパケットの完全性保証（パケットが改竄されていないことの保証）などの機能を提供している．ESP にはトランスポートモードとトンネルモードがあり，前者は End-to-End の IPsec 通信を適用する際に利用し，後者は主に Gateway-to-Gateway や Host-to-Gateway の IPsec 通信を適用する際に利用する．しかし現実の適用例を見ると，インターネット VPN（Virtual Private Network）の構築手段として Gateway-to-Gateway でトンネルモードを用いる場合以外にはあまり普及していないのが現状である．これは，パケットの暗号化や完全性保証がもたらす NA(P)T やファイアウォールとの相性の悪さに起因していると考えられる．NA(P)T との相性の悪さを解決するための一方法として，UDP ヘッダで ESP をカプセル化する“UDP Encapsulation of IPsec Packets”が RFC と

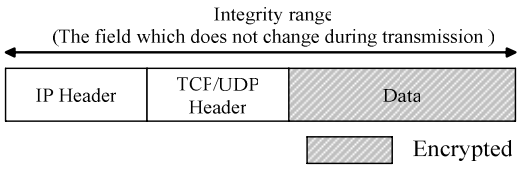


図 1　PCCOM のパケットフォーマット

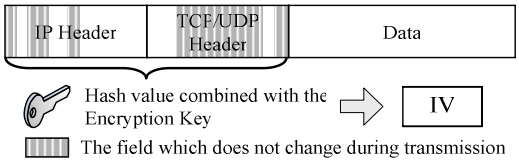


図 2　IV (Initialization Vector) の生成

して公開されており，有効な手段として普及しつつあるが [5]，カプセル部分は完全性保証の範囲に含まれていない，ヘッダなどの追加によってオーバヘッドやフラグメントが発生する，上位層プロトコルの情報を見るルータなどはヘッダの追加や暗号化されていることなどによって正しく処理できない場合があるなどの課題が残されている．

我々はこれまでに，必要最低限のセキュリティを備えつつ，NA(P)T やファイアウォールなどの既存システムに影響えないこと，高スループットを実現できること，などの実用面に重点を置いた暗号通信プロトコル PCCOM（Practical Cipher COMmunication）[6]を提案し，検討を行ってきた．PCCOM は主に，多様な利用形態への対応が求められる一般ユーザ端末で利用することを想定している．本稿では，PCCOM の実装について述べ，PCCOM がパケットフォーマットを変えずに処理する方式であることが，実装の容易さをもたらし，性能的にも有利であることを説明する．また，性能測定を行いスループットの面で IPsec ESP よりも有利であることを示す．

以下，2 章で PCCOM の機能と原理，3 章で PCCOM の実装，4 章で評価，5 章でまとめと今後の課題について述べる．

2. PCCOM

PCCOM が提供する機能は，暗号化による機密性確保と本人性確認・完全性保証で，NA(P)T やファイアウォールなどの既存システムに影響を与えない，パケットフォーマットを変えないため高スループットを実現できるなどの特徴がある．本章ではその実現方式を記述する．

2.1. 暗号化範囲

PCCOM のパケットフォーマットを図 1 に示す．PCCOM では，ユーザデータ部分のみを暗号化の対象とする．NA(P)T やファイアウォール，上位層プロトコルの情報を見るルータなどに影響を与えないよう，TCP/UDP ヘッダはあえて平文のままとする．しかし，PCCOM では次節で述べる本人性確認とパケットの完全性保証のための工夫が施されているため，改竄や偽造による通信の割り込みや遮断を試みる不正なパケットを廃棄することが可能であり，安全性低下の問題は少ない．むしろ，ファイアウォールが当該ヘッダの内容を用いたフィルタリングを行うことが可能になり，実用面でのメリットが大きい．また，PCCOM ではパケット長を変えずに暗号化するために，任意長のデータを暗号化できるブロック暗号の CFB モードを採用する．よって，IPsec などに見られるように暗号化によってフラグメントが発生することはない．

2.2. 本人性確認・完全性保証

PCCOM では，暗号鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，TCP/UDP チェックサムに独自の計算を施すことで，本人性確認とパケットの完全性保証を行う．以下にその原理を示す．

暗号化/復号の際は，暗号鍵とは別に IV（Initialization Vector）と呼ばれる初期値を与える必要がある．IV は暗号化/復号時に同じ値であり，かつ使用する度に異なる値である必要がある．また，第三者には分からない値を用いることが望ましい．図 2 は本提案における IV の生成方法である．PCCOM では，IP ヘッダ，TCP/UDP ヘッダで転送中に値の変化しないフィールド（IP アドレス，ポート番号，TCP/UDP チェックサムは除く）と，事前に秘密裏に共有している暗号鍵を含めた値からハッシュ値を求め，これを IV とする．IV の種として暗号鍵を含めているため，第三者に IV が知られることはない．この IV は，以下のように本人性確認とパケットの完全性保証を実現するためのキーデータとなる．

一般の通信では TCP/UDP チェックサムは，

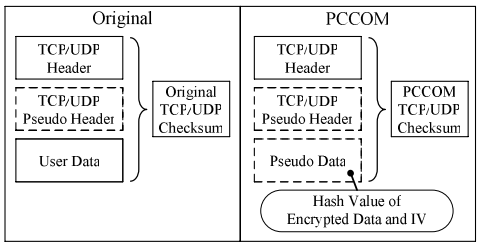


図 3　チェックサムの計算範囲

TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，ユーザデータから計算されるが，PCCOM では IV をチェックサムの計算に含めて再計算する．オリジナルデータと PCCOM の，TCP/UDP チェックサムの計算範囲の違いを図 3 に示す．図中の点線はチェックサム計算時に疑似的に作成するヘッダ，データを指す．図 3 において疑似データ（Pseudo Data）とは，暗号化データと IV を元に求めたハッシュ値のことで，この値を含めて TCP/UDP チェックサムの再計算を行う．

完全性保証の流れを以下に述べる．送信側ではデータの暗号化後，上記疑似データを用いて TCP/UDP チェックサムの再計算を行う．受信側ではデータの復号を行う前に，同様の方法で生成した疑似データを用いて TCP/UDP チェックサムを検証する．検証結果が正常であれば，復号を行いオリジナルパケットに対応するチェックサムの再計算を行って上位層（TCP/UDP）に渡す．この方式により，暗号化データと IV 生成に用いたフィールドの完全性を保証することができると同時に，本人性確認も実現される．パケットの改竄者が改竄を隠蔽するために TCP/UDP チェックサムを再計算しようとしても，疑似データの内容が分からないので，正しい計算を行うことはできない．

この方式によると，通信径路上に NA(P)T が介在して IP アドレス，ポート番号，チェックサムが書き換えられたとしても，完全性保証，本人性確認の考え方は維持される．すなわち，NA(P)T は IP アドレスとポート番号の変換時に，チェックサムの書き換えも行うが，NA(P)T におけるチェックサムの書き換えは変換部分の差分を計算するだけであるため [7]，受信側で行うチェックサムの検証には影響を与えない．IP アドレスとポート番号の保証は次節で述べる考え方で実現できる．

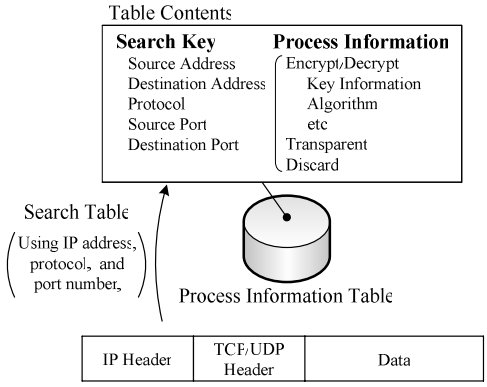


図 4　テーブル検索処理

2.3. IP アドレス・ポート番号の保証

上記のように，IP アドレスとポート番号は IV 生成の範囲に含めていないが，これらの部分の完全性は，パケットの処理内容を記述した動作処理情報テーブルの検索過程で保証することができる．テーブル検索の処理を図 4 に示す．動作処理情報テーブルには，送信元と宛先の IP アドレスとポート番号，およびプロトコル番号の情報とそれに対応する暗号化/復号，透過中継，廃棄などのパケットの処理内容，暗号化/復号に用いる鍵情報やアルゴリズムなどが記述されている．一方，このテーブルは受信パケットの IP アドレス，プロトコル番号，ポート番号を元に検索される．従ってテーブル検索後，テーブルの内容から IP アドレス，プロトコル番号，ポート番号を再度確認し，テーブル内に該当パケットの情報が正しく存在したら，IP アドレスとポート番号は改竄されていなかったことが保証される．但し，この方式では事前に正しい内容のテーブルが生成されていることが前提となる．ここで正しいテーブルの生成を保証する方式としては，IKE（Internet Key Exchange）[4]や DPRP（Dynamic Process Resolution Protocol）[8),9)]などを流用する方式が考えられる．

3. PCCOM の実装

PCCOM の試作システムを開発し，動作検証を行った．本章では試作システムの実装方式，仕様・構成と動作概要について記述する．

3.1. 実装方式

試作システムは，IP 層の詳細な処理フローに関する情報が多い FreeBSD（5.1 Release）のカ

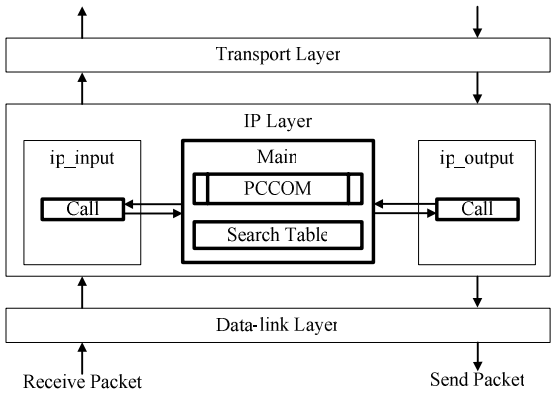


図 5　試作システムの実装方式

表 1　試作システムの仕様

項　　目	内　　容
テーブル検索方式	ハッシュ法
暗号アルゴリズム	AES（CFB モード）
鍵長	128 ビット
ハッシュ関数	MD5

ーネル内に実装した．試作システムの実装方式を図 5 に示す．IP 層で行われる既存の処理に一切の変更を加えず，カーネル空間の関数である ip_input()，ip_output()でメインモジュールに処理を渡し，処理を終えたら差し戻す．PCCOM はパケットフォーマットを変えずに処理する方式であるため，この様な方式を容易に実現できる．IPsec などではヘッダの追加などパケットフォーマットに変更があるため，IP 層全体に渡って処理の変更が必要となる．このため，PCCOM は高スループットの暗号通信を実現できるという利点がある．

3.2. 試作システムの概要

試作システムの仕様を表 1 に示す．動作処理情報テーブルはハッシュテーブルとして実装する．暗号アルゴリズムは AES（鍵長は 128 ビット）を採用し，ハッシュ関数は，AES で用いる IV が 128 ビットであることから，出力値が 128 ビットとなる MD5 を用いた．尚，暗号ライブラリとして OpenSSL（openssl-0.9.7d）を採用した．

試作システムは，メインモジュールとそのサブモジュールである PCCOM モジュール，PCCOM のサブモジュールである IV 生成モジュール，暗号化/復号モジュール，疑似データ生成モジュール，チェックサム再計算モジュール，チェックサム検証モジュールから構成される．メインモジュールに渡されたパケットは，RIP や DHCP のようなルーティング・IP アドレス設定に関わるパケットでないことを判別後，予め用意した動作処理情報テーブルに基づき処理を実行する．動作処理情報テーブルには IP アドレス，プロトコル番号，ポート番号と，それに対応する暗号化/復号，透過中継，廃棄などの動作内容が記されている．テーブル検索キーである IP アドレス，プロトコル番号，ポート番号から算出したハッシュ値でレコードを検索し，レコードに記された動作内容に応じて対応する処理を行う．

試作システムを用いて，パケットフィルタリングタイプのファイアウォールおよび NA(P)T を中継して通信できることを確認し，フィールドの内容を書き換えた場合，不正パケットとして検出できることを確認した．

表 2　IPsec ESP との比較．

	機密性	本人性確認	完全性保証	NA(P)T	FW	Fragment
IPsec ESP	◎	◎	◎	△	△	×
PCCOM	○	○	○	○	○	○

4. 評　価

4.1. IPsec ESP とのすみわけ

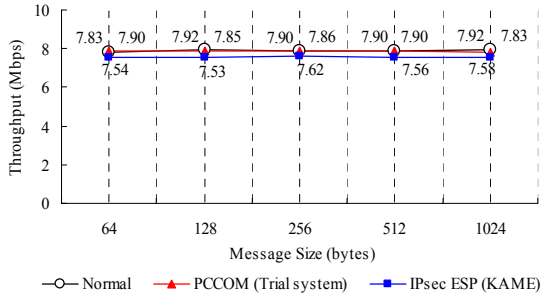
IPsec ESP と PCCOM を 6 項目において定性的に比較した結果を表 2 に示す．

IPsec ESP は，高い機密性と強力な認証機能を提供しているが，TCP/UDP ヘッダの暗号化や完全性保証が原因で NA(P)T やファイアウォールと相性が悪い．“UDP Encapsulation of IPsec Packets ”によって NA(P)T を通過させる手法があるが，カプセル部分は完全性保証の範囲に含まれず，オーバヘッドが増してしまう．また，ヘッダの追加によるオーバヘッドやフラグメントが発生する．

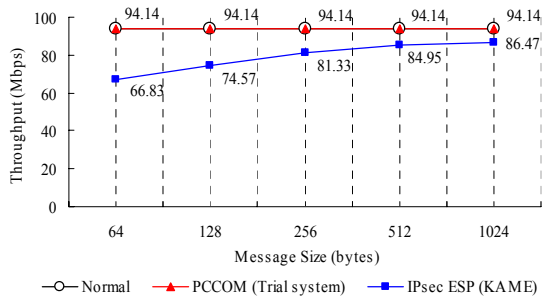
PCCOM は，ユーザデータ部分のみを暗号化の対象とし，本人性確認・完全性保証の実現により TCP/UDP ヘッダが平文であることによる安全性低下を防止しており，むしろファイアウォールのパケットフィルタリングによって，管理者が許可した用途のパケットのみを通過させることができるという利点がある．また，

表 3　実験端末の仕様

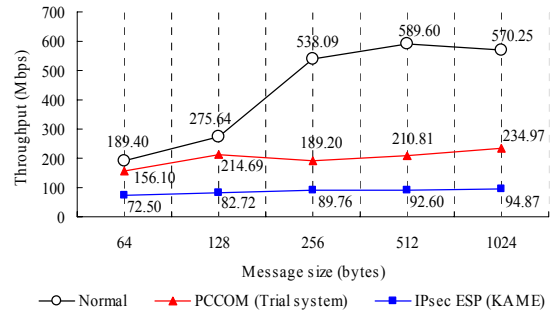
Items	Contents
CPU	Pentium4 2.4GHz
Memory	256MB
NIC	100BASE-TX, 1000BASE-TX
OS	FreeBSD (5.1 Release)



(a) 10BASE environment



(b) 100BASE environment



(c) 1000BASE environment

図 6　スループット測定結果

NA(P)T の通過が可能であり，PCCOM の処理によるフラグメントは発生しない．

IPsec を導入する場合は，強靭なセキュリティを必要とする部門が適しており，NA(P)T やファイアウォールとの相性問題をはじめとした課題に注意しながら導入を検討することが重要である．それに対し PCCOM は，既存システムに影響を与えない，最低限のセキュリティ機能を備えている，高スループットを実現できるなどの点で，実用性が高く企業ネットワークなどに比較的容易に導入できると考えられる．

4.2. 試作システムの性能評価

試作システムと IPsec（KAME）を実装した 2 台の端末間の通信性能を測定した．また，PCCOM 内部の処理時間をモジュール別に測定し，処理のネックとなっている部分を明らかにした．実験に用いた端末の仕様を表 3 に示す．IPsec の設定は，試作システムの仕様と条件が同じになるように，ESP トランスポートモードで，暗号アルゴリズムは AES(鍵長は 128 ビット)，認証アルゴリズムは HMAC-MD5 とし，リプレイ防御機能は OFF とした．

4.2.1. 通信性能の測定

図 6(a),(b),(c)はメッセージサイズ（IP データグラム長）とスループットの関係を，10BASE，100BASE，1000BASE の通信環境ごとに，暗号化をしない場合（以下，Normal），PCCOM および IPsec ESP において比較したものである．スループットの測定にはネットワークベンチマークソフト Netperf[10]を用いた．測定結果は 10 回試行の平均値である．

10BASE の環境では，ESP においては若干の性能低下が見られたものの，処理すべきパケット数が少ないため，PCCOM，ESP の処理オーバヘッドはネックとなっていない．100BASE の環境では，Normal と PCCOM は NIC の上限性能を発揮しており PCCOM に性能低下は見られなかった．それに対し ESP は長パケットでは Normal から約 9.7%性能が低下しており，短パケットでは約 28.5%低下している．また 1000BASE の環境では，長パケットの場合 PCCOM は Normal から約 17.6%性能が低下しており，ESP では約 61.5%低下している．短パケットの場合 PCCOM は Normal から約 58.8%性能が低下しており，ESP では約 83.4%低下している．

短パケットになるほどスループットが落ち込むのは，相対的に処理すべきパケット数が多くなるので，ソフトウェアによるオーバヘッドの占める割合が大きくなるためと考えられる．とりわけ ESP の短パケットでは，ヘッダの追加など暗号化以外の処理ネックが顕著に現れているといえる．

次に，1000BASE の環境において，FTP で 500MB のファイルをダウンロードするのに要

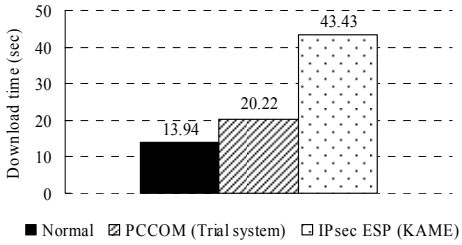


図 7　500MB ファイルの FTP ダウンロード時間

表 4　各モジュールの処理時間とその比率

	モジュール	処理時間（μs）	比率（%）
送信側	IV 生成	0.868	3
	暗号化	26.043	90
	疑似データ生成	1.704	6
	チェックサム再計算（独自）	0.294	1
受信側	IV 生成	0.890	3
	疑似データ生成	2.863	9
	チェックサム検証（独自）	0.281	1
	復号	25.547	83
	チェックサム再計算(通常)	1.286	4

した時間を図 7 に示す. 測定結果は 10 回試行の平均値である．PCCOM は Normal の約 145.1%の時間であるのに対し，ESP は約 311.6%の時間を要している．

4.2.2. PCCOM 内部の処理コスト

PCCOM における処理過程での処理コストを調べるために PCCOM の内部処理時間をモジュール別に測定した．内部処理時間は，RDTSC（ReaD Time Stamp Counter）を用いて処理前後の CPU クロックカウンタ値を求め, 両者の差から算出した．

各モジュールの処理時間とその比率を表 4 に示す．測定結果は FTP の通信中に流れた 1500 バイトの IP パケット 10 個の結果の平均値である．表 4 より，送信側，受信側ともに暗号化/復号が処理の大部分を占めていることが分かる．パケットフォーマットを変えないため，それ以外の処理のオーバヘッドは小さい．試作システムでは暗号化/復号の処理をソフトウェアで処理しているが，専用のハードウェア暗号エンジンを用いるなどで，処理時間の大幅な短縮が期待できる．ESP では，ヘッダオーバヘッドなどの暗号化/復号以外の処理の割合が大きいため，ハードウェア暗号エンジンを用いた PCCOM 程の効果は得られないと考えられる．

5. ま と め

実用性を重視した暗号通信プロトコル PCCOM の実装について述べ，評価を行った．

評価の結果, PCCOM は NA(P)T やファイアウォールとの相性といった柔軟性や，スループットの面で有効であることを確認した．また，PCCOM 内部の処理時間をモジュール別に測定し, 処理の大部分が暗号化/復号であることを示した．

今後は，リプレイ攻撃への対策について検討する. PCCOM は IPv4 と IPv6 で原理的な相違はないが，IPv6 の場合についても検討していく予定である．

謝 辞

本研究は（財）栢森情報科学振興財団の助成を受けて実施したものである．

参 考 文 献

1) S. Kent and R. Atkinson “Security Architecture for the Internet Protocol”, RFC2401, Aug. 1998.
2) R. Atkinson, “IP Authentication Header” RFC2402, Dec. 1998.
3) R. Atkinson, “IP Encapsulation Security Payload (ESP)”, RFC2406, Dec. 1998.
4) D. Harkins and D. Carrel, “The internet key exchange (IKE)”, RFC2409, Dec. 1998.
5) A. Huttunen, B. Swander, V. Volpe, L. Diburro, and M. Stenberg, “UDP Encapsulation of IPsec Packets”, RFC3948, Jan. 2005.
6) 増田真也，渡邊晃，“実用性を重視した暗号通信方式の提案”，情処研法，2004-CSEC-26, pp.267-274, Jul. 2004.
7) K. Egevang and P. Francis, “The IP Network Address Translator (NAT)”, RFC1631 May. 1994”.
8) 渡邊 晃，井手口 哲夫，笹瀬 巌，“イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案”, 信学論(D-I), vol.J84-D-I, no.3, pp.269-284, Mar 2001.
9) 鈴木秀和，渡邊晃，“フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の仕組み”, 情処研法，2004-CSEC-26, pp.259-266, Jul. 2004.
10) Netperf, http://www.netperf.org/