NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装

増田真也[†] 鈴木秀和[†]
岡崎直宣[††] 渡邊晃[†]

ネットワークにおけるセキュリティ上の脅威が問題となっており，通信パケットの暗号化技術が重要な技術として認識されている．既存の暗号化通信技術として IPsec ESP があげられるが，セキュリティは強靭なものの，NAT やファイアウォールを挟むような環境では使用できない，スループットが低下する，などの課題があり，拠点間通信などの一部でしか利用されていない．そこで本論文では，NAT やファイアウォールと共存でき，かつ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）を実現する暗号通信方式 PCCOM（Practical Cipher COMmunication）を提案する．PCCOM の有効性を確認するために試作システムを FreeBSD 上に実装し，NAT やファイアウォールとの親和性が高いことを確認した．また，スループットを測定した結果，パケットフォーマットを変えないことによる性能上の効果があることを確認した．

Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls

Shinya Masuda,[†] Hidekazu Suzuki,[†] Naonobu Okazaki[††] and Akira Watanabe[†]

Threats to network security have become a serious problem, and encryption technologies for communications are an important issue these days. Although the security of IPsec ESP (a typical existing cipher communication technology) is strong, it has such problems that it can not be used in the environment where it coexists with NAT and firewalls, and that there also causes some degradation of throughput. For such reasons, ESP is used only for some limited applications such as VPN (Virtual Private Network). In this paper, we propose a new cipher communication protocol, called PCCOM (Practical Cipher COMmunication), that can verify the identity of the corresponding counterpart and assure the integrity of packets in the environment where it coexists with NAT and firewalls, without changing the format of the original packets. To confirm the effectiveness of PCCOM, we installed a trial system in FreeBSD, and confirmed the coexistibility with NAT and firewalls. We also measured its throughput, and good performance was confirmed owing to "no change" of the packet format.

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，IPsec ESP [1)~4)] のように 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期待されている．しかし実際には IPsec ESP は，NAT/NAPT（以後 NAT と総称する）やファイアウォールを挟むような環境では使用することができず，普及が進んでいないのが現状である．このことから，ファイアウォールや NAT との共存が可能な暗号化通信は有効な技術と考えられる．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，1 つの技術であらゆる要求に対応するのは困難である．したが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，それぞれに適

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†† 宮崎大学工学部情報システム工学科
Faculty of Computer Science and Systems Engineering, University of Miyazaki

した方式を検討することが重要になると考えられる．

IPsec ESP は，盗聴を防止する暗号化のほかに，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．また，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例を除くとあまり普及していない．これは，パケットの暗号化や完全性保証がもたらす NAT やファイアウォールとの相性の悪さに起因している．これらの課題を解決するために，UDP ヘッダでさらに ESP パケットをカプセル化して NAT を通過させる方法（UDP Encapsulation of IPsec Packets）[5] が提案されているが，カプセルヘッダの部分は完全性保証の範囲に含めることはできず，ヘッダの追加によるオーバヘッドの増加やフラグメントの発生などの課題が発生する．また，ESP の暗号化を階層化し，TCP/UDP ヘッダの内容をルータやファイアウォールが参照できるようにする ML-IPsec（Multi-Layer IPsec）[6] が提案されているが，この方法では既存のシステムを変更する必要がある．

一方，文献 7) ではパケットフォーマットを変えないまま特定の範囲を暗号化する方式が提案されている（以下，置換方式と呼ぶ）．置換方式は，ポート番号を平文のままとするため，ファイアウォールの通過が可能であり，パケットフォーマットを変えないためヘッダオーバヘッドやフラグメントが発生せず高スループットを実現できるという利点がある．しかし，置換方式では TCP/UDP チェックサム[8)~10)] を暗号化範囲に含めているため，NAT によるチェックサムの書き換えに対応できず，NAT を通過することができない．また単に平文と暗号文を置き換えるだけのため，本人性確認とパケットの完全性保証を実現していない．

本論文では置換方式の利点に着目し，置換方式を改良することによって，NAT とも共存でき，かつ本人性確認とパケットの完全性保証も確実に行える暗号通信方式 PCCOM（Practical Cipher COMmunication）を提案する．PCCOM は本人性確認とパケット全体の完全性保証を，共通秘密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 チェックサムを新たに再計算することにより実現する．この方法によると NAT やファイアウォールと共存することが可能で，かつパケットフォーマットを変えないためヘッダオーバヘッドやフラグメントが発生せず高スループットを実現できる．なお，PCCOM は事前に送信側と受信側で共通秘密鍵を共有していること，パケットの処理内容を記述した動作処理情報テーブルをすでに保持していることを前提としている．

PCCOM の有効性を確認するために試作システムを開発した．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について述べる．評価の結果，高スループットを実現できることを確認した．また，PCCOM の安全性評価を行い，IPsec ESP とのすみわけについて考察した．

本論文の構成は以下のとおりである．2 章で既存技術とその制約について説明した後，3 章で実用暗号通信 PCCOM を提案する．4 章では PCCOM の実装について説明し，5 章では実装したシステムを用いた PCCOM の性能評価を行い，PCCOM の安全性評価と，IPsec ESP とのすみわけについて述べる．最後に 6 章でまとめる．

2. 既存技術とその制約

IPsec ESP のトランスポートモードとトンネルモードのパケットフォーマットを**図 1** に示す．

トランスポートモードでは，IP ヘッダとそのペイロードの間に ESP ヘッダを挿入し，元の IP パケットのペイロード部分を暗号化する．トンネルモードでは，セキュリティゲートウェイのアドレスを含む新しい IP ヘッダでカプセル化し，カプセル内のデータすなわち元の IP パケットを暗号化する．ESP トレーラは，ブロック暗号のブロック長の整数倍に暗号化するデータの長さを揃えるために用いる．また，ESP ヘッダから ESP トレーラまでの完全性を保証する認証値 ICV（Integrity Check Value）を計算し，ESP 認証値（ESP Auth）としてパケットの末尾に付加する．いずれのモードにおいても TCP/UDP のポート番号が暗号化範囲に含まれているため，そのパケットがどのような用途に用いられるかがファイアウォールで判別できない．その結果，ファイアウォールではすべての IPsec の通過を禁止してしまう場合が多い．また，TCP/UDP チェックサムフィールドが暗号化範囲・完全性保証の範囲に含まれているため，IP アドレスの変換をともなう NAT を通過すると偽造パケットと見なされ，IPsec 処理によってパケットが廃棄される．これは TCP/IP が綺麗な階層構造になっておら

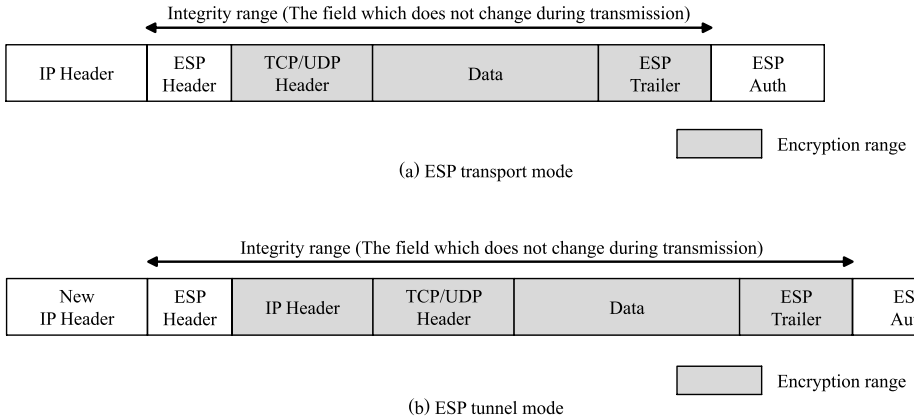


図 1 IPsec ESP のパケットフォーマット
Fig. 1 Packet format of IPsec ESP.

ず，TCP/UDP チェックサムでありながら IP アドレスもチェックサムの演算範囲に含んでいることが根本的な理由である．トンネルモードにおいては，IP アドレスのみを変換する純粋の NAT を通過することは可能であるが，ポート番号の変換もともなう NAPT（IP マスカレード）は通過できない．このような状況に対処するために，市販のルータにおいて，UDP ポート 500 番のエントリを持っているノードに対して ESP パケットを転送することで NAT を通過させているものがある（IPsec パススルーと呼ぶ）が，この方法では 1 つのノードだけしか ESP の通信は機能しない．一方 IETF では，UDP ヘッダでさらに ESP をカプセル化して NAT を通過させる方法（UDP Encapsulation of IPsec Packets）が提案されているが，カプセル部分は完全性保証の範囲に含むことはできず，ヘッダの追加によるオーバヘッドの増加やフラグメントの発生などの課題が発生する．

以上のことから，IPsec をシステムに導入するには既存設備との相性やスループットの低下を考慮する必要がある．

図 2 に，PCCOM のベースとなっている置換方式のパケットフォーマットを示す．暗号化後のパケットフォーマットはオリジナルフォーマットから変化させず，平文と暗号文をそのまま置き換える．ファイアウォールがポート番号を識別できるように，また TCP/UDP チェックサムから暗号文の内容が推測されるのを防ぐために，暗号化範囲を TCP/UDP ヘッダのチェックサムフィールド以降のすべての部分としている．TCP/UDP ポート番号が平文であるため，ファイアウォールによるフィルタリングが有効になるうえ，パケット長が変わらないためスループットの低下が少ないという利点がある．この方式はイントラネット内

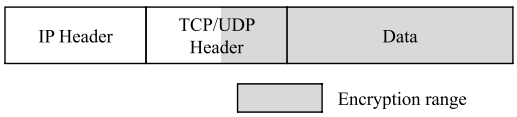


図 2 置換方式のパケットフォーマット
Fig. 2 Packet format of the replacement method.

では有効であるが，TCP/UDP チェックサムフィールドが暗号化範囲に入っているためチェックサムの書き換えをともなう NAT を通過できない．また，本人性確認とパケットの完全性保証を実現していないため，なりすましや改竄の恐れがある．

3. 実用暗号通信 PCCOM の提案

PCCOM が提供する機能は，暗号化による機密性確保，本人性確認とパケットの完全性保証である．また，NAT やファイアウォールとの共存ができ，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．なお，IP アドレスとポート番号は NAT で内容が変換されるため完全性保証の範囲に含めない．この部分の保証に関しては，パケットの処理内容を記述した動作処理テーブルの検索過程でその内容を保証する．

3.1 PCCOM の原理

PCCOM のパケットフォーマットを**図 3** に示す．PCCOM では，共通秘密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により，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．

PCCOM では本人性確認と完全性保証を実現するために，まず CB（Checksum Base）と呼ぶチェックサムベース値を定義する．CB 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（**図 4** の

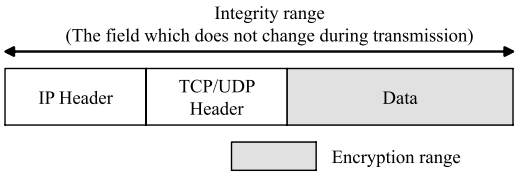


図 3 PCCOM のパケットフォーマット
Fig. 3 Packet format of PCCOM.

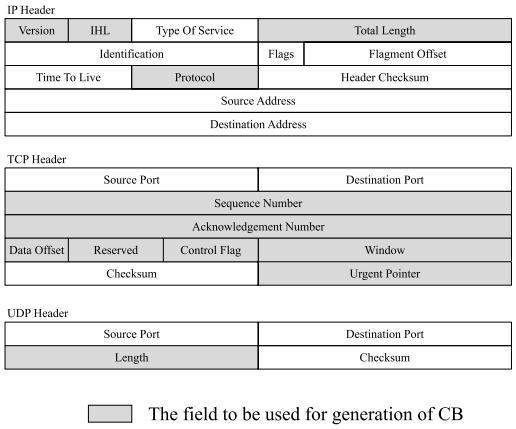


図 4 CB 生成に用いるフィールド
Fig. 4 The field to be used for generation of CB.

灰色部分）と，事前に秘密裏に共有している共通秘密鍵を含めた値から生成したハッシュ値である．CB の種には共通秘密鍵のほかにシーケンス番号のように初期値が乱数で決まりパケットごとに値が変化するフィールドを含んでおり，CB 値を第三者が推測するのはきわめて困難である．この CB 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．

一般通信と PCCOM の，TCP/UDP チェックサムの計算範囲の違いを**図 5** 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情報を指す．一般の通信では TCP/UDP チェックサムは，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．ここで，TCP/UDP 疑似ヘッダには IP アドレスの値を含む．このため，NAT を経由して IP アドレスが変わると，TCP/UDP チェックサムも書き換えが必要となる．一方，PCCOM では TCP/UDP チェックサムは，TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，疑似データから計算される．ここで，疑似データとは暗号化後のデータと CB をもとに求めたハッシュ値である．

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

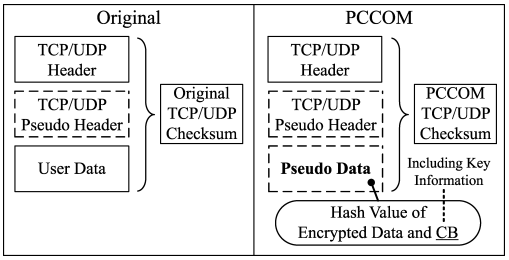


図 5 チェックサム計算範囲の違い
Fig. 5 Calculation range of checksum.

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 CB 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，パケットの一部を書き換えると同時に 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．なお，IP アドレスとポート番号は NAT で変換されるので CB 生成の範囲には含めない．IP アドレスとポート番号の保証方法については次節で述べる．

上記の演算方式によると，通信経路上に NAT 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．なぜなら，NAT における TCP/UDP チェックサムの書き換えは，文献 11) で規定されているように変換部分の差分を計算するだけであり，受信側で行うチェックサムの検証には影響を与えないためである．PCCOM ではパケットの暗号化範囲はユーザデータ部分のみとしているが，本人性確認とパケット全体の完全性保証が施されているため，パケットの偽造による TCP セッションハイジャックなどの攻撃を防ぐことができる．また，PCCOM ではファイアウォールが TCP/UDP 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であるため，実用面でのメリットが大きいと考えられる．

暗号アルゴリズムとしては，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，暗号化によってパケット長が変化することがなく，高スループットが実現でき，かつフラグメントの発生を懸念する必要がない．なお，暗号化で必要な初期値 IV（Initialization Vector）には CB 値を流用する．

3.2 IP アドレス・ポート番号の保証

PCCOM では，IP アドレスとポート番号は NAT を経由する際に値が変化するため CB 生成の範囲に含めていない．そのため，このままでは通信経路上で送信元アドレスの改竄や，ポート番号の改竄によるアプリケーションの誤作動などを招く可能性がある．これらを防ぐために，IP アドレスとポート番号の完全性は，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．テーブル検索の処理を**図 6** に示す．動作処理情報テーブルとは IPsec における SAD（Security Association Database）に相当するもので，テーブル内には送信元と宛先の IP アドレスとポート番号，プロトコル番号とそれに対応する，パケットの処理内容（暗号化/復号，透過中継，廃棄），使用する共通秘密鍵の格納場所，適用するハッシュ関数，暗号アルゴリズムが記述されている．送信側と受信側の両端末は通信の開始前に設定情報の交換を行い，両端末で，通信パケットの処理に必要となる動作処理情報テーブルを生成してカーネルに保存する．送信側の端末はパケット送信時に，受信側の端末はパケット受信時に，パケットの IP アドレス，ポート番号，プロトコル番号をキーに動作処理情報テーブルを検索し，その内容に従って暗号化/復号などの処理を実行する．したがって，受信側の動作処理情報テーブルを検索後，テーブルの内容から IP アドレス，ポート番号，プロトコル番号を再度確認し，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．なお，一定時間以上参照されない動作処理情報テーブルのレコードは削除する．また，事前に設定した有効期限より長い間通信が継続された場合には，再度その内容を更新するための手続きが実行される．

この方式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．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] などの既存の技術を流用することが可能である．ここで，IKE は安全な通信路を確立する SA（Security Association）と共通秘密鍵を管理するプロトコルであり，たとえば，受信側での SA の特定には IP アドレス，ポート番号，プロトコル番号を用い，PCCOM 特有の部分を PCCOM DOI（Domain of Interpretation）として定義することにより，動作処理情報テーブルの生成が実現できる．

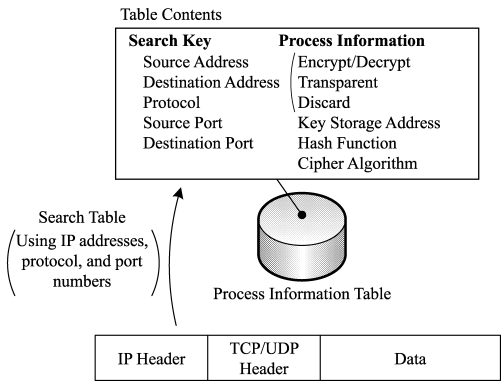


図 6 テーブル検索処理
Fig. 6 Table search process.

4. 実装方式

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．

4.1 実装方式

試作システムは，FreeBSD（5.3 Release）のカーネル内に実装した．試作システムの実装方式を**図 7** に示す．IP 層で行われる既存の処理にいっさいの変更を加えず，カーネル空間の関数である `ip_input()`，`ip_output()` で PCCOM 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，このような方式を容易に実現できるうえ，高スループットを発揮できるという利点がある．一方，IPsec 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 層全体にわたって処理の変更が必要となる．

4.2 システムの仕様・構成と動作概要

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

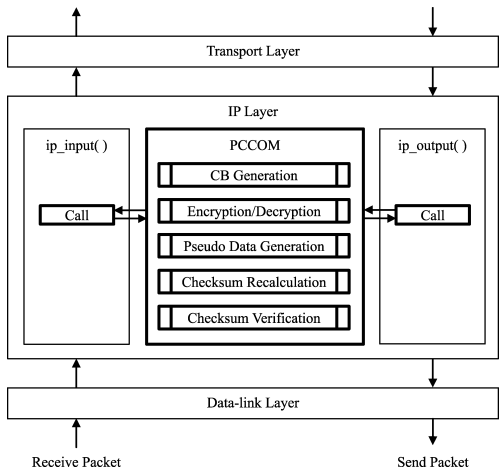


図 7 試作システムの実装方式
Fig. 7 Implementation method of the trial system.

表 1 試作システムの仕様
Table 1 Specification of the trial system.

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

表 2 実験端末の仕様
Table 2 Specifications of the terminals.

項目	内容
CPU	Pentium4 2.4 GHz
Memory	256 MB
NIC	10BASE-T，100BASE-TX，1000BASE-TX
OS	FreeBSD（5.3 Release）

ゴリズムは AES（鍵長は 128 ビット）を採用し，ハッシュ関数は MD5 を用いた．なお，暗号ライブラリとして OpenSSL（openssl-0.9.7d）を採用した．

PCCOM モジュールは主処理とサブモジュールから構成される．主処理ではテーブル検索処理や各サブモジュールを呼び出す処理を行う．サブモジュールは，CB 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．PCCOM モジュールは通信パケットに対し，あらかじめ作成済みの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，ポート番号，プロトコル番号と，それに対応する動作内容，すなわち暗号化/復号，透過中継，廃棄などが記されている．`ip_input()`，`ip_output()` で PCCOM モジュールが呼び出されると，送受信パケットの IP アドレス，ポート番号，プロトコル番号から算出したハッシュ値で，該当する動作処理情報を検索し，テーブル内容に正しい IP アドレス，ポート番号，プロトコル番号が存在することを確認する．その後，テーブル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 NAT を中継して通信できることを確認し，パケット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．

5. 評　　価

5.1 試作システムの性能評価

試作システムを実装した 2 台の端末間の通信性能を測定した．参考のために IPsec ESP（KAME[12]）を実装した場合を測定し比較した．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 2** 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．

5.1.1 通信性能の測定

図 8 は IP パケット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 と呼ぶ），PCCOM の場合，IPsec ESP の場合のそれぞれについて示したものである．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[13] を用いて，10 回試行の平均値をとった．

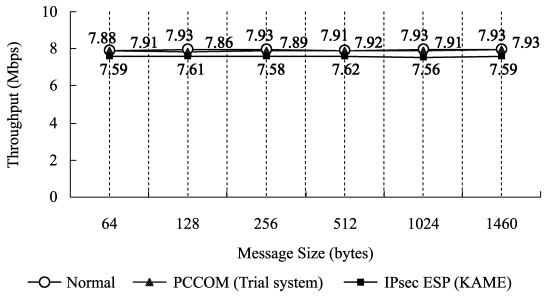
10BASE の環境では，ESP においては若干の性能低下が見られたものの，処理すべきパケット数が少ないため，PCCOM，ESP とも処理オーバヘッドはネックとなっていない．100BASE の環境では，Normal と PCCOM は NIC の上限性能を発揮しており PCCOM に性能低下は見られなかった．それに対し ESP はメッセージサイズ 1,460 バイトのパケット（以下，長パケットと呼ぶ）では Normal から約 6%性能が低下しており，メッセージサイズ 64 バイトのパケット（以下，短パケットと呼ぶ）では約 28.1%低下している．また 1000BASE の環境では，長パケットの場合 PCCOM は Normal から約 60.1%性能が低下しており，ESP では約 83.6%低下している．短パケットの場合 PCCOM は Normal から約 16.2%性能が低下しており，ESP では約 61.3%低下している．

パケットサイズが短く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である．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．

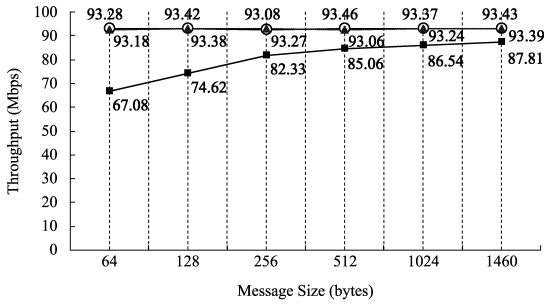
次に，1000BASE の環境において，FTP で 500 MB のファイルをダウンロードするのに要した時間を**図 9** に示す．測定結果は 10 回試行の平均値である．PCCOM は Normal の約 145.1%の時間であるのに対し，ESP は約 311.6%の時間を要している．

5.1.2 PCCOM 内部の処理コスト

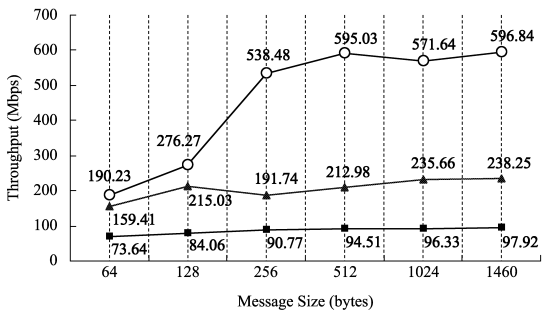
PCCOM における処理過程での処理コストを調べるために PCCOM の内部処理時間をモジュール別に測定した．内部処理時間は，RDTSC（ReaD Time Stamp Counter）を用いて処理前後の CPU クロック



(a) 10BASE environment



(b) 100BASE environment



(c) 1000BASE environment

図 8 スループット測定結果
Fig. 8 Measurement results of throughput.

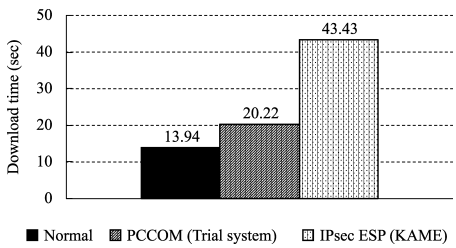


図 9 500 MB ファイルの FTP ダウンロード時間
Fig. 9 Download time of a 500 MB file using FTP.

表 3 PCCOM 内部の処理時間とそれぞれの比率
Table 3 Internal processing time of the PCCOM and each ratio.

	測定対象	処理時間 (μs)	比率 (%)
送信側	主処理（テーブル検索以外）	0.547	1.8
	主処理（テーブル検索）	0.268	0.9
	CB 生成	0.868	2.9
	暗号化	26.043	87.6
	疑似データ生成	1.704	5.7
	チェックサム再計算（独自）	0.294	1.0
受信側	主処理（テーブル検索以外）	0.545	1.7
	主処理（テーブル検索）	0.269	0.8
	CB 生成	0.890	2.8
	疑似データ生成	2.863	9.0
	チェックサム検証（独自）	0.281	0.9
	復号	25.547	80.6
	チェックサム再計算（通常）	1.286	4.1

カウンタ値を求めて算出した．

PCCOM 内部の処理時間とそれぞれの比率を**表 3** に示す．表 3 の主処理とは，PCCOM モジュールが呼ばれたときに最初に実行される処理で，主処理の中で動作処理情報テーブルの検索が実行され，その結果に基づいて各サブモジュールが呼び出される．測定結果は FTP の通信中に流れた IP データグラム長 1,460 バイトのパケット 10 個の結果の平均値である．表 3 より，送信側，受信側ともに暗号化/復号が処理の 8 割以上を占めていることが分かる．専用のハードウェア暗号エンジンを用いることなどで，処理時間の大幅な短縮が期待でき，より Normal に近い性能を発揮できると考えられる．また，動作処理情報テーブルの検索処理は約 0.27 μs と PCCOM 全体の約 1%程度であり，検索処理のオーバヘッドは問題とならない．

5.1.3 PCCOM の安全性

PCCOM が提供する機能はデータの機密性確保，本人性確認，パケットの完全性保証である．そのうえで考えられる脅威を以下に述べる．

PCCOM では IP ヘッダ，TCP/UDP ヘッダが平文であるためトラフィックの内容を解析される恐れがあるが，ファイアウォールの通過を可能とするにはヘッダ部分がファイアウォールに見えることが必須である．すなわち，ファイアウォールのパケットフィルタリングを可能にすることとトラフィック解析を不可とすることを同時に満足させることはできない．PCCOM は前者に重点を置くシステムを対象とする場合に有効である．

PCCOM では認証値がチェックサムフィールド長が 16 bit であるため，1/216 の確率でパケットの偽造や完全性保証範囲のフィールドの改竄に成功する．パケットの偽造を利用した代表的な攻撃として TCP セッションハイジャックが考えられるが，ハイジャック

を成功させるには，通信を中断させる RST パケット，再接続の SYN パケットとその SYN/ACK に対する ACK パケットの，3 ステップのパケットの偽造を成功させる必要があるため，実際にハイジャックに成功する確率はきわめて低い．また，仮にハイジャックに成功したとしても，ユーザデータは暗号化範囲であるため意図したデータを送ることはできない．また，ユーザデータは暗号化されているため意図した改竄は困難である．仮にユーザデータ部分が改竄された場合，受信側で行う復号の結果が予期せぬ値となり，多くのアプリケーションではエラー処理により廃棄される．また，音声などのストリーミングのパケットは，改竄されて予期せぬ復号結果となった場合はノイズとして扱われる．

PCCOM では，IP アドレスとポート番号は NAT を経由する際に値が変化するため完全性保証の範囲に含めていない．これらの完全性は，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．したがって，通信経路上で送信元アドレスの改竄や，ポート番号の改竄によるアプリケーションの誤作動などを招く行為を防ぐことができる．

動作処理情報テーブルはカーネル内に保存されるため，カーネルをハックされない限りその内容を改竄することは困難である．またテーブルを生成する際には，両端末間の確実な認証を必要とするため，誤った情報登録の可能性は低いと考えられる．

5.1.4 IPsec ESP とのすみわけ

IPsec ESP と PCCOM を 7 項目において定性的に比較した結果を**表 4** 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 NAT やファイアウォールと共存することができない．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，パケットフォーマットを変えないまま本人性確認とパケットの完全性保証を実現しており，NAT やファイアウォールと共存することができる．また，フラグメントが発生せず，高スループットを実現できるというメリットがある．暗号化範囲はポート番号によるフィルタリングを可能とするためユーザデータ部分のみとしているが，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いる．IP ヘッダ，TCP/UDP ヘッダは平文であるため，トラフィック解析をされる懸念があるが，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．

表 4 IPsec ESP との比較
Table 4 Comparison with IPsec ESP.

	IPsec ESP	PCCOM
機密性	Excellent	Good
本人性確認	Excellent	Good
完全性保証	Excellent	Good
NAT	Poor	Good
ファイアウォール	Poor	Good
フラグメント	Poor	Good
トラフィック解析	Good	Poor

IPsec ESP は，強靭なセキュリティを必要とする部門への適用が適しており，通信経路上に NAT やファイアウォールが存在してはいけない．また，スループットの低下が問題とならないことを確認する必要がある．用例としては，イントラネット内部でも特に強靭なセキュリティを要する部門や，インターネット上で拠点間通信などの重要データの取引が行われるような環境に適している．それに対し PCCOM は，NAT やファイアウォールとの共存が可能で，高スループットを実現できるなどの理由で，比較的広範囲への適用が可能と考えられる．用例としては，高スループットを要するアプリケーションの通信形態として多い P2P 通信や，パケットフィルタリングタイプのファイアウォールを備えたホームネットワークへのアクセス，部門ごとにファイアウォールを設置している場合が多いイントラネット内の通信に有効と考えられる．

6. ま と め

NAT やファイアウォールと共存でき，オリジナルパケットのフォーマットを変えないまま，本人性確認とパケットの完全性保証を行うことができる暗号通信方式 PCCOM を提案した．PCCOM は本人性確認と IP アドレス・ポート番号を除くパケットの完全性保証を，共通秘密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 チェックサムを再計算することにより実現する．また，IP アドレスとポート番号については動作処理情報テーブルを検索する過程でその内容を保証する．PCCOM の有効性を確認するために試作システムを実装し，動作検証を行った．性能測定の結果，高スループットが得られることを確認した．また，PCCOM の安全性について考察し，IPsec ESP とのすみわけが可能であることを示した．

参 考 文 献

1) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC2401 (1998).
2) Atkinson, R.: IP Authentication Header, RFC2402 (1998).
3) Atkinson, R.: IP Encapsulation Security Payload (ESP), RFC2406 (1998).
4) Harkins, D. and Carrel, D.: The internet key exchange (IKE), RFC2409 (1998).
5) Huttunen, A., Swander, B., Volpe, V., Diburro, L. and Stenberg, M.: UDP Encapsulation of IPsec Packets, RFC3948 (2005).
6) Zhang, Y. and Singh, B.: A Multi-Layer IPsec Protocol, *Proc. 9th USENIX Security Symposium* (2000).
7) 渡邊 晃，厚井裕司，井手口哲夫，横山幸夫，妹尾尚一郎： 暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌，Vol.38, No.4, pp.904–914 (1997).
8) Braden, R., Borman, D. and Partridge, C.: Computing the Internet Checksum, RFC1071 (1988).
9) Mallory, T. and Kullberg, A.: Incremental Updating of the Internet Checksum, RFC1141 (1990).
10) Rijsinghani, A.: Computation of the Internet Checksum via Incremental Update, RFC1624 (1994).
11) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC1631 (1994).
12) KAME Project. http://www.kame.net/
13) Netperf. http://www.netperf.org/
14) 増田真也，渡邊 晃： 実用性を重視した暗号通信方式の提案，情報処理学会研究報告，2004-CSEC-26, pp.267–274 (2004).
15) 増田真也，渡邊 晃： 実用暗号通信 PCCOM の実装と評価，情報処理学会研究報告，2004-CSEC-28, pp.205–210 (2005).
16) 増田真也，鈴木秀和，渡邊 晃： IPv4/IPv6 混在環境における暗号通信方式の考察，DICOMO 2005, pp.693–696 (2005).
17) Masuda, S., Suzuki, H., Okazaki, N. and Watanabe, A.: Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls, *ICOIN2006* (2006).

(平成 17 年 9 月 16 日受付)
(平成 18 年 4 月 4 日採録)

増田 真也（正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．同年 NTT ソフトウェア株式会社入社．モバイル&セキュリティ・ソリューション事業グループに所属．修士（工学）．2004 年情報処理学会全国大会学生奨励賞受賞．

鈴木 秀和（学生会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．現在，同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程に在学中．ネットワークセキュリティ，モバイルネットワーク等の研究に従事．修士（工学）．2006 年 IEEE 名古屋支部学生奨励賞受賞．

岡崎 直宣（正会員）

1986 年東北大学工学部通信工学科卒業．1991 年同大学大学院工学研究科電気および通信工学専攻博士後期課程修了．同年三菱電機株式会社入社．2002 年宮崎大学工学部助教授．通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事．博士（工学）．電子情報通信学会，電気学会，IEEE 各会員．

渡邊 晃（正会員）

1974 年慶應義塾大学工学部電気工学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．