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

043432038　増田真也
渡邊研究室

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（Encapsulation Security Payload）が挙げられるが，セキュリティは強靭なものの，NAT/NAPT（以後 NAT と総称）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，などの課題があり企業間通信などの一部でしか利用されていない．そこで本研究では，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．

2. 既存技術とその制約

IPsec ESP（Transport mode）のパケットフォーマットを図 1 に示す．ESP 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．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 を計算し，ESP 認証値としてパケットの末尾に付加する．ESP は，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全ての 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 アドレスの変換を行なう 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．また，パケット長が変化することによりスループットの低下を伴う．

以上のことから，IPsec をシステムに導入するには，通信経路上に NAT やファイアウォールが存在せず，かつスループットの低下が許容される環境下である必要がある．

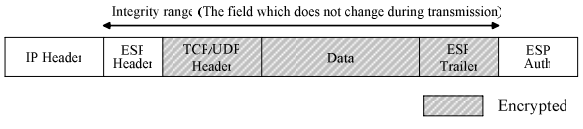


図 1　IPsec ESP のパケットフォーマット

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の他に本人性確認と完全性保証が可能である．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．

3.1 PCCOM の原理

PCCOM のパケットフォーマットを図 2 に示す．PCCOM では，疑似データと呼ぶ CB （Checksum Base）と暗号化後のデータのハッシュ値を用いて，独自の計算を施し，TCP/UDP チェックサムフィールドを書き換える．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．

完全性保証の流れを以下に述べる．送信側ではパケット送信時，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．検証結果が正しければ，復号後に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．

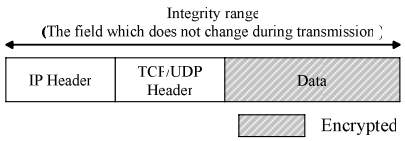


図 2　PCCOM のパケットフォーマット

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 生成の範囲に含めない．これらの情報の完全性は，パケットの処理内容を記述した動作処理情報テーブル（Process Information Table；PIT）の検索過程で保証する．テーブル検索の処理を図 3 に示す．PIT 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），共通秘密鍵の識別情報が記述されている．PIT は通信に先立ち，端末同士が設定情報を交換することにより生成される．送信側の端末はパケットの送信時に，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，プロトコル番号を元に PIT を検索し，テーブル内に該当パケットの動作処理情報が存在する場合はその情報に応じてパケットを処理する．従って受信側のテーブル検索後，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

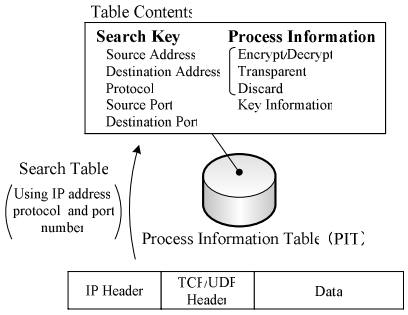


図 3　テーブル検索処理

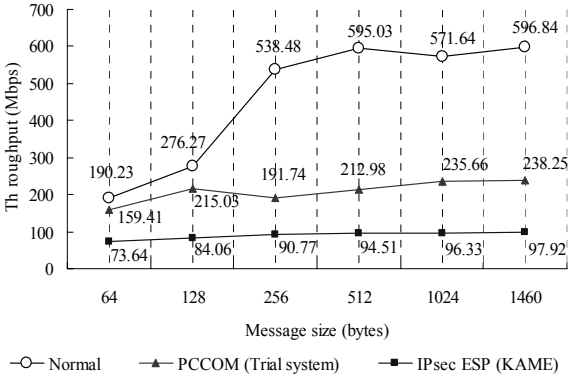


図 4　スループット測定結果

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．

4. PCCOM の実装

PCCOM の試作システムを開発し，動作検証を行った．試作システムは，FreeBSD（5.3 R）のカーネル内に実装した．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 PCCOM モジュールに処理を渡し，処理を終えたら差し戻す．

PIT 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 MD5 を用いた．なお，暗号ライブラリとして OpenSSL を採用した．

5. 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）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は，CPU は Pentium4 2.4GHz，メモリは 256MB，NIC は 1000BASE-T，OS は FreeBSD5.3R である．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 通信性能の測定

図 4 は IP パケット長とスループットの関係を，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 を用いて，10 回試行の平均値をとった．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．

5.2 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て算出した．

各モジュールの処理時間とその比率を表 1 に示す．測定結果は FTP の通信中に流れた IP データグラム長 1460 バイトのパケット 10 個の結果の平均値である．表 1 より，送信側，受信側ともに暗号化/復号が処理の 80~90%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．

PCCOM は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は発生せず，メモリバッファに記憶されたパケットの情報をそのまま処理することができる．その結果，暗号化/復号の処理が大部分を占め，5.1 項の通信性能測定においても高性能を発揮したと考えられる．

表 1　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	CB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	CB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

6. むすび

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，本人性確認と完全性保証を実現する暗号通信方式 PCCOM を提案した．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．

参考文献

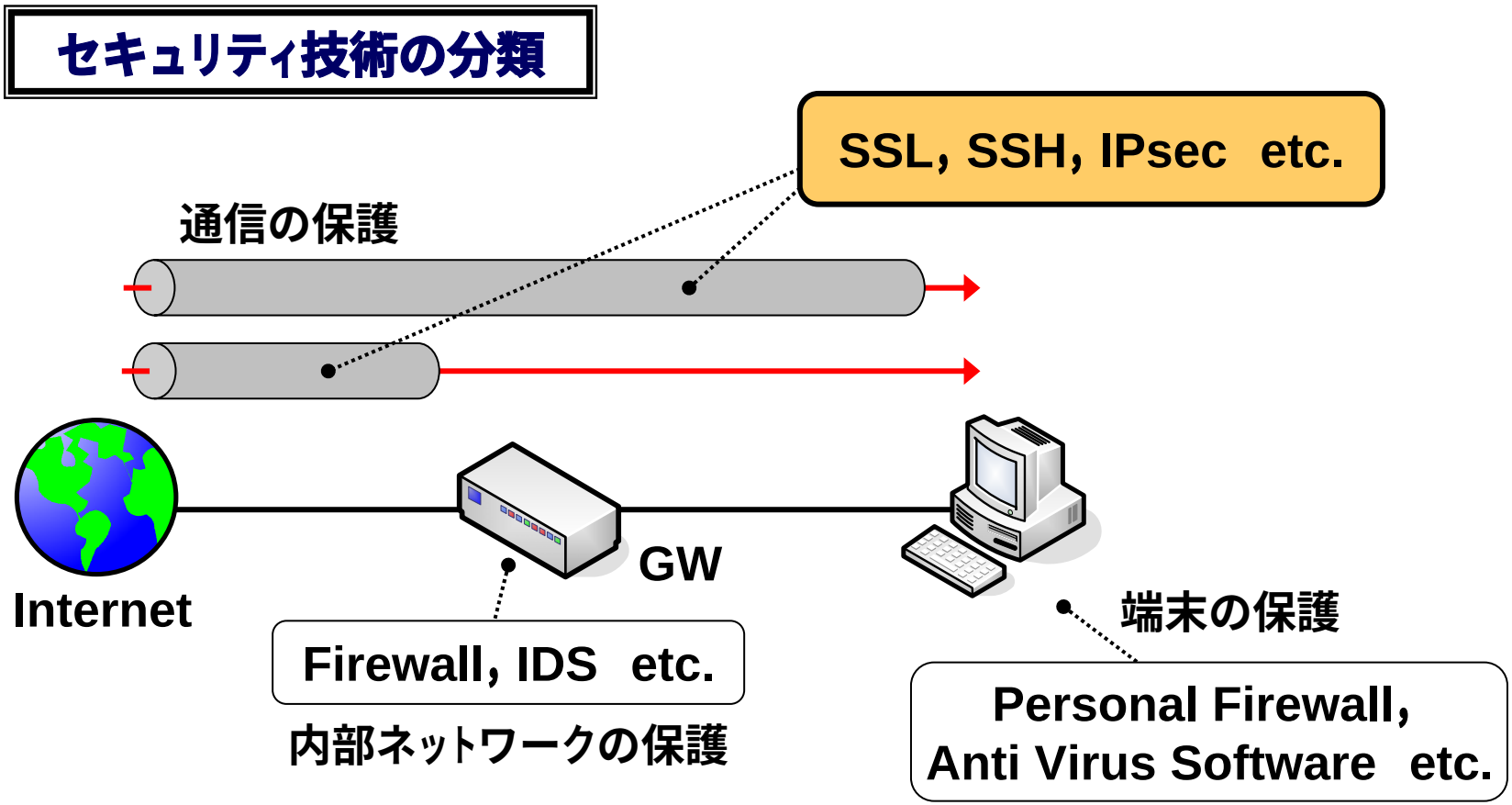
[1] 渡邊，厚井，井手口，横山，妹尾，“暗号技術を用いたセキュア通信グループの構築方式とその実現”，情処学論， vol.38, no.4, pp.904-914, Apr 1997.

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

名城大学大学院理工学研究科情報科学専攻
渡邊研究室
043432038　増田 真也

研究背景

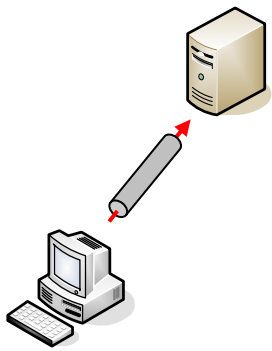
- ネットワークにおけるセキュリティ上の脅威
  → セキュリティ技術の重要性



研究背景

- **通信を保護する技術**
  - **アプリケーションセキュリティ**

SSL



SSH

PGP

etc.

  - **ネットワークセキュリティ**

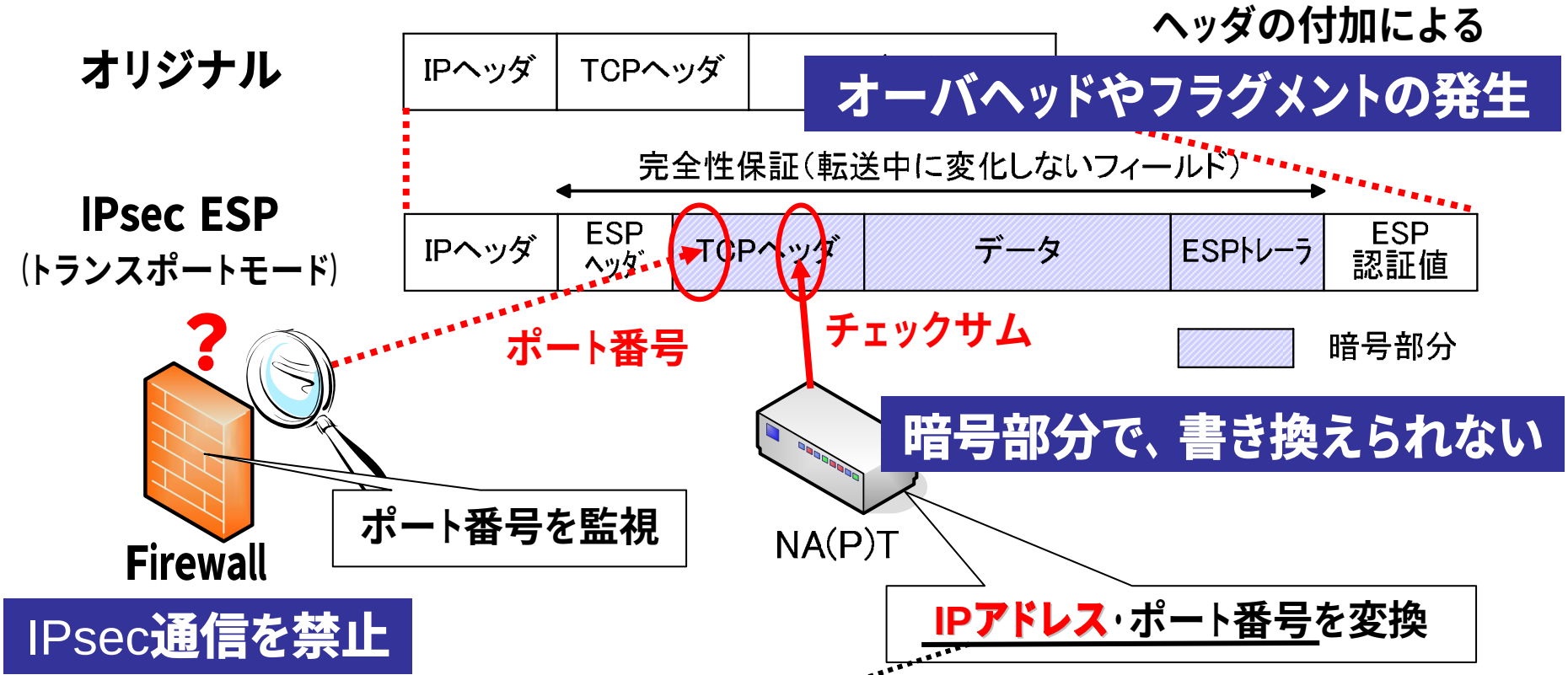
IPsec etc.

アプリケーションに依存することなく安全を確保

研究背景 －IPsec ESP －

既存技術

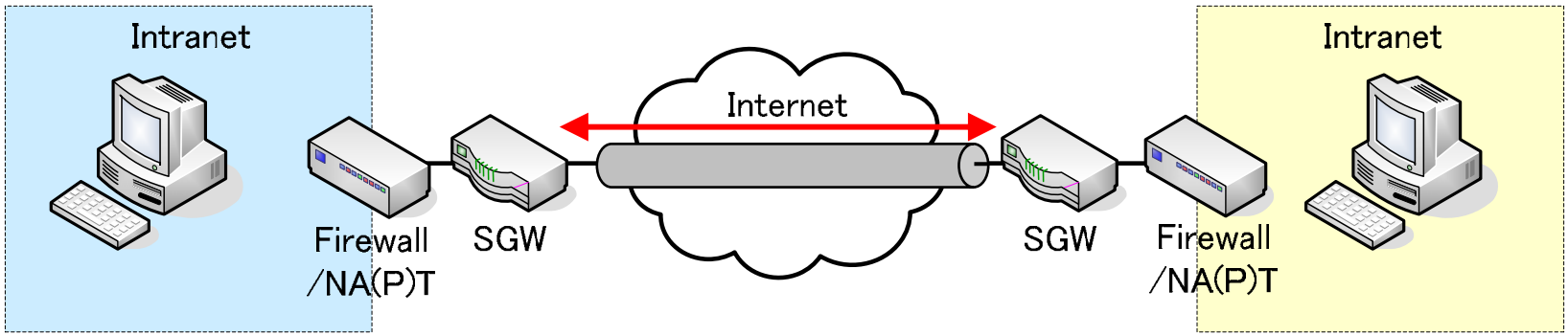
- **既存のネットワークセキュリティ技術**
  - IPsec ・・・ **IP層の技術で，強力なセキュリティを提供**
    - IPsec ESP (Encapsulation Security Payload) ・・・**暗号通信方式について規定**



研究背景 －IPsec ESP －

既存技術

主な用途



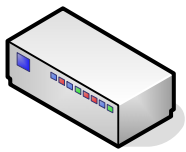
インターネットVPN（Virtual Private Network）

他の用途ではあまり普及していない

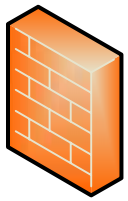
NA(P)Tやファイアウォールとの共存が困難なことに起因

研究背景 －補完技術の必要性－

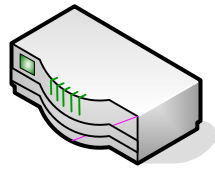
補完技術の必要性



NA(P)T



Firewall



QoS対応ルータ

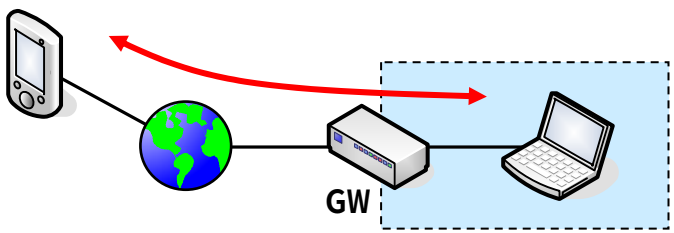
既存システムや新たな技術に対応したセキュリティ技術

セキュリティ強度 ⟷ 実用度（柔軟性・利便性）

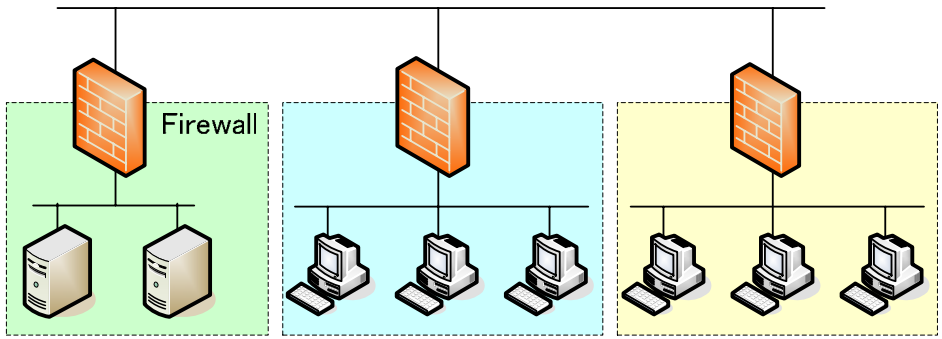
利用形態に適した方式を検討することが重要

- PCCOM (Practical Cipher COMmunication)
  - NA(P)Tやファイアウォールなどの既存システムと共存可能
  - フラグメントは発生せず，高スループットを実現

想定環境



P2P通信



企業ネットワーク

PCCOMの原理 ―特 徴―

- パケットフォーマットを変えない
  - フラグメントは発生しない
  - 処理オーバヘッドは小さく，高スループットを実現

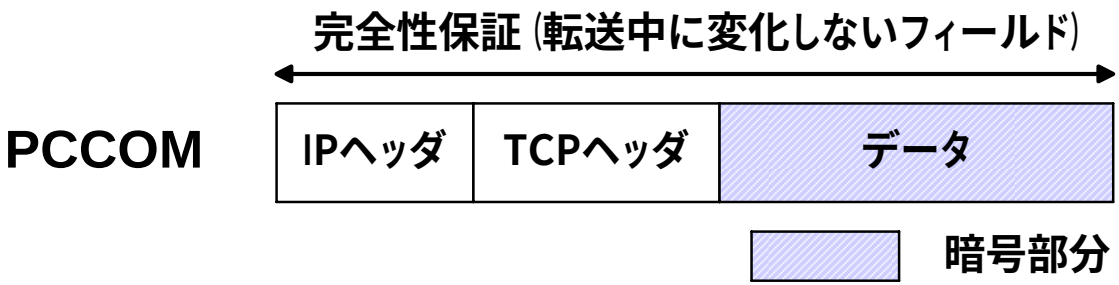
完全性保証･本人性確認

疑似データを用いたTCP/UDPチェックサムの独自計算により実現

IPアドレスとポート番号の完全性は動作処理テーブルの検索過程で保証

→ NA(P)Tと共存可能

- 敢えてユーザデータのみを暗号化
  - 従来どおりパケットフィルタリング可能で，ファイアウォールと共存可能



PCCOMの原理 －完全性保証・本人性確認－

完全性保証・本人性確認

– **疑似データを用いたTCP/UDPチェックサムの独自計算により実現**

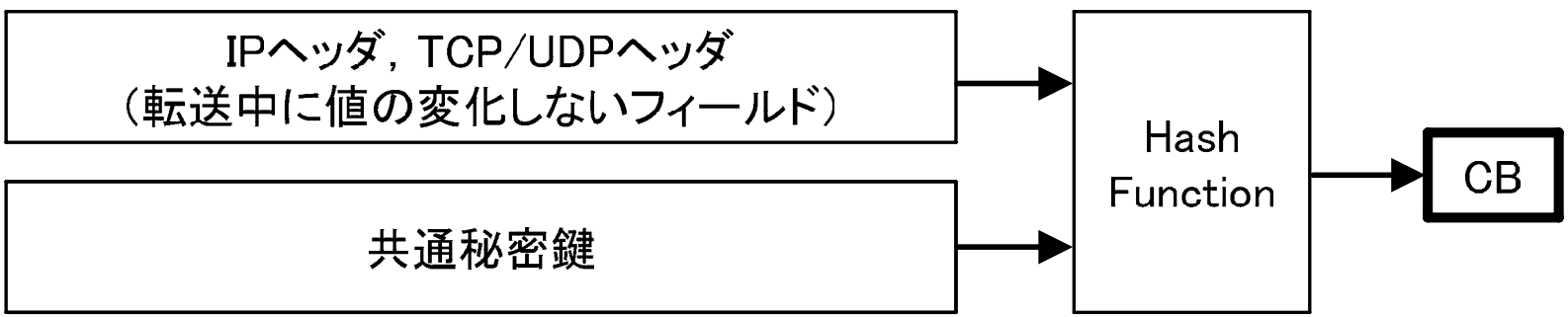
暗号データとCBのハッシュ値

ハッシュ値：入力データから生成した固定長の疑似乱数（不可逆）

CB (Checksum Base) :

完全性保証で用いるチェックサムベース値

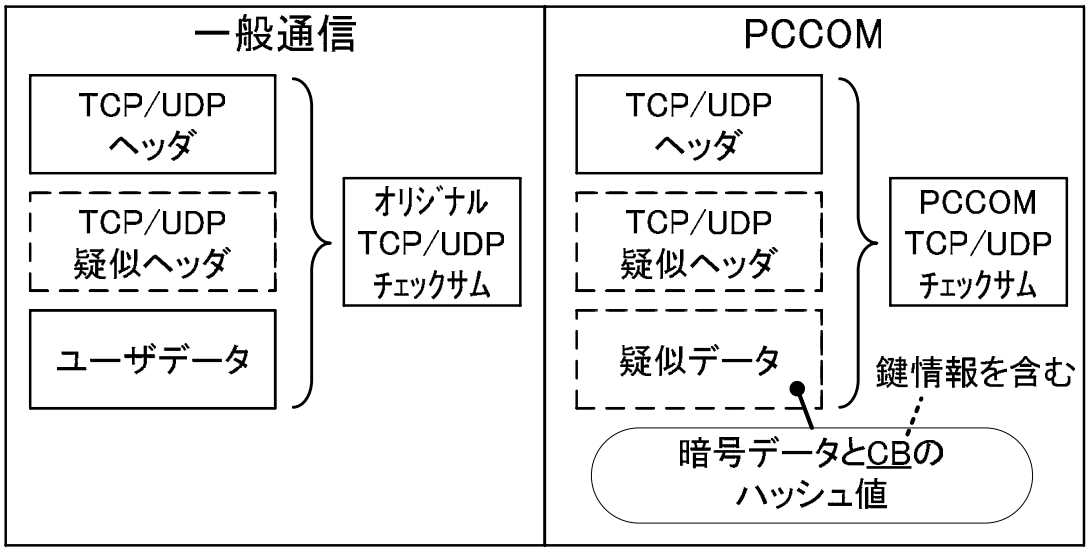
CBの生成方法



PCCOMの原理 －完全性保証･本人性確認－

完全性保証･本人性確認

- チェックサムの計算範囲の違い



- 送信側/受信側のチェックサムの計算範囲を，独自（右側）の方式にする

暗号化データ，CB生成に用いたフィールド　の完全性を保証

- 攻撃者は疑似データを作ることができない

本人性確認の実現

PCCOMの原理 －完全性保証・本人性確認－

完全性保証・本人性確認

- NA(P)Tを経由する場合
  - → IPアドレス，ポート番号が変換される
  - → 同時に，チェックサムの書き換えも行われる

- NA(P)Tにおけるチェックサムの書き換え

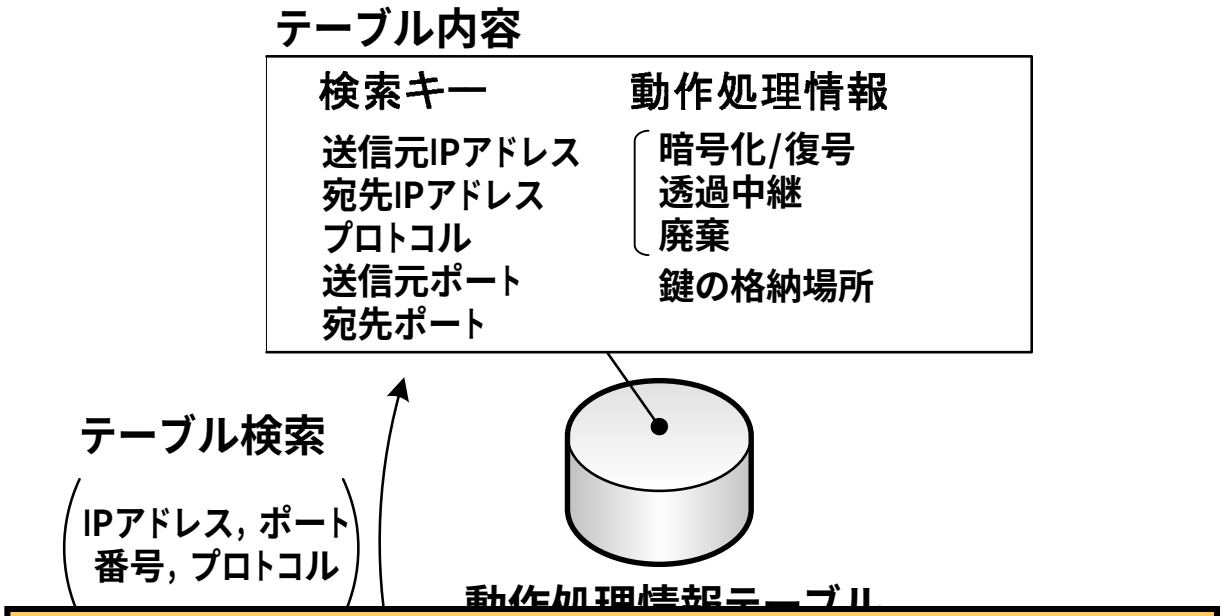
チェックサム計算範囲全体の再計算ではなく、
変換部分（IPアドレス，ポート番号）の差分計算

→ PCCOMのチェックサム検証には影響を与えない

PCCOMの原理 －IPアドレス，ポート番号の保証－

IPアドレス，ポート番号の保証

- PCCOM：IPアドレス，ポート番号を完全性保証の範囲に含めていない
  → 動作処理情報テーブルの検索過程で保証



正しいパケットの情報がテーブルに存在した場合…

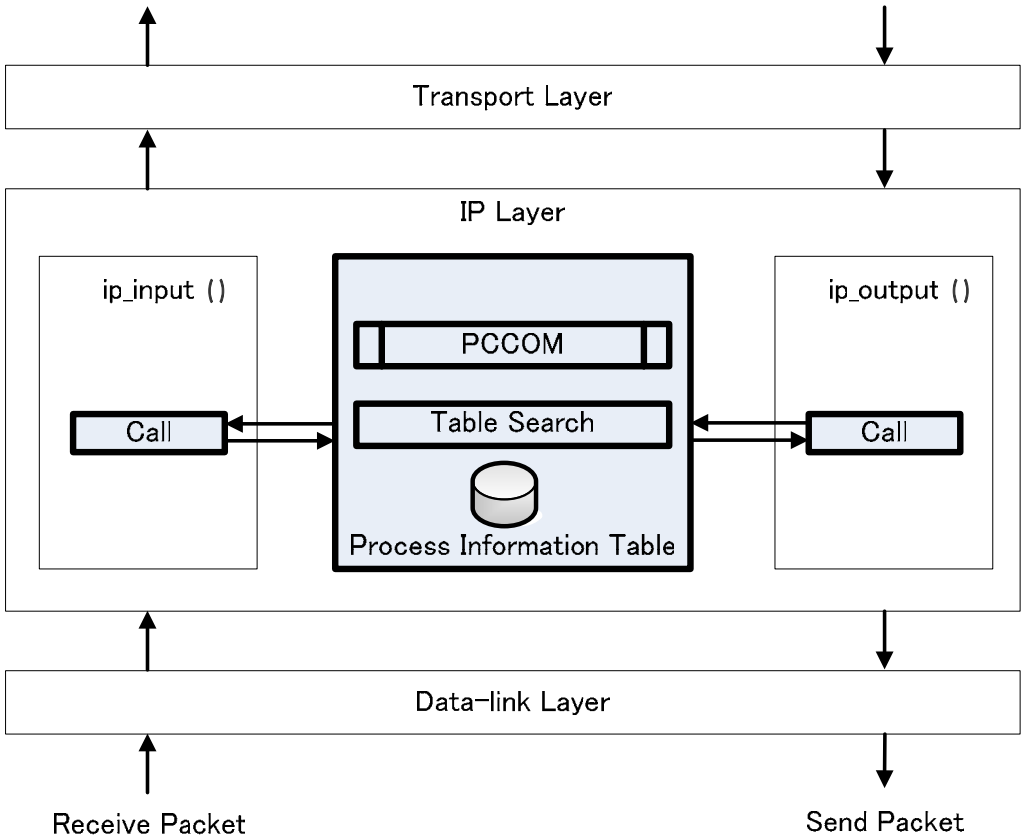
→ IPアドレスとポート番は改ざんされていない

- 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

実　装

実装方法

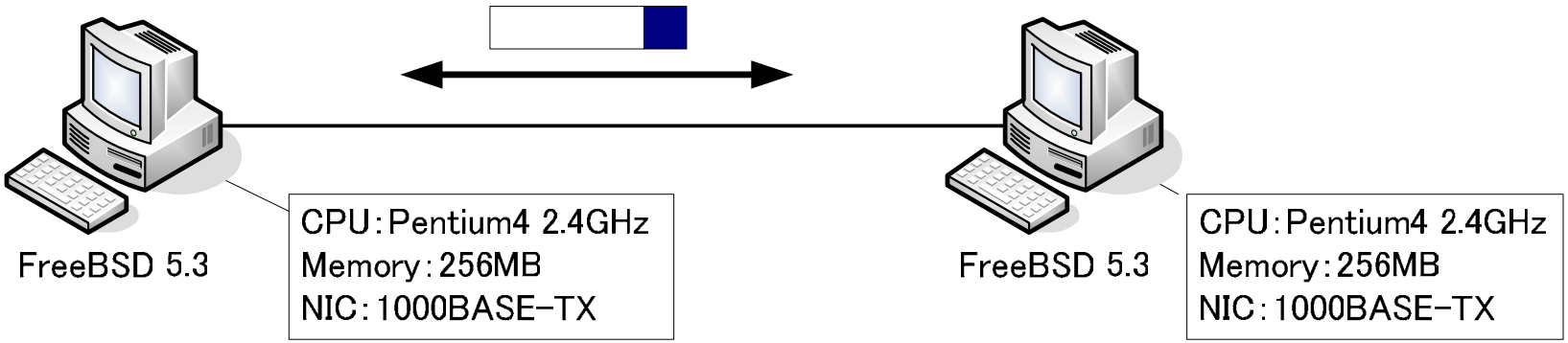
- FreeBSD (5.3R) のカーネルにモジュールを組み込む
- カーネルの関数 ip_input() / ip_output() でPCCOMモジュールをコールして処理を終えたら差し戻す



性能評価

実験目的

- 試作システムを実装した2台の端末間の通信性能の測定 (①)



- PCCOM内部の処理時間をモジュール別に測定し，処理ネックの部分を明らかにする　(②)

性能評価 ①

スループットの測定

- **以下，3つの性能を測定（通信環境：**1000BASE）

✓ **暗号化しない場合（以降，**Normal）

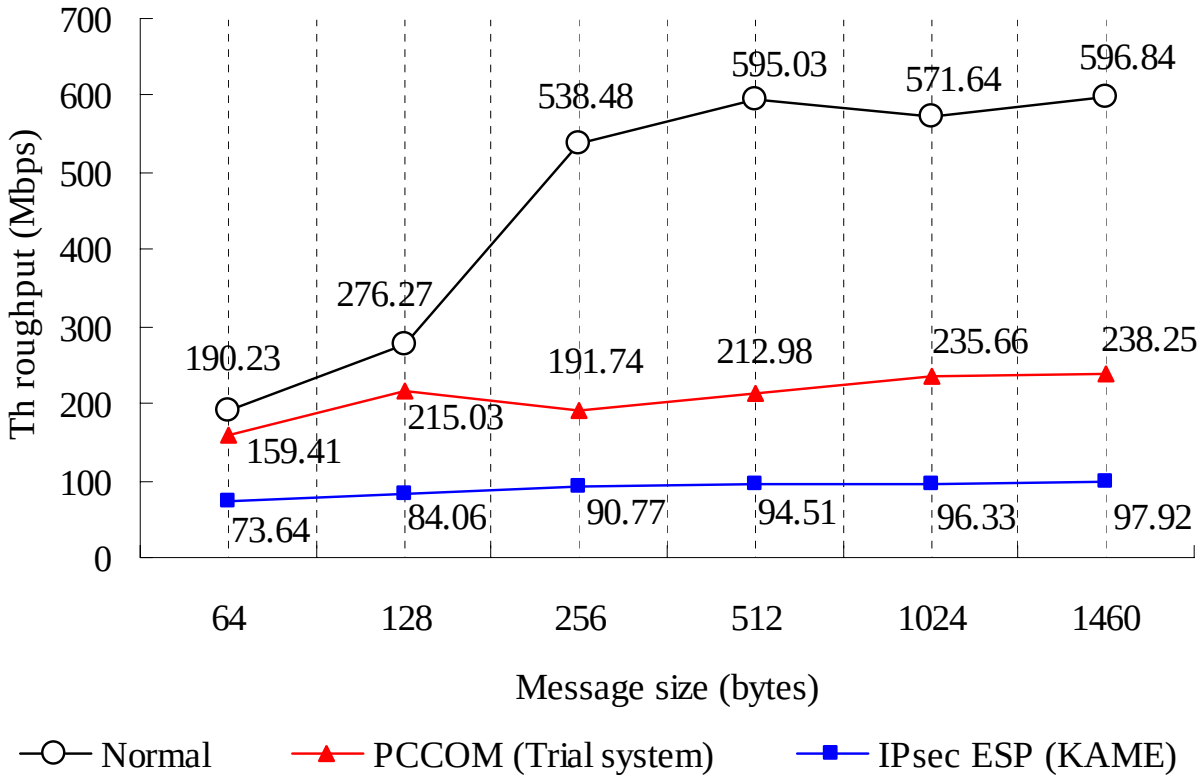
✓ PCCOM

✓ IPsec ESP

- **スループット測定：ネットワークベンチマークソフト** Netperf **を使用**
- **測定結果は**10**回試行の平均値**

性能評価 ①

スループットの測定



- **長パケット**：PCCOM**は**Normal**から約**60%，ESP**は約**84%**低下**
- **短パケット**：PCCOM**は**Normal**から約**16%，ESP**は約**61%**低下**

性能評価 ②

PCCOM内部の処理コスト

- RDTSC (ReaD Time Stamp Counter) **を利用**
- 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**

	モジュール	処理時間 (μs)	比率 (%)
送信側	CB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	CB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

IPsec ESPとのすみわけ

IPsec ESP

- ✓ 強靭なセキュリティ
- ✓ NA(P)Tやファイアウォールとの共存が困難
- ✓ ヘッダオーバヘッドやフラグメント発生によるスループットの低下

・イントラネットで特に強靭なセキュリティを要する部門
・拠点間通信での重要データの取引

PCCOM

- ✓ NA(A)Tやファイアウォールと共存可能
- ✓ フラグメントは発生せず，高スループットを実現

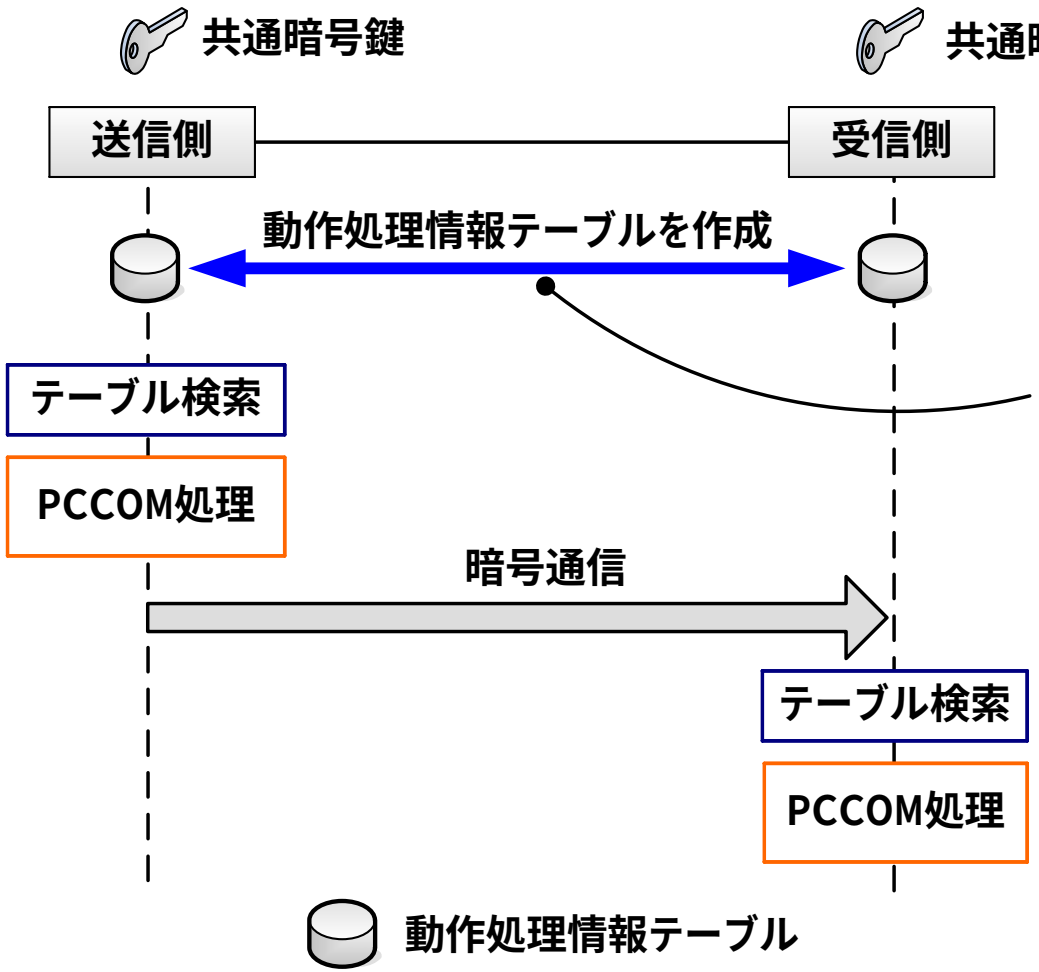
・P2P通信　(高スループットを要するアプリケーションが多い)
・ホームネットワークへのアクセス
・イントラネット内の通信　(部門間にファイアウォールが存在する)

実用性と安全性のトレードオフ

まとめと今後の課題

- **まとめ**
  - PCCOMの提案
    - 既存システム（NATやファイアウォール）と共存可能
    - フラグメントは発生せず，高スループットを実現
  - 試作システムによる性能評価
    - 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を確認
- **今後の課題**
  - リプレイ攻撃の対策

動作処理情報テーブル



動作処理情報テーブルは事前交渉プロトコルによって通信に先立って作成される

事前交渉プロトコル：DPRP，IKE など

PCCOMの安全性

- **提供機能**
  - **データの機密性確保**
  - **パケットの完全性保証，本人性確認**
- **考えられる脅威**
  - IPヘッダ，TCP/UDPヘッダは平文
    - トラフィック解析の恐れ
    - FWのパケットフィルタリングが可能　(こちらに重点)
  - $1/2^{16}$ の確率で改竄に成功
    - TCPセッションハイジャック　(意図したデータは送れない)
    - ユーザデータの改竄　(意図した改竄は不可能)