社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

実用性を重視した暗号通信方式の提案

増田 真也† 渡邊 晃†

†名城大学大学院理工学研究科 〒468-8502 名古屋市天白区塩釜口 1-501

E-mail: †m0432038@ccmailg.meijo-u.ac.jp, watanabeakr@ccmfs.meijo-u.ac.jp

あらまし 近年，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，ネットワークセキュリティ技術が重要視されてきている．暗号技術を用いたセキュリティ技術として，IP 層での技術である IPsec が挙げられるが，セキュリティは強靭なものの，NA(P)T やファイアウォールとの相性が悪い，フラグメントが発生するなど多くの課題がある．そこで本研究では，既存システムに影響を与えず，またオリジナルパケットとサイズを変えないまま，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方式 PCCOM(Practical Cipher COMmunication protocol)を提案する．本方式では，パケット長が変化しないため十分なスループットが期待できる上，NA(P)T やファイアウォールを通過できる実用的なシステムを構築できる．

キーワード 暗号通信，ネットワークセキュリティ，PCCOM

The Proposal of Practical Cipher Communication Systems

Shinya MASUDA† and Akira WATANABE‡

†Postgraduate Course in Science and Technology, Meijo University 1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan

E-mail: †m0432038@ccmailg.meijo-u.ac.jp, watanabeakr@ccmfs.meijo-u.ac.jp

Abstract In recent years, threads via network have become serious problem, hence people place a special emphasis on network security technologies. *IPsec*, the technology on IP layer, has been studied as the most popular protocol. However, it has a lot of subjects to be solved. Those are the compatibility problems with NA(P)T and Firewall, and occurrence of fragments, etc. In this paper, we propose the cipher communication systems, called *PCCOM(Practical Cipher COMmunication protocol)*, which can authenticate sender and receiver, guarantee the integrity of the packets. It does not give any influences to the existing systems because it is familiar with NA(P)T and Firewall, and we can expect high throughput systems, because it does not change the packet size.

Keyword Cipher Communication, Network Security, PCCOM

1. は じ め に

近年，ネットワークにおいて様々なセキュリティ上の脅威が問題となっており，それに伴いネットワークにおけるセキュリティが重要視されてきている．その中でも，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非常に有効な手段とされている．

ネットワークにおけるセキュリティ上の脅威はインターネットだけでなく，イントラネットにも存在する．実際，企業ネットワークにおける不正アクセス被害のうち半数近くが企業内部からのものであるという報告が出されている[1]．このようなことから，インターネットのみならずイントラネットも含めた総合的なセキュリティ対策を適用したいというニーズが最近増加している．イントラネットを視野に入れた場合，通信経路上に NA(P)T やファイアウォールが存在することがあり，これら既存システムとの相性を十分に考慮する必要があるが，これらが普及を阻害する原因となることがしばしばある．ゆえに，既存システムに影響を与えることなく容易に導入できることが，実用性を考える上で重要なポイントとなる．最近では，QoS 対応ルータのように上位層のプロトコルの情報を見るタイプが多く出てきたが，これらもまたセキュリティ技術との相性が悪いという問題がある．今後も様々な面

でネットワークの発展は期待されるが，セキュリティ技術がこれらの発展を阻害することがあってはならない．

既存のネットワークセキュリティ技術の代表として，IP パケットの暗号方式などを規定している IPsec が挙げられる[2]～[5]．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以外に，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．しかし IPsec は，セキュリティは強靭なものの，パケットの暗号化や完全性保証によって NA(P)T やファイアウォールを通過できなくなることや，パケット長の増加によってフラグメントが発生することなどが問題とされている．また，上位層の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多い．

これに対し，既存システムに影響を与えないよう暗号化範囲を規定し，パケット長を変えずに暗号化を行う方式も提案されている（以下，単に置換方式と呼ぶ）[6]．しかし，この方式においても TCP/UDP チェックサム[7]～[9]の書き換えを行う NA(P)T を通過できないことや，本人性確認とパケットの完全性保証を考慮していないという課題がある．

IPsec と置換方式以外では，暗号通信方式を規定しているものはほとんどない．そこで，本研究では従来の置換方式の利点を継承し，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 protocol)を提案する．本方式では，パケット長が変化しないため十分なスループットが期待できる上，NA(P)T やファイアウォールを通過できる実用的なシステムを構築できる．また，上位層のプロトコルの情報を見るルータなどとも相性が良い．

PCCOM の実現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崩さないで処理する方式であることが，実装の容易さをもたらすことについて述べる．

以下，2 章で既存の暗号通信方式とその課題，3 章で実用性を重視した暗号通信方式の要件と提案方式，4 章で試作システムの仕様と構成および実装方式，5 章で既存技術との比較検討，6 章でまとめと今後の課題について述べる．

2. 既存の暗号通信方式とその課題

IPsec は，IP 層のセキュリティとして盛んに研究が行われている．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，後者は主にセキュリティゲートウェイ間で IPsec 通信を適用する際に利用する．

しかし実際には，ESP トンネルモードを，インターネットを介して分散した拠点を結ぶ VPN(Virtual Private Network)[10]の構築手段として利用している場合が多い．これは，IPsec における設定の複雑さや以下で述べる NA(P)T やファイアウォールとの相性問題などが原因で，VPN のような特定の用途以外では利用が困難なためである．

そこで，以下では VPN 以外に考えられる用途を例に挙げ，トランスポートモードとトンネルモードのいずれにおいても NA(P)T やファイアウォールの通過が不可欠であることを示す．

WWW を代表とするクライアント/サーバシステムに IPsec を適用する場合，サーバ側にはセキュリティゲートウェイを設置するので，自ずとトンネルモードを利用することになる．このとき，プライベートアドレスのクライアントが外部サーバにアクセスする場合は NA(P)T やファイアウォールの通過は必須である．

近年急増している P2P(Peer-to-Peer)ネットワークでは，個人間の通信が主体となっており，IPsec を適用する場合は End-to-End であるトランスポートモードの利用が望ましい．このとき，NA(P)T やファイアウォールを経由することは十分にあり得る（図 1）．

また，イントラネットで IPsec を適用する場合はトンネルモードとの併用が考えられる．企業ネットワークでは，部門間にファイアウォールを設置することが多く，ファイアウォールの通過は必須である．

このように，いずれのモードにせよ NA(P)T やファイアウォールの通過は欠かせない．しかし， IPsec はこれら既存システムとの相性が問題とされている．

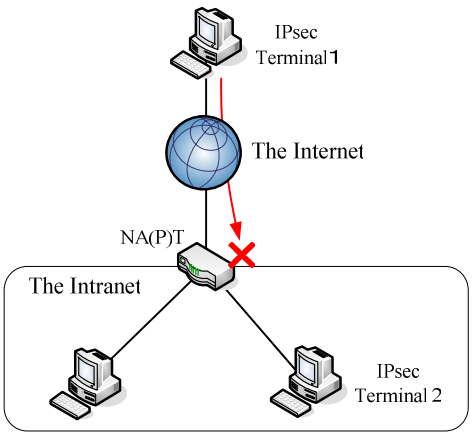


図 1　トランスポートモードで NA(P)T を経由する例

Fig.1　Example of NA(P)T traversal with transport mode.

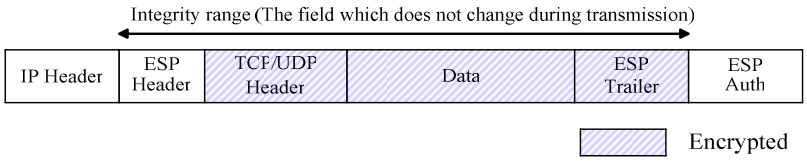


図 2　ESP トランスポートモードのパケットフォーマット

Fig.2　Packet format of ESP transport mode.

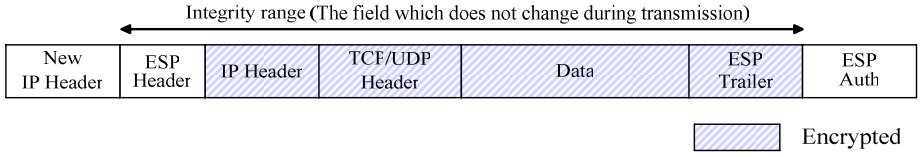


図 3　ESP トンネルモードのパケットフォーマット

Fig.3　Packet format of ESP tunnel mode.

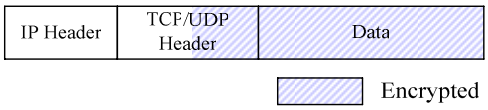


図 4　置換方式のパケットフォーマット

Fig.4　Packet format of the replace method.

ESP トランスポートモードの場合，図 2 のようにポート番号が暗号化により見えなくなるため，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ことが多い．また，TCP/UDP チェックサムが暗号化範囲・完全性保証の範囲に含まれているためチェックサムの書き換えを行う NA(P)T の通過はできない．この問題については UDP ヘッダでカプセル化することで NA(P)T を通過させる“UDP Encapsulation of IPsec Packets”がインターネットドラフトとして公開されており[11]～[13], 有効な手段として普及しつつあるが，カプセル部分は完全性保証の範囲に含まれていない．また，ヘッダなどの追加によるオーバヘッドやフラグメントの発生などの問題がある．

ESP トンネルモードの場合も，図 3 のようにポート番号が暗号化されているため，トランスポートモードと同様に，ファイアウォールを通過できない場合が多い．このモードにおいては，IP ペイロードにアドレスに依存したデータが存在しなければ NAT を通過できる．しかし，多くの場合がポート番号の変換も伴う NAPT を利用している．NAPT の場合は，変換時に TCP/UDP チェックサムの書き換えを行うのでトランスポートモードと同様に，NAPT を通過できない．更に，トンネルモードの場合はカプセル化を行うので，トランスポートモード以上にオーバヘッドやフラグメントが発生する懸念がある．

また，いずれのモードもヘッダの追加や暗号化を行うので，上位ヘッダのプロトコルの情報を見るルータなどは正しく処理できない場合が多い．

一方，置換方式では，既存システムに影響を与えないよう暗号化範囲を規定しているが，図 4 のように TCP/UDP ヘッダの後半部分以降を暗号化しているため，TCP/UDP チェックサムの書き換えを行う NA(P)T を通過できない．また，この方式はパケット長を変えない暗号化を実現しているが，本人性確認とパケットの完全性保証を考慮していないため，なりすましや改竄の恐れがある．

3. 実用性を重視した暗号通信方式 PCCOM の提案

3.1. 要　件

2 章で述べた課題を踏まえて，実用性を重視した暗号通信方式の要件を以下のように整理する．

(1) 既存システムに影響を与えることなく容易に導入できる．

(2) セキュリティ技術の導入によって発生するオーバヘッドやフラグメントを極力抑えることができる．

(3) パケットの暗号化だけでなく，本人性確認と完全性保証も行うことができる．

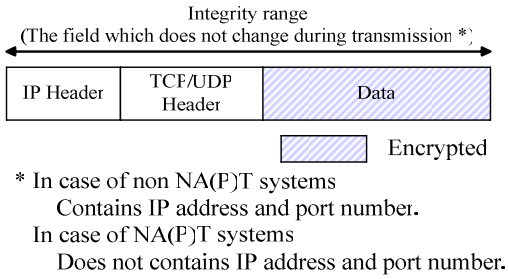


図 5　PCCOM のパケットフォーマット

Fig.5　Packet format of PCCOM.

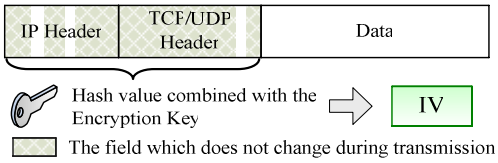


図 6　IV (Initialization Vector) の生成

Fig.6　Generation of IV (Initialization Vector).

3.2. 提 案 方 式

実用性を考える上で要件(1)は重要である．この要件を満たすには，NA(P)T やファイアウォールの通過が欠かせない．最近では上位層のプロトコルの情報を見るルータなどが出てきているように，既存システムに限らず新たなシステムを導入する際にも同様のことが言える．また，高スループットを実現するためには要件(2)がポイントとなる．パケットの暗号化により盗聴の防止が実現するが，要件(3)で示した改竄やなりすましの対策も不可欠な要素である．

本研究では，置換方式の利点を継承し，かつ置換方式で課題であった NA(P)T の通過を可能にしつつ，パケット長を変化させないまま，本人性確認とパケットの完全性保証も実現する方式として PCCOM(Practical Cipher COMmunication protocol)を提案する．PCCOM は，3.1 で示した要件を全て満たすことができる．尚，PCCOM の処理は全て IP 層で行う．また，PCCOM で用いる暗号鍵は事前に共有してあることを前提とする．

(1) 暗号化範囲

NA(P)T では TCP/UDP チェックサムの書き換えが行われる．また，ファイアウォールではパケット判別時にポート番号をチェックする．よってこれらのフィールドを暗号化してはならない．PCCOM では，図 5 のようにユーザデータ部分のみを暗号化の対象とする．すなわち，TCP/UDP ヘッダをあえて暗号化範囲から外すことで，ファイアウォールを通過できるようにする．また，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 モードを用いる．よって，PCCOM の処理によるフラグメントは発生しない．

(2) 完全性保証の方法

PCCOM では，図 5 のようにシステム構成によってパケットの完全性保証に関わる処理を分ける．NA(P)T を経由しない特定の環境において暗号通信を適用したい場合は，IP アドレスとポート番号を完全性保証の範囲に含める．この場合は本方式を独立して使用することができる．NA(P)T を経由する環境で暗号通信を適用したい場合は，IP アドレスとポート番号を完全性保証の範囲から外す．IP アドレスとポート番号については，他の技術との組み合わせで保証する方式を提案する．両者の区別は設定による．

① NA(P)T なしのシステム

暗号化/復号の際は，暗号鍵とは別に IV（Initialization Vector）と呼ばれるブロック暗号の先頭ブロックで用いる初期値を与える必要がある．IV は暗号化/復号で同じ値であり，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．そこで，図 6 のように 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 アドレスとポート番号を含む．TCP/UDP チェックサムを除く．）と，秘密裏に共有している暗号鍵を合わせたハッシュ値を IV とする．これにより，暗号化/復号で同じ値であり，パケットごとに異なる IV を生成することができる．IV の種として鍵情報を含めているため，第三者に IV が知られることはない．更にこの IV は，以下で述べる本人性確認とパケットの完全性保証の役割も果たす．

IPsec ESP ではヘッダに認証データを追加することで本人性確認とパケットの完全性保証を可能としているが，PCCOM ではパケット長を変えないためヘッダの追加はせず，TCP/UDP チェックサムフィールドを用いることで本人性確認とパケットの完全性保証を行う．本来 TCP/UDP チェックサムは，データの誤り検出を行うために用いるが，ここでは IP 層に独自の処理を追加することで本人性確認とパケットの完全性保証を行う．

送信側ではデータの暗号化後，図 7 のように暗号データと IV を合わせたハッシュ値をユーザデータと見なして（疑似データと呼ぶ）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，同様の方法で作成した疑似データによって計算したチェックサムを検証し，復号後に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（図 8）．

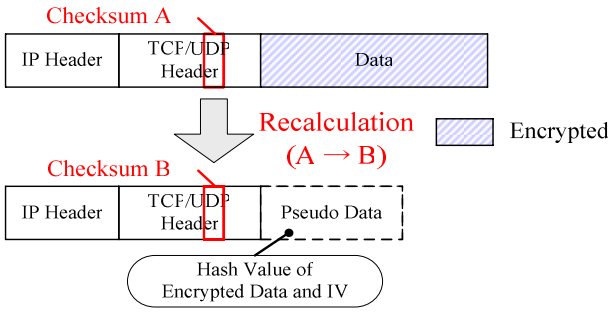


図 7　疑似データによるチェックサムの再計算

Fig.7　Recalculation of Checksum with Pseudo Data.

パケットを改竄した場合，改竄者は TCP/UDP チェックサムを再計算しようとするが，正当な者しか疑似データを作ることはできないので，改竄時に再計算を行うことはできない．この方式では，疑似データによって正当な相手であることが保証されるので本人性確認も実現する．

このように，疑似データによる TCP/UDP チェックサムの計算を行うことで，ヘッダの追加をせずに本人性確認とパケットの完全性保証が実現する．

② NA(P)T ありのシステム

NA(P)T を経由する場合は IP アドレスとポート番号が変化するため，これらを IV 生成の範囲から外す必要がある．同時に NA(P)T では，チェックサムの書き換えが行われる．ここで，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なので，受信側で行うチェックサムの検証には影響を与えない[14]．このような環境では IP アドレスとポート番号の完全性保証は，チェックサムとは別の方法で実現する必要がある．例えば，図 9 のように暗号通信に先立って行う DPRP（Dynamic Process Resolution Protocol）[15], [19]と本方式を組み合わせることで，IP アドレスとポート番号の完全性保証を実現できる．

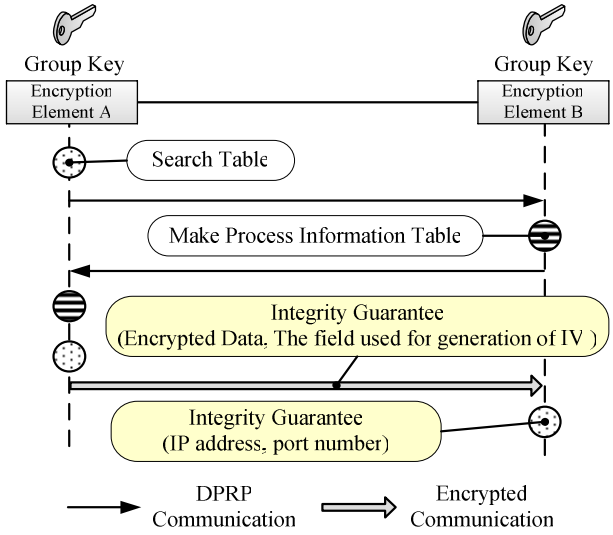


図 9　DPRP と組み合わせたパケットの完全性保証

Fig.9　Packet Integrity combined with DPRP.

DPRP は，暗号通信に先立って暗号化/復号などの動作処理情報を記したテーブルを作成する．テーブル作

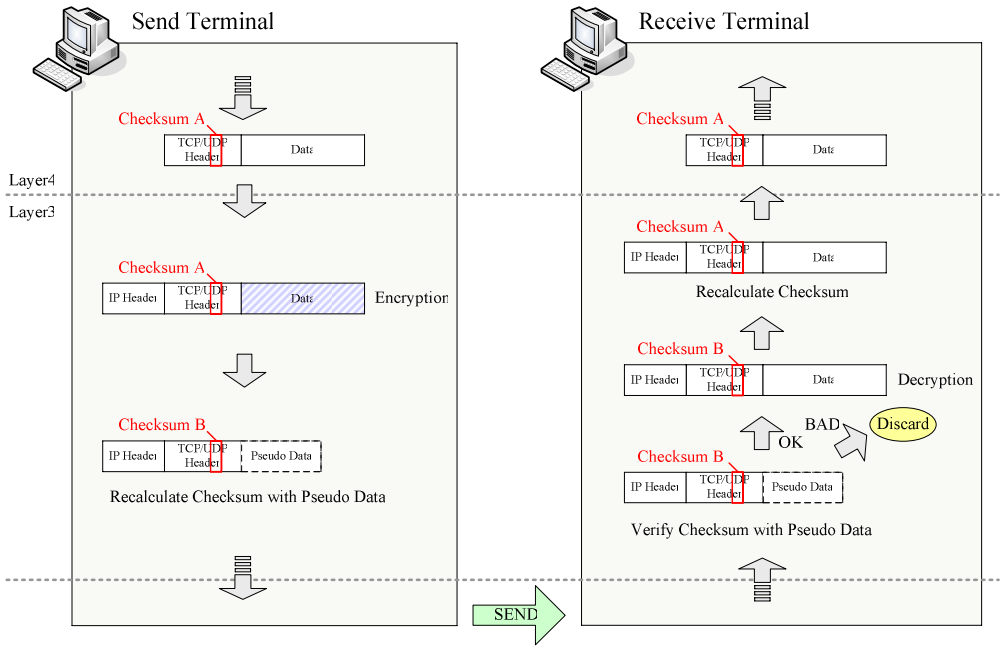


図 8　チェックサムの演算方法（End-to-End の場合）

Fig.8　Flow of the Checksum execution (case of End-to-End).

成時に流れる DPRP パケットの情報は暗号化されているため，信頼性のあるテーブルが作成される．暗号通信は，そのテーブルを基に行う．動作処理情報テーブルには IP アドレスとポート番号の情報が含まれており，IP アドレスとポート番号と上位層のプロトコル番号のハッシュ値を検索キーとしてテーブル検索を行う．すなわち，受信側でテーブル検索にヒットしたら 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．尚，DPRP は手段のひとつであり，この考え方を用いれば他の手段との併用も考えられる．

4. 試作システムの開発

PCCOM の実現性を確認するために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概要を述べ，システムの仕様と構成および実装方式について記述する．

4.1. 試作システムの概要

現在我々は，FPN(Flexible Private Network)[16]の構築を目指しており，それを実現するためのネットワークセキュリティアーキテクチャ GSCIP(Grouped Secure Communication for Internet Protocol; ジースキップ)[16]～[23]の開発を行っている．GSCIP は PCCOM 以外に，暗号通信に先立って行う事前交渉プロトコル DPRP，セキュア鍵配送プロトコル SKDP(Secure Key Distribution Protocol)，移動端末が通信中に移動しても通信が保証される移動体通信処理プロトコル Mobile P2P，グローバルアドレス空間からプライベートアドレス空間へのアクセスと可能とする NATF(NAT Free protocol)，渡り歩き検知機能などから構成される．

試作システムは，PCCOM の動作に最低限必要な，PCCOM モジュールと一連の処理を組み立てるメインモジュールを，端末に実装するソフトウェア型暗号装置として開発した．PCCOM モジュールは，呼び出し時に与えられる暗号化/復号などの動作内容を記した動作処理情報を基に処理を行う．動作内容が暗号化の場合は送信側の処理として，動作内容が復号の場合は受信側の処理として図 8 の手順に基づき処理する．

4.2. システムの仕様と構成

試作システムの仕様を表 1 に示す．テーブル検索にはハッシュ探索（チェイン法）を採用した．パケットの暗号方式は提案方式である PCCOM，暗号アルゴリズムは AES[24]，鍵長は 128 ビットとした．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 MD5[25]を用いた．尚，暗号ライブラリとして OpenSSL[26]を採用した（Version : openssl-0.9.-7d）．

試作システムのモジュール構成を表 2 に示す．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，そして 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．

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	ハッシュ探索（チェイン法）
暗号方式	PCCOM
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　試作システムのモジュール構成と機能

Table 2　Function table of the trial system.

モジュール	機　　能
メイン	テーブル検索機能，パケット判別機能，PCCOM モジュールを呼び出し，一連の処理を組み立てる．
PCCOM	本提案方式のメイン．各サブモジュールを呼び出し，一連の処理を組み立てる．
IV 生成	IP ヘッダ，TCP/UDP ヘッダで転送中に変化しないフィールドと暗号鍵を合わせたハッシュを生成する．
暗号化/復号	入力データをブロック暗号の CFB モードで暗号化/復号する．
疑似データ生成	暗号データと IV を合わせたハッシュを生成する．
チェックサム再計算	通常または疑似データによる独自の計算範囲でチェックサムの再計算を行う．
チェックサム検証	疑似データによる独自の計算範囲でチェックサムの検証を行う．

4.3. 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）のカーネル内に，4.2 で述べたモジュールを組み込むことで実現した．図 10 のように，IP 層で行われる既存の処理に一切の変更を加えず，IP 層の入出力の最適な場所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形を採用している．これは，PCCOM がオリジナルのパケットフォーマットを崩さずに処理する方式だから実現できることである．ヘッダの追加などパケットフォーマットに変更がある場合は，IP 層全体に渡って処理の変更が必要となる．

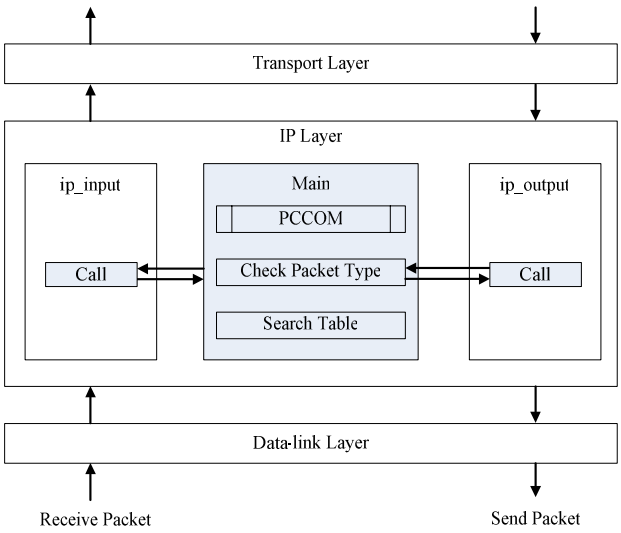


図 10　試作システムの実装方式

Fig.10　Implementation of the trial system.

5. 既存技術との比較検討

IPsec ESP と置換方式，PCCOM を 6 つの項目において比較した結果を表 3 に示す．

IPsec ESP は，TCP/UDP ヘッダを暗号化範囲に含めているが，特殊な処理・設定を行わないと NA(P)T やファイアウォールを通過できない．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，TCP/UDP ヘッダを暗号化範囲に含めない代わりに，NA(P)T やファイアウォールを通過できる．また，置換方式の課題である本人性確認とパケットの完全性保証も行える．パケット長が変化しないため，PCCOM の処理によるフラグメントは発生しない．

IPsec が強力な認証機能を提供するのに対し，PCCOM は認証値として TCP/UDP チェックサムフィールドを用いており，フィールド長が 16 ビットと短い．しかし，実用上は十分なものであり NA(P)T やファイアウォールの通過が可能になるなど，実用性が高いと言える．

IPsec は，セキュリティは強靭だが 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多くの課題がある．強力なセキュリティを要する場合は，これらの問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よう配慮しているため，実用性が高く比較的容易に導入できると考えられる．

6. む　す　び

実用性を重視した暗号通信方式として，既存システムに影響を与えず，またオリジナルパケットとサイズを変えないまま，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．

表 3　既存技術との比較

Table 3　Comparison with existing technologies.

	機密性	本人性確認	完全性保証	NA(P)T	ファイアウォール	フラグメント
IPsec ESP	◎	◎	◎	△	△	×
置換方式	○	×	×	×	○	○
PCCOM	○	○	○	○	○	○

PCCOM の実現性を確認するために試作システムを開発し，その実装方式について述べた．

今後は試作システムの性能測定を行い，既存技術との定量的な比較を行う予定である．また，正常なパケットを多量に送りつけるリプレイ攻撃の対策や，UDP パケットにおけるフラグメントの扱いについても検討する予定である．

文　献

[1] R. Richardson, “Issues and Trends: 2003 CSI/FBI Computer Crime and Security Survey”, CSI Press Release, Jun 2003.

[2] S. Kent and R. Atkinson “Security Architecture for the Internet Protocol”, RFC2401, Aug. 1998.

[3] R. Atkinson, “IP Authentication Header” RFC2402, Dec. 1998.

[4] R. Atkinson, “IP Encapsulation Security Payload (ESP)”, RFC2406, Dec. 1998.

[5] D. Harkins and D. Carrel, “The internet key exchange (IKE)”, RFC2409, Dec. 1998.

[6] 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，” 情処学論，vol.38, no.4, pp.904-914, Apr 1997.

[7] R. Braden, D. Borman, and C. Partridge, “Computing the Internet Checksum”, RFC1071, Sep. 1988.

[8] T. Mallory and A. Kullberg, “Incremental Updating of the Internet Checksum”, RFC1141, Jan. 1990.

[9] A. Rijsinghani, “Computation of the Internet Checksum via Incremental Update”, RFC1624, May. 1994.

[10] E. Rosen and Y. Rekhter “BGP/MPLS VPNs”, RFC2547 Mar. 1999.

[11] A. Huttunen, B. Swander, V. Volpe, L. Diburro, and M. Stenberg, “UDP Encapsulation of IPsec Packets”, Internet Draft,draft-ietf-ipsec-udp-encaps-09.txt, May. 2004.

[12] B. Aboba and W. Dixon, “IPsec-Network Address Translation (NAT) Compatibility Requirements”, RFC3715, Mar. 2004.

[13] T. Kivinen, A. Huttunen, B. Swander and V. Volpe, “Negotiation of NAT-Traversal in the IKE”, Internet Draft, draft-ietf-ipsec-nat-t-ike-08.txt, Feb. 2004.

[14] K. Egevang and P. Francis, “The IP Network Address Translator (NAT)”, RFC1631 May. 1994”.

[15] 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.

[16] Flexible Private Network, Watanabe lab. Division of Information Sciences, Meijo University, http://www-is.meijo-u.ac.jp/~watanabe/research/fpn.html

[17] 竹内元規，渡邊晃，“移動体通信におけるコネクションを維持した通信方式の研究”，情報処理学会第 66 回全国大会 講演論文集 3-463，Mar 2004.

[18] 加藤尚樹，渡邊晃，“NAT を意識しない個人ネットワークを管理する Home Fire Wall の提案”，情報処理学会第 66 回全国大会 講演論文集 3-469，Mar 2004.

[19] 鈴木秀和，渡邊晃，“GSCIP を構成する DPRP の仕組みの検討”，情報処理学会第 66 回全国大会 講演論文集 3-479，Mar 2004.

[20] 竹尾大輔，渡邊晃，“GSCIP を構成する渡り歩き検出機能の仕組みの検討”，情報処理学会第 66 回全国大会 講演論文集 3-481，Mar 2004.

[21] 増田真也，渡邊晃，“閉域通信グループにおける暗号化通信方式の検討”，情報処理学会第 66 回全国大会 講演論文集 3-483，Mar 2004.

[22] 保母雅敏，渡邊晃，“多段構成ネットワークにおける鍵配送方式の一検討”，情報処理学会第 66 回全国大会 講演論文集 3-495，Mar 2004.

[23] 前羽理克，渡邊晃，“生体認証を利用したセキュアネットワーク通信”，情報処理学会第 66 回全国大会 講演論文集 3-503，Mar 2004.

[24] Daemen. J and Rijmen. V, “AES Proposal: Rijndael”, http://csrc.nist.bov/encryption/aes/rijndael/Rijndael.pdf

[25] R.Rivest, “The MD5 Message-Digest Algorithm”, R-FC1321 Apr. 1992.

[26] The OpenSSL Project, http://www.openssl.org/

実用性を重視した暗号通信方式の提案

The Proposal of Practical Cipher Communication Systems

名城大学大学院理工学研究科
増田 真也　渡邊　晃

はじめに

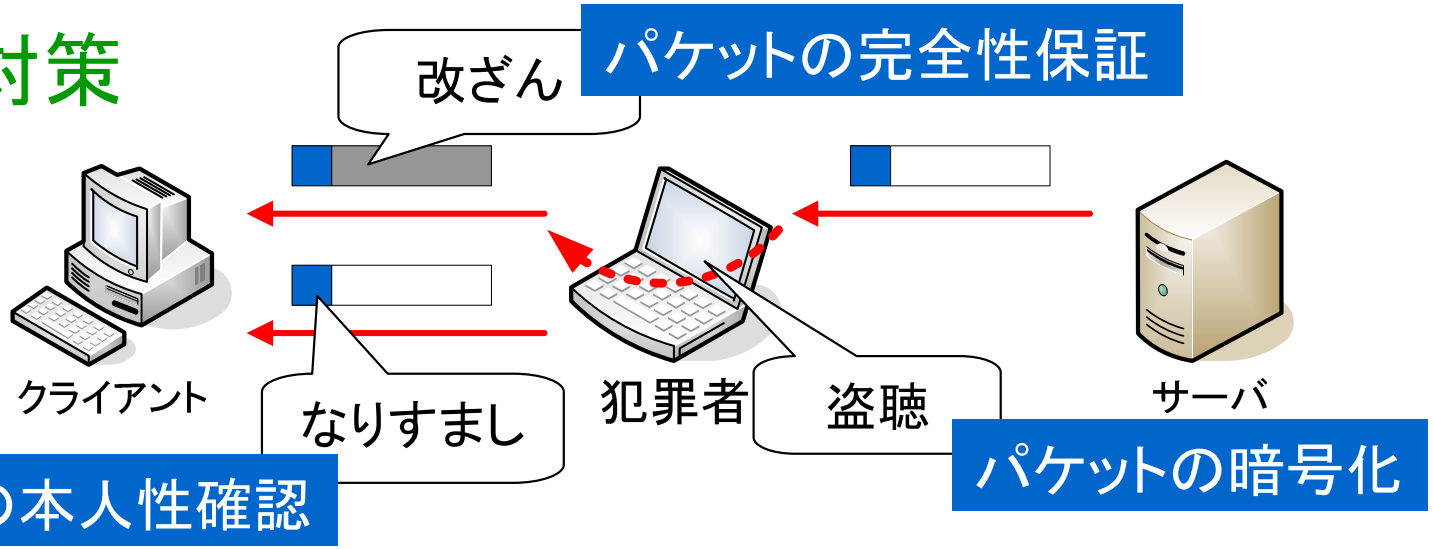
- ネットワークにおけるセキュリティ上の脅威

→ セキュリティ技術の重要性

- アプリケーションセキュリティ
  - SSL/TLS、SSH…
- ネットワークセキュリティ
  - IPsec…

アプリケーションに依存することなく安全を確保

主な対策



はじめに

- しかし、セキュリティ上の脅威は・・・
  - インターネットだけでなく、イントラネットにも存在する
    - → イントラネットも含めた総合的なセキュリティ対策
  - イントラネットを視野に入れた場合
    - 通信経路上にNA(P)Tやファイアウォールが存在することがある

これら既存システムとの相性を十分に考慮する必要性

→ セキュリティ対策の普及を阻害

既存システムに影響を与えず、 容易に導入できる

実用性を考える上で重要なポイント

はじめに

- 更に最近では・・・
  - QoS対応ルータのように上位層プロトコルの情報を見るタイプの出現

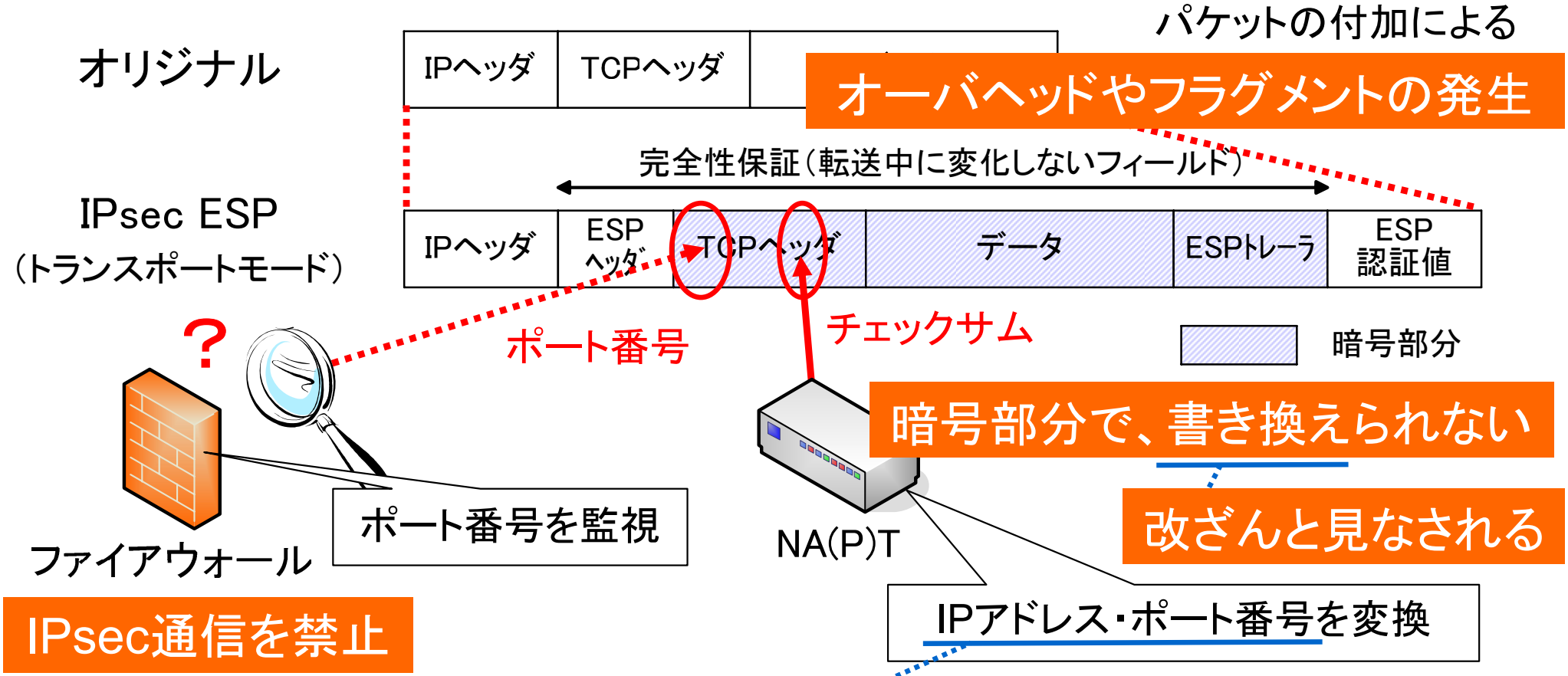
これらもセキュリティ技術との相性が悪い

- 今後も様々な面でネットワークの発展は期待される

セキュリティ技術がこれらの発展を
阻害することがあってはならない

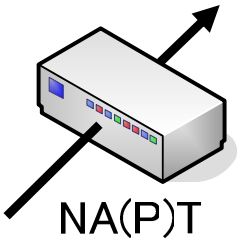
既存技術とその課題

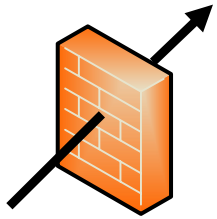
- 既存のネットワークセキュリティ技術
  - IPsec ・・・ IP層の技術で、強力なセキュリティを提供
    - IPsec ESP（Encapsulation Security Payload）・・・暗号通信方式について規定



→ アドレス・ポート変換時に、チェックサムの書き換えも行う

PCCOMの提案





NA(P)T、ファイアウォールを通過できる

オリジナル

IPヘッダ	TCPヘッダ	データ

パケット長を変化させない

提　案

これらを可能にしつつ

本人性確認と完全性保証も確実に行う暗号通信方式

PCCOM（Practical Cipher COMmunication protocol）

PCCOMの概要

- 暗号化範囲・暗号方式
  - ファイアウォールの通過
  - 上位層プロトコルの情報を見るタイプのルータと相性が良い
- 疑似データによる本人性確認・完全性保証
  - パケット長を変えないまま実現
- 他の技術と組み合わせた、IPアドレス・ポート番号の完全性保証
  - NA(P)Tの通過

PCCOM　暗号化範囲・暗号方式

暗号化範囲をあえてユーザデータ部分のみとする

→ ファイアウォールの通過

平文と暗号文をそのまま置き換え、パケット長は変化させない

→ PCCOMの処理によるフラグメントは発生しない

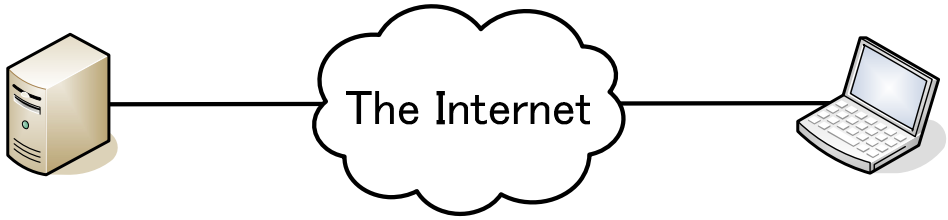
手段として・・・　任意長のデータを暗号化できる、ブロック暗号のCFBモードを利用

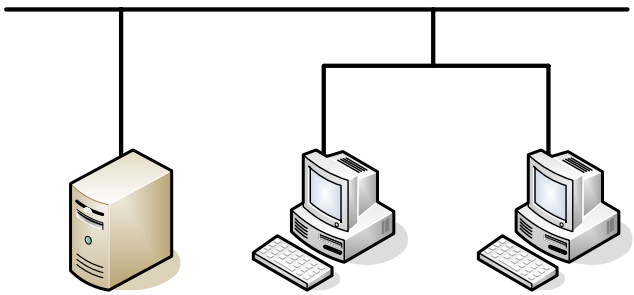
※　NA(P)Tなしのシステム　　NA(P)Tありのシステム
IPアドレス・ポート番号を含む　IPアドレス・ポート番号を含まない

システム構成によって、完全性保証に関わる処理を分ける

PCCOM　システム構成例

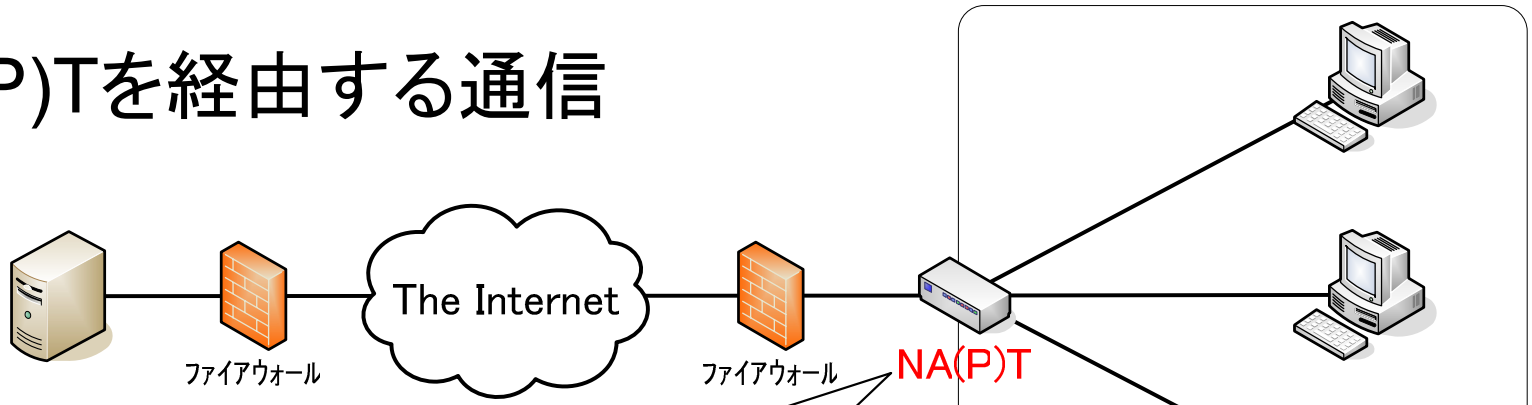
NA(P)Tを経由しない通信





本方式を独立して使用可能

NA(P)Tを経由する通信



IPアドレス・ポート番号を変換

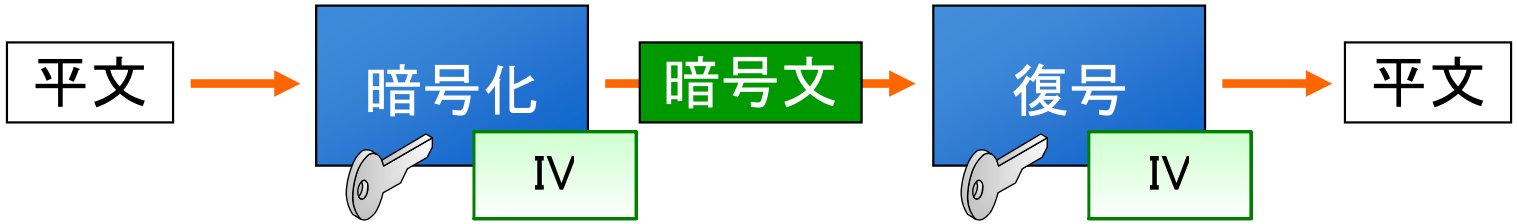
→　完全性保証の範囲から外す

他の技術との組み合わせで保証

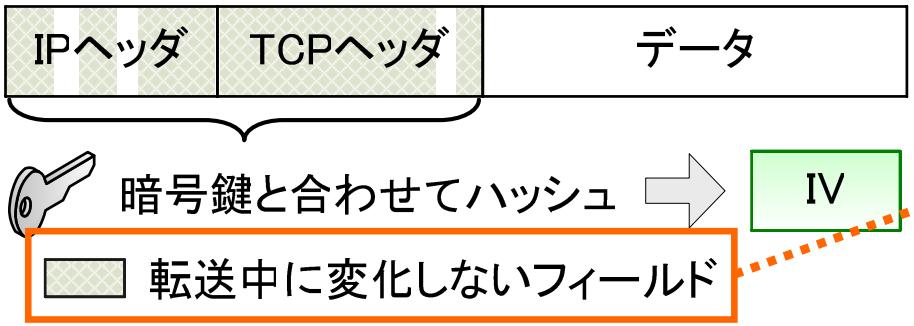
PCCOM　NA(P)Tを経由しない通信

ポイント！

- IV（Initialization Vector）の生成
  - IV とは・・・ 暗号化/復号の際に、暗号鍵とは別に必要な初期値



IVの条件
- 暗号化/復号で同じ値
- パケットごとに異なる値（セキュリティ上の問題）
- 第三者に知られない値（必須ではないが推奨）



NA(P)Tは経由しない場合なので、
IPアドレス・ポート番号を含む

→ 全ての条件を満たせる

更に・・・ 本人性確認と完全性保証の役割も果たす

PCCOM　NA(P)Tを経由しない通信

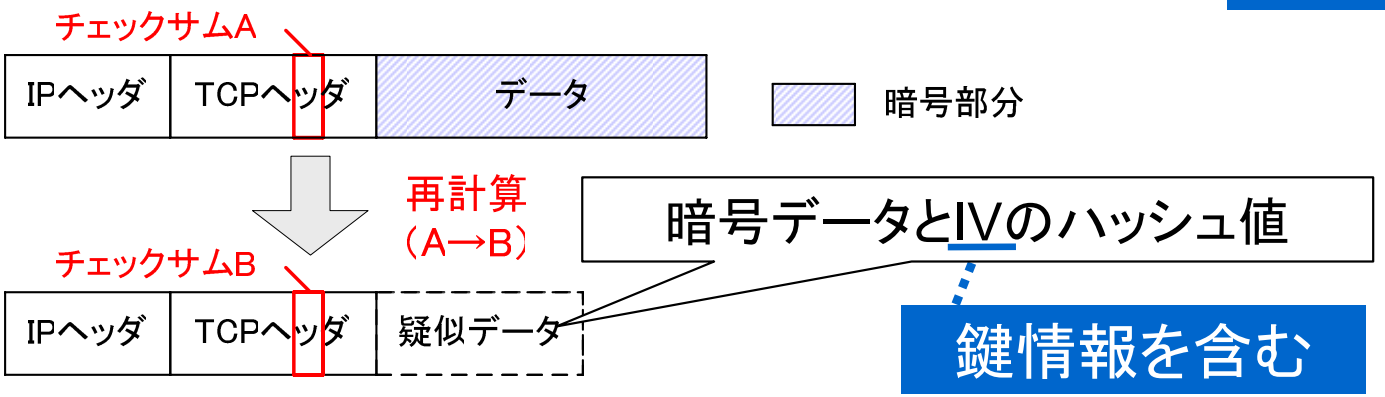
- 本人性確認とパケットの完全性保証
  - パケット長を変えないため、ヘッダの追加はしない
    → TCP/UDPチェックサムを用いる

従来の計算範囲：TCP/UDP疑似ヘッダ、TCP/UDPヘッダ、データ

暗号データとIVのハッシュ値をユーザデータと見なして、再計算/検証を行う

疑似データと呼ぶ

独自の計算方式

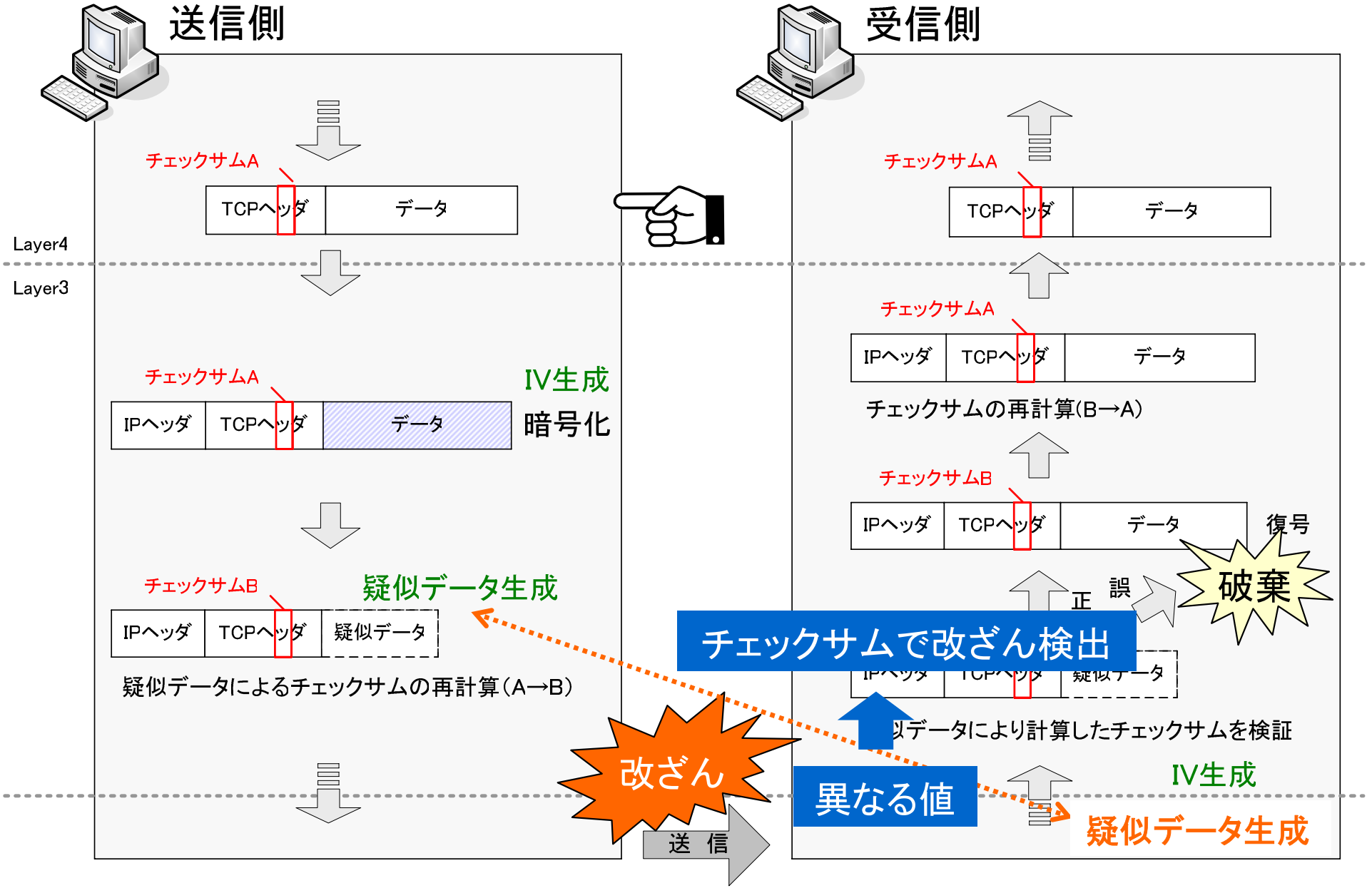


→ 暗号部分とIV生成に用いたフィールドの完全性を保証

- 疑似データによって正当な相手であることが保証される
  → 送信元の本人性確認

PCCOM　NA(P)Tを経由しない通信

- 改ざん検出の流れ



PCCOM　NA(P)Tを経由する通信

- 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
    - → IV生成の範囲から外す　**改ざんと見なされない**
  - TCP/UDPチェックサムが書き換えられる

NA(P)Tは、独自の計算（疑似データによる再計算）ができないのでは？

再計算ではなく、変換部分の差分計算を行うだけで問題ない

- IPアドレスとポート番号の完全性保証
  - → 他の技術との組み合わせで保証する

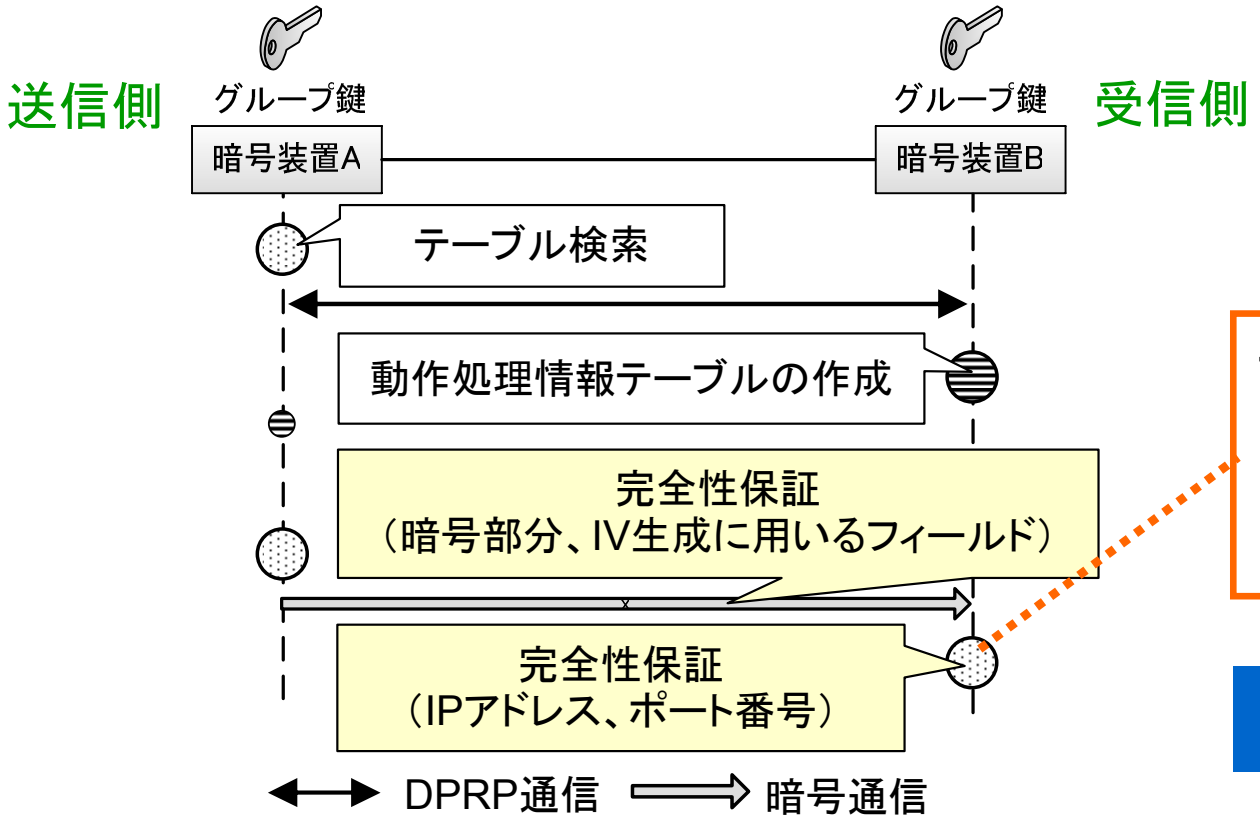
例：　**PCCOM**　＋　**DPRP**

DPRP（Dynamic Process Resolution Protocol）：

暗号通信に先立って行われる事前交渉プロトコル

DPRPと組み合わせた完全性保証

- DPRP（Dynamic Process Resolution Protocol）
  - 暗号通信に先立って暗号化/復号などの動作処理情報を記したテーブルを作成
- DPRPが作成したテーブルを基に暗号通信を行う
- 動作処理情報テーブル
  - IPアドレスとポート番号の情報
  - IPアドレスとポート番号とプロトコル番号のハッシュ値を検索キーとしてテーブル検索

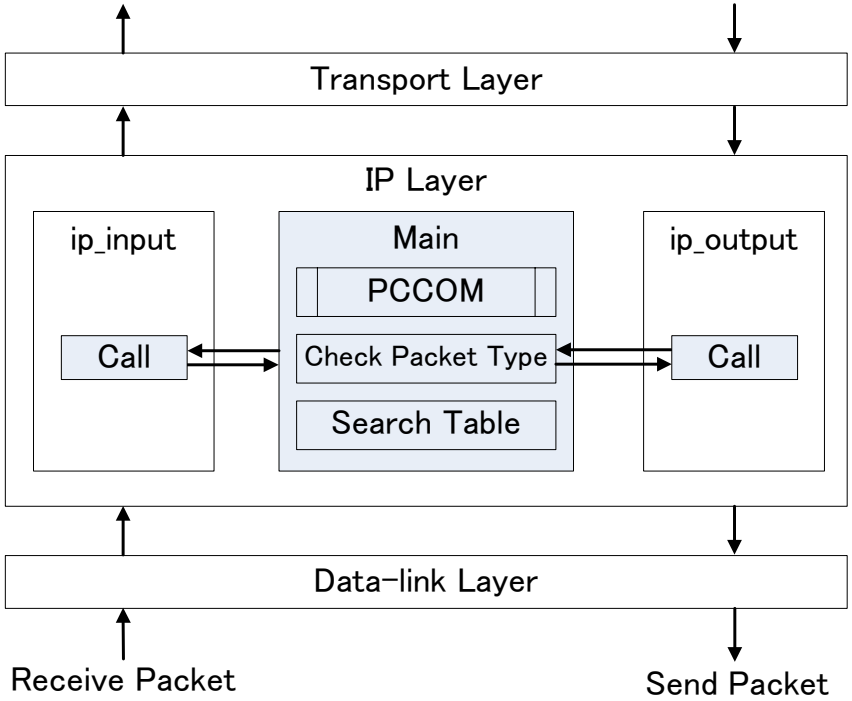


テーブル検索にヒット
→ IPアドレスとポート番は
改ざんされていなかった

DPRPは手段のひとつ

試作システムの開発

- PCCOMの有効性確認として、試作システムを開発
- 実装方式
  - FreeBSD (R 5.1) のカーネルにモジュールを組み込む
  - IP層で行われる既存の処理に一切変更を加えない
  - IP層の入出力の最適な場所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方式



試作システムの開発

- 試作システムの仕様

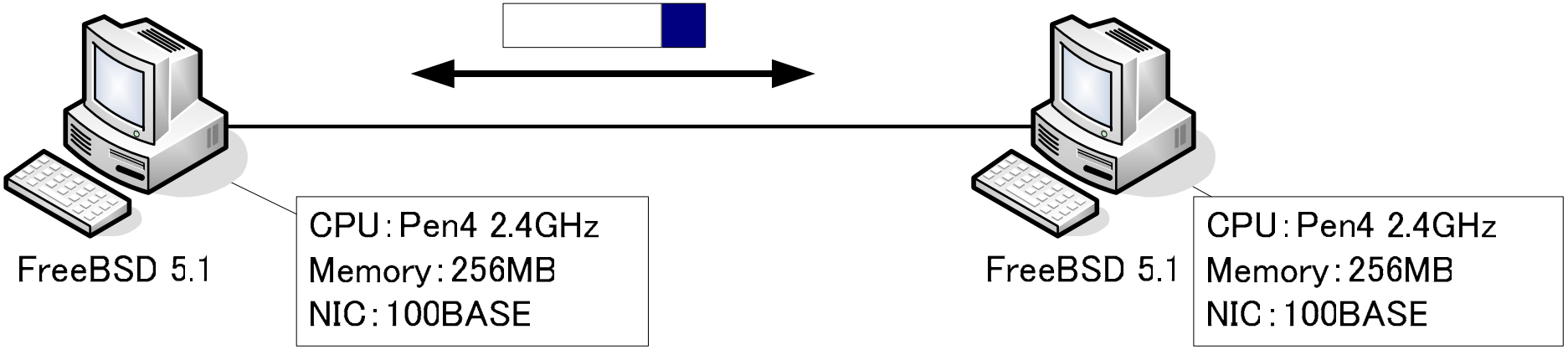
項　　目	内　　容
テーブル検索方式	ハッシュ探索（チェイン法）
暗号方式	PCCOM
暗号アルゴリズム	AES（CFBモード）※
鍵長	128ビット
ハッシュ関数	MD5 ※

※　暗号ライブラリとして openssl-0.9.7d を使用

- 端末に実装するソフトウェア型暗号装置として開発
- 暗号鍵は事前に共有
- 動作処理情報テーブルは事前に作成

試作システムによる性能評価

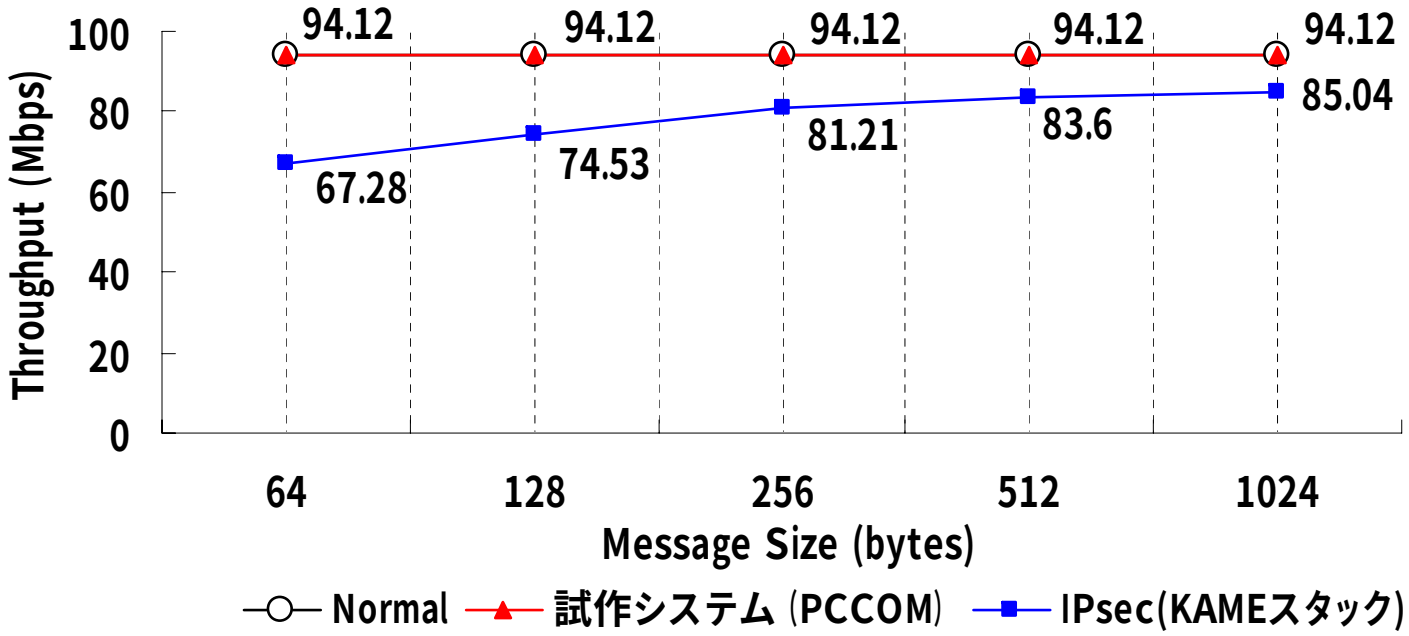
- **実験目的**
  - **試作システムとIPsec (KAMEスタック) を実装した2台の端末間の通信性能を測定し、定量評価を行う**



  - IPsecの設定
    - ESPトランスポートモード
    - **暗号アルゴリズム** ：AES (**鍵長**128**ビット**)
    - **認証アルゴリズム** ：HMAC-MD5
    - **リプレイ防御機能** ：OFF

試作システムによる性能評価

- **スループットの測定**
  - **ネットワークベンチマークソフト** Netperf **を使用**



- **考察**
  - Normal**と試作システム** (PCCOM) **は**NIC**の上限まで性能を発揮しており、性能低下は見られない**
  - **長パケットの場合、**IPsec (KAME**スタック**) **は**Normal**から約**9.7%**低下**
  - **短パケットの場合は約**28.5%**低下**

試作システムによる性能評価

- FTPによる性能測定
  - 500MBのファイルをダウンロードするのに掛かった時間を測定

項　　目	ダウンロード時間 （秒）
Normal	42.9
試作システム（PCCOM）	42.9
IPsec（KAMEスタック）	49.1

- 考察
  - Normalと試作システム（PCCOM）は同じ結果となり、性能低下は見られない
  - IPsec（KAMEスタック）は、Normalから約12.6%低下

  → 長パケットでのスループットの結果とほぼ等しい結果

比較検討

既存技術の比較

	機密性	本人性確認	完全性保証	NA(P)T	ファイアウォール	フラグメント
IPsec ESP	◎	◎	◎	△	△	×
PCCOM	○	○	○	○	○	○

- IPsec ESP
  - TCP/UDPヘッダを暗号化・完全性保証の範囲に含めている
    - → NA(P)Tやファイアウォールを通過できない

  “UDP Encapsulation of IPsec Packets” インターネットドラフト
  カプセル部分は完全性保証の範囲ではない
  - ヘッダの追加によるオーバヘッドやフラグメントの発生
- PCCOM
  - TCP/UDPヘッダを暗号化範囲に含めない代わりに
    - → NA(P)Tやファイアウォールを通過できる
  - パケット長が変化しないため、PCCOMの処理によるフラグメントは発生しない

むすび

- まとめ
  - 実用性を重視した暗号通信方式 PCCOM
    - NA(P)T、ファイアウォールを通過できる
    - パケット長を変えないまま本人性確認と完全性保証も行える
  - 試作システムの性能評価
    - 100BASEの環境において、上限まで性能を発揮

IPsec　強力なセキュリティ　但し、既存システムとの相性などに十分注意

PCCOM　既存システムに影響を与えないので比較的容易に導入できる

- 今後の課題
  - ギガビットイーサを用いた、より精度の高い測定
  - 端末同士ではなく、通信径路上でPCCOM、IPsecの処理をした場合の性能測定と評価

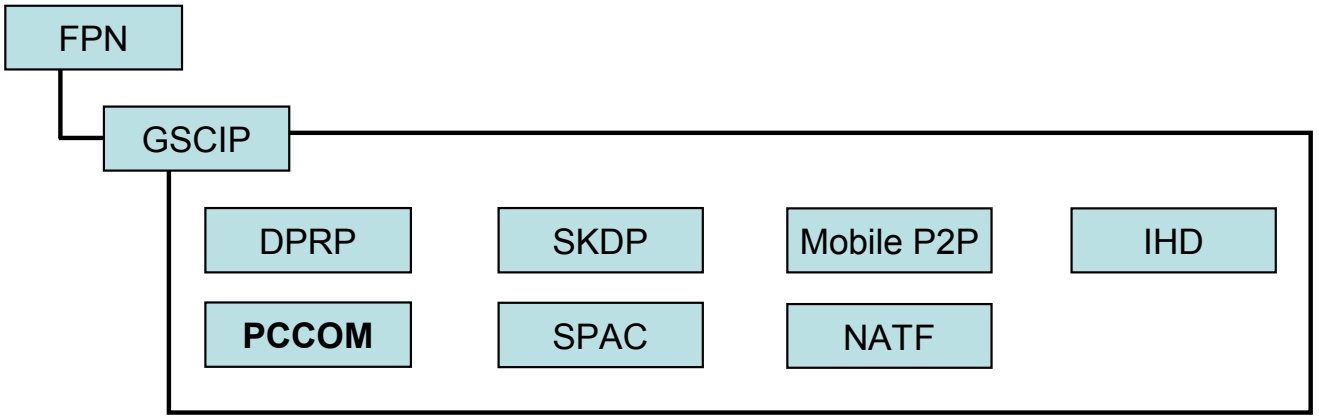
お わ り

※ 本研究は柏森財団の助成を受けて実施したものである

補足資料　INDEX

GSCIPとは

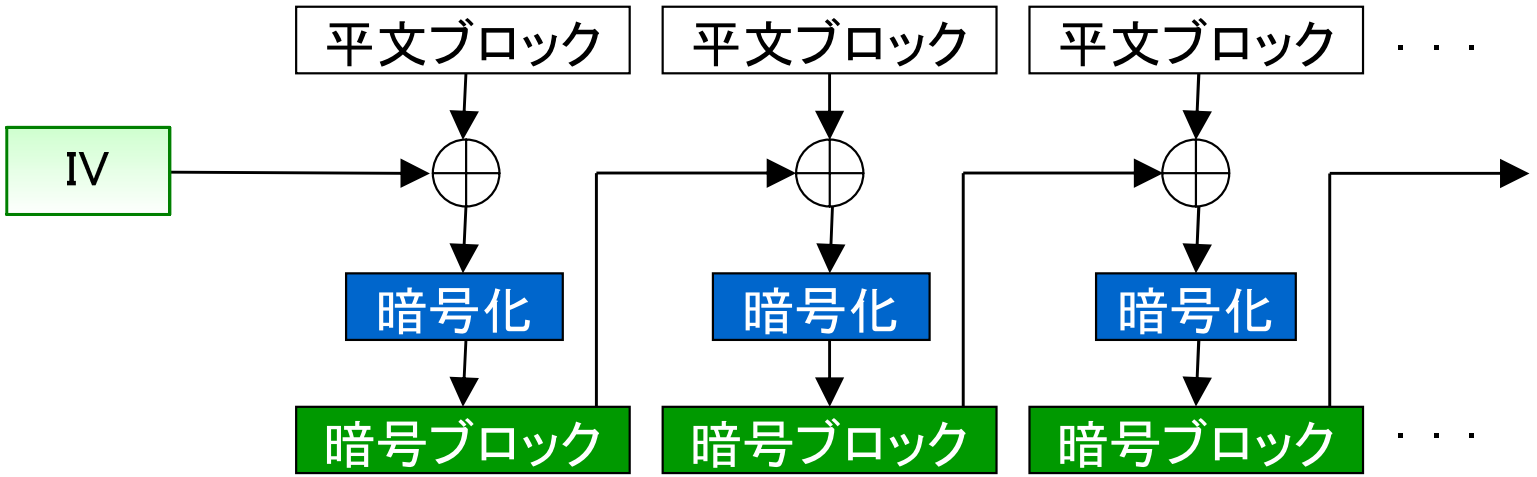
- GSCIP（Grouped Secure Communication for Internet Protocol；ジースキップ）
  - FPN（Flexible Private Network）を実現するためのネットワークセキュリティアーキテクチャ
  - FPN
    - セキュリティと管理負荷軽減の両立が可能なシステム
    - 閉域通信グループの構築
    - DPRPによるアクセス許可と自動設定
    - ユーザの物理的位置透過性の保証



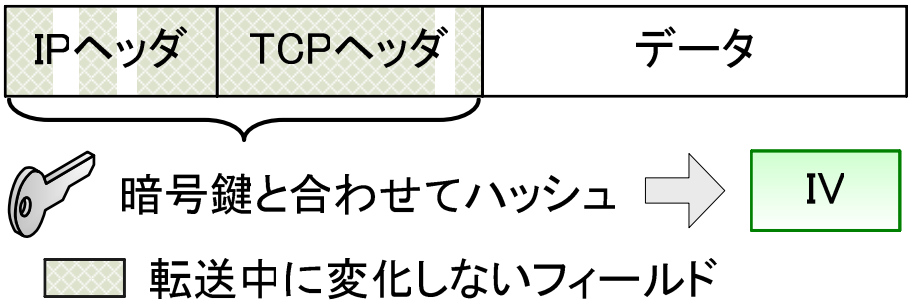
DPRP：Dynamic Process Resolution Protocol
PCCOM：Practical Cipher COMmunication protocol
SKDP：Secure Key Distribution Protocol
SPAC：Secure Protocol for Authentication with IC Card
Mobile P2P
NATF：NAT Free protocol
IHD ：”Island Hop” Detection system

IV（Initialization Vector）の詳細

- IVとは
  - ブロック暗号のCFBモードなどで必要
  - 暗号化、復号の際に、暗号鍵とは別に必要となる初期値
    - 暗号化/復号で同じ値
    - パケットごとに異なる値（セキュリティ上の問題）
    - 第三者に知られない値（必須ではないが推奨）
  - ブロックサイズと同じ大きさ



IVの3つの条件を満たす理由

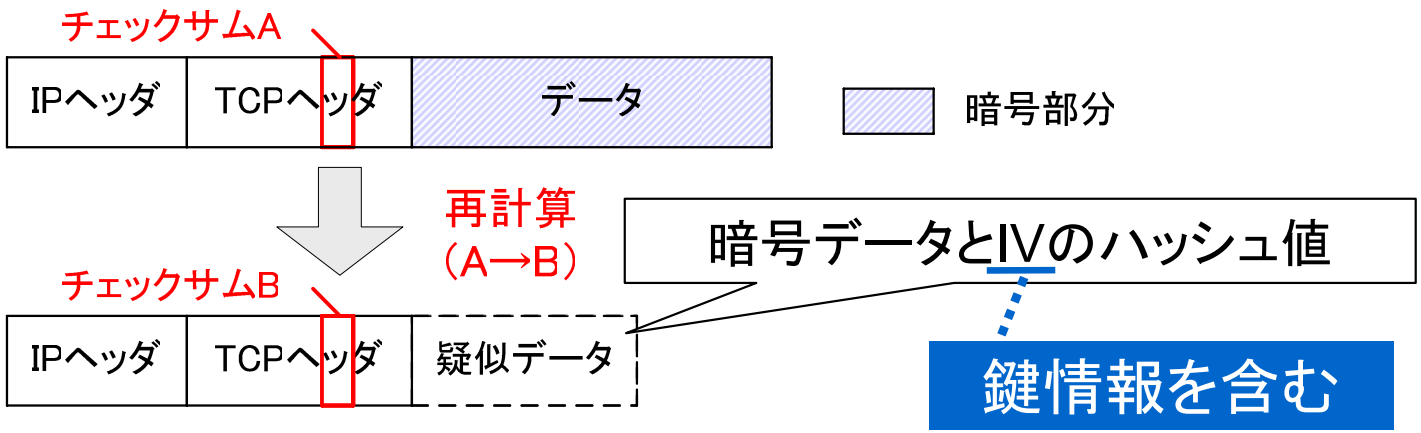


→ 全ての条件を満たせる

IVの条件

- 暗号化/復号で同じ値
  - → 同じメッセージからIVを生成しているため
    - 転送中に変化しないフィールド、暗号鍵
- パケットごとに異なる値（セキュリティ上の問題）
  - → IPヘッダのIDフィールドなどを含むため
    - フラグメントの復元に用いる識別子　通常は1ずつ加算
- 第三者に知られない値（必須ではないが推奨）
  - → 互いに共有している鍵情報を含めているため

疑似データを含めたチェックサムの再計算/検証の詳細



→ 暗号部分とIV生成に用いたフィールドの完全性を保証

- 暗号部分

  暗号部分は疑似データ生成の範囲

  → 改ざんされると、受信側で生成する疑似データは異なる値となり、チェックサムで改ざんが検出される

- IV生成に用いたフィールド

  IVは疑似データ生成の範囲

  → 改ざんされると、IVは異なる値となるので疑似データも異なる値となり、チェックサムで改ざんが検出される

CFBモードを採用した理由

- CFBモード
  - 任意長のデータを暗号化できるモードで、ストリーム暗号としての役割を果たす
- ストリーム暗号にはRC4などが挙げられるが、CFBモードを採用した理由は？
  - パケットの完全性保証にIVを用いる
    - IVはブロック暗号のCFBモードなどで必要となる初期値
  - 実装上ブロック暗号の方が普及しており利用しやすい
  - 類似モードにOFBモードがあるが、セキュリティの面でCFBの方が強力と言われている

DPRPとNA(P)T

- 現在のDPRPはNA(P)Tを通過できない
  - 解決策 ：NATF（NAT Free protocol）の適用
    - NATF・・・アドレス空間の違いを意識しないで通信可能

- 本提案は、他の技術との組み合わせによるIPアドレスとポート番号の完全性保証
  - 従来の完全性保証
    - 認証値の計算に、IPアドレス・ポート番号を含める

    → NA(P)Tを通過できない
  - 提案方式
    - 他の技術、例えばDPRPと組み合わせることで完全性を保証

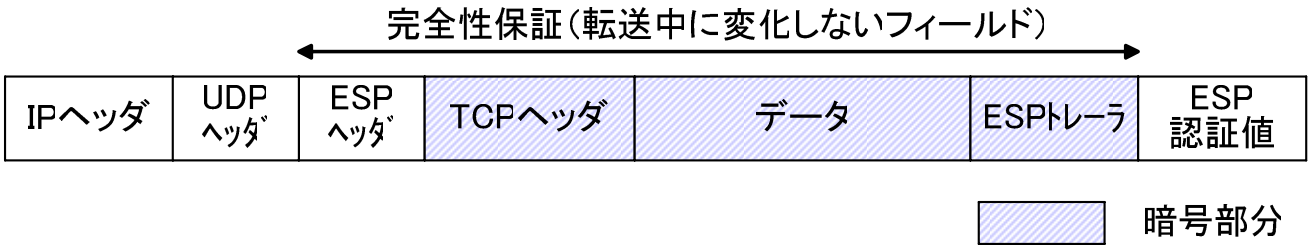
他の技術との組み合わせによる保証

- 他の技術との組み合わせ
  - 例えば DPRP

- 他には？
  - IKE（Internet Key Exchange）
    - SAの自動生成
    - セキュリティポリシの設定（手動）で、IPアドレス・ポート番号を指定
    - セレクタで、IPアドレス・ポート番号・プロトコル番号を選択基準に入れる

IPsec　NA(P)T・FWの対策

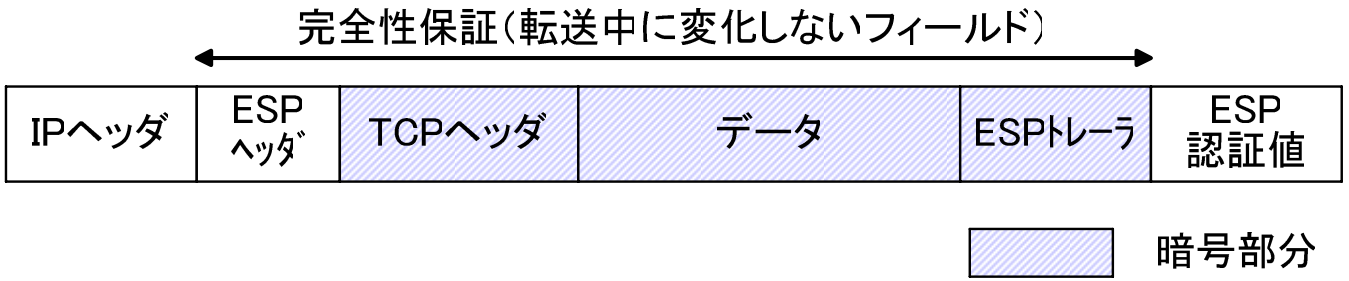
- NA(P)T
  - “UDP Encapsulation of IPsec Packets”
    - 相互で対応していることが前提
    - UDPポートは500番の場合が多く、FWでポート番号を制限している環境では利用が困難
    - カプセル部分は完全性保証の範囲ではない
    - ヘッダの追加によるオーバヘッドやフラグメントの発生



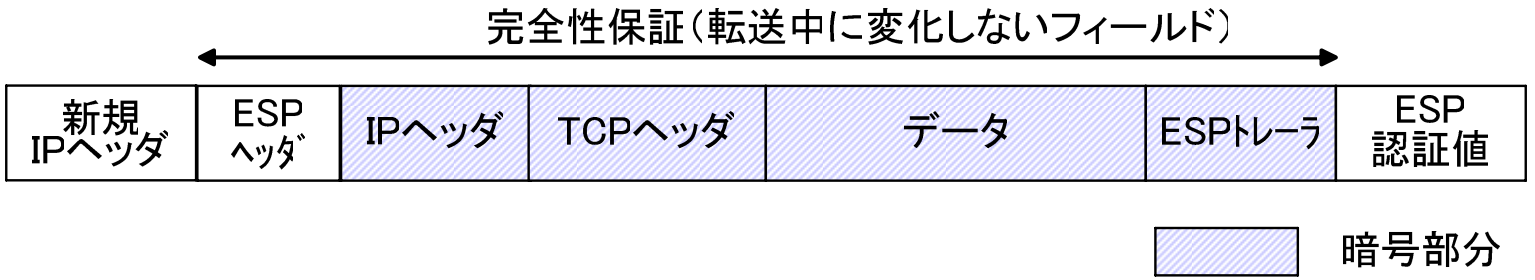
- FW
  - FWを経由するIPsec通信を避ける
    - End-to-EndのIPsec通信ではない（主にSGW間のVPNに使われる）
  - SGW（IPsecゲートウェイ）と並列に設置する
    - 用途に応じた経路設定が必要
    - 一般的のこの方法が多い
    - End-to-EndのIPsec通信ではない

IPsec トランスポートモードとトンネルモード

- IPsec ESP　トランスポートモード
  - 主にEnd-to-Endの通信で利用



- IPsec ESP　トンネルモード
  - 主にSGW間の通信で利用



IPsec トランスポートモードとトンネルモード

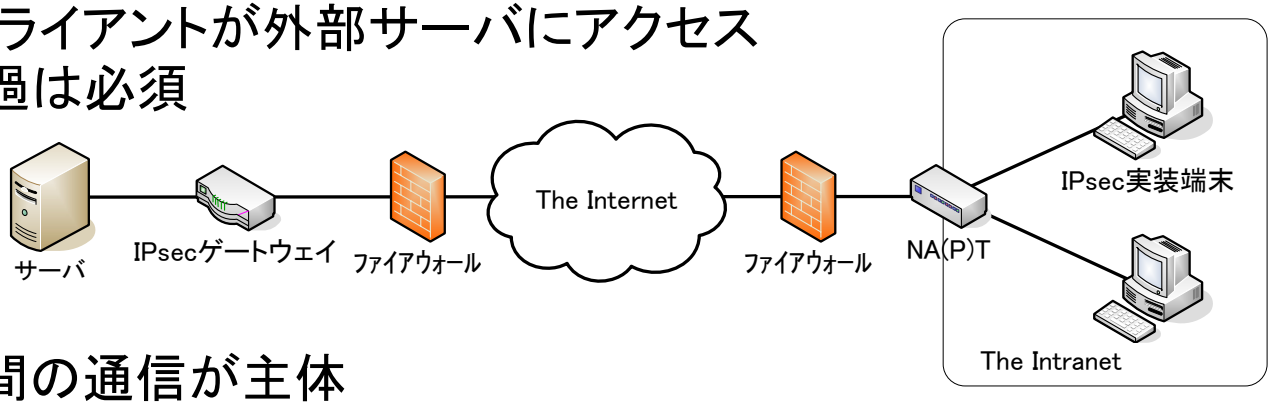
WWWを代表とするクライアント/サーバシステム

IPsecを適用する場合、サーバ側にはIPsecゲートウェイを設置

→ トンネルモードを使用

プライベートアドレスのクライアントが外部サーバにアクセス

→ NA(P)T、FWの通過は必須



P2Pネットワーク ・・・ 個人間の通信が主体

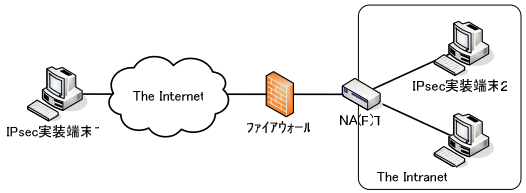
IPsecを適用する場合、End-to-Endであるトランスポートの利用が望ましい

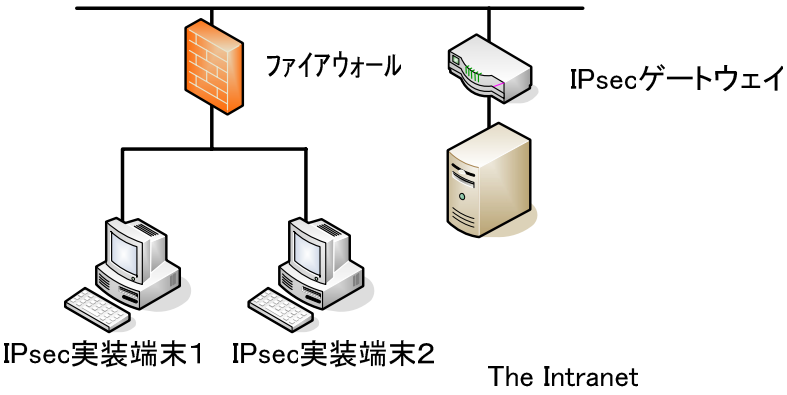
→ NA(P)T、FWの経由は十分にあり得る

イントラネットでIPsecを適用 ・・・ トンネルモードとの併用が考えられる

企業ネットワーク： 部門間にFWを設置することが多い

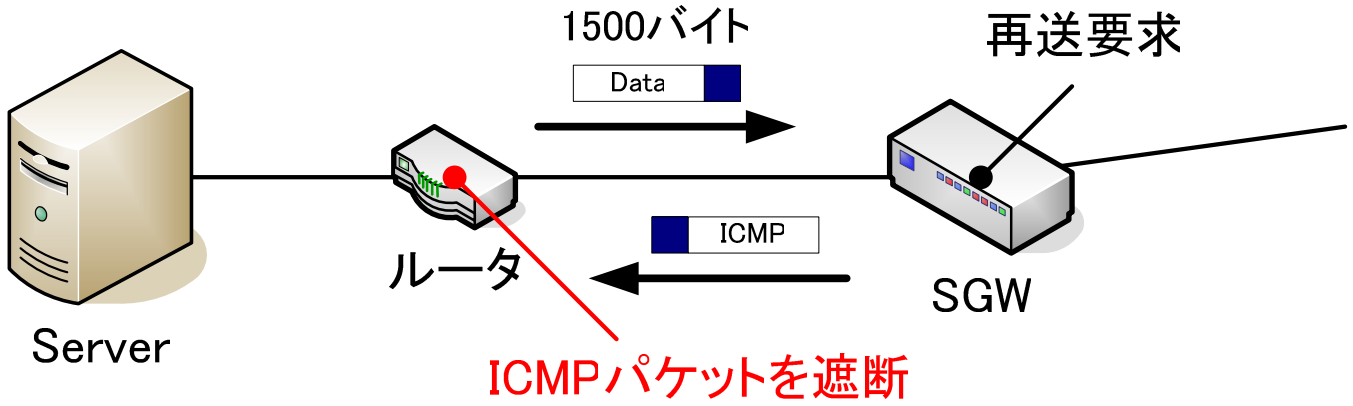
→ FWの通過は必須





IPsec フラグメント問題

- SGWでIPsec処理を行う場合
  - ヘッダの追加により、パケット長が1500バイトを超える
    → 1500バイト以下になるように再送要求
  - 途中経路でルータがあり、ルータがICMPパケットを通さない設定にしている場合に問題



  - ICMPパケットを通すようにルータの設定をする
    - 管理外のルータは設定できない
  - 強制的にSGWでパケットを分割する方式
    - 伝送効率の低下
    - SGWの負荷

TCP/UDPヘッダが平文であることの考察

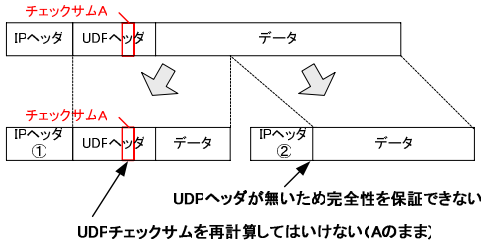
- TCPヘッダ
  - ポート番号とシーケンス番号がセキュリティ上重要な情報
    - ポート番号
      - アプリケーションの推測の可能性
        - → 実際はFWで使用できるポート番号は制限されており、それ自体がプレイバシーの侵害などになるとは考えにくい
    - シーケンス番号
      - TCPシーケンス番号の不整合を利用したハイジャック
        - → 送信元の本人性確認を行うため、この手段は取れない
- UDPヘッダ
  - ポート番号がセキュリティ上重要な情報
    - TCPポート番号と同様

TCP/UDPチェックサムのフィールド長16ビット

- 提案方式では、TCP/UDPチェックサムが認証値
  - フィールド長16ビットでは足りないのでは
    - TCP/UDPチェックサムそのものは、第三者は知ることができない疑似データを含めたチェックサムの計算値
      → この値から中身を推測することはできない
    - 問題となるのはチェックサムの衝突（重複）
      - 16ビット長　：　65,536通り
      - チェックサムの値65,536通りのパケットを順に送りつければ、やがて正しい値に辿り着く
      - 大量にパケットを送りつけて、不正パケットを通過させる攻撃法
        » ログを見る等で対処できそうだが、今後検討していく必要がある

UDPパケットにおけるフラブメントの扱い

- 提案方式では、分割されたUDPパケットを扱うことができない
  - フラグメントによってUDPヘッダの情報が変わることはない
    → UDPチェックサムを再計算してしまうと，元のチェックサムには戻せなくなる（フラグメントパケットの再組み立て後に再計算すれば別）
  - 分割パケットの先頭以外は、UDPヘッダがない
    → UDPチェックサムを用いた本人性確認・完全性保証ができない



- 対策案
  - フラグメントパケットは扱わない（分割前に送信側処理、結合後に受信側処理）
  - IP層から呼び出す手順を変える
  - UDPパケットは、復号後にOSが行うチェックサムの検証を利用する
  - TCP/UDPチェックサムの代わりにIPチェックサムを用いる

リプレイ攻撃に対する検討

- 復号処理負荷を狙った攻撃を考慮する必要性
  - 正常なパケットは当然ながら復号される
    - → クラッカーが正常なパケットを盗み取ってそのパケットのコピーを大量に送信するリプレイ攻撃を行った場合が問題
- 対策案
  - TCPのシーケンス番号を用いる方法
    - IPsecのシーケンス番号のように1ずつ加算するのではなく、送信したデータのオクテット数だけ値が加算される
      - → IPsecのように既に受信したパケットより大幅に小さい番号を不正と見なすことはできない
- この問題には何らかの対策が必要
  - 今後検討していく