IPv4/IPv6 混在環境における暗号通信方式の考察

増田　真也　　鈴木　秀和　　渡邊　晃
名城大学大学院理工学研究科

A study on cipher communication system for mixture environment of IPv4/IPv6

Shinya Masuda　Hidekazu Suzuki　Akira Watanabe
Graduate School of Science and Technology, Meijo University

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，普及が進んでないのが現状である．このことから，既存システム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．

一方，ユビキタス社会の実現に向けて IPv6 のインフラ整備が進められている．しかし，企業ネットワークなどは IPv4 のインフラやアプリケーションが確立されており，IPv6 への移行には時間を要する．そのため，デュアルスタックによる IPv4/IPv6 の混在環境が暫く続くことになると考えられる．このような混在環境では，IPv4 のプライベートアドレスは当分の間使われ続けるため，NA(P)T の存在を無視することはできない．従って，NA(P)T との親和性が高い通信方式が求められる．

既存のネットワークセキュリティ技術の代表として IPsec[1)~4)]が挙げられる．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．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．そのため IPsec は NA(P)T やファイアウォールを経由する環境ではほとんど利用されていないのが現状である．尚，TCP/UDP ヘッダの情報を ESPQ（ESP considered QoS）ヘッダと呼ばれるヘッダの先頭に格納し，QoS 制御を行えるようにする ESPQ[5)] や，ESP の暗号化を階層化し，一部のヘッダの内容をルータ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，NA(P)T との相性の悪さや，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課題は解決されていない．

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との相性がよいこと，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）[7,8)]を提案し，検討を行ってきた．PCCOM は本人性確認とパケット全体の完全性保証を，共通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 チェックサムを新たに再計算することにより実現する．この方法では NA(P)T やファイアウォールとの相性が良く，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．PCCOM では，暗号化範囲はファイアウォールを通過するためにユーザデータ部分のみとしているが，パケット全体の完全性保証を実現しているため，必要最低限のセキュリティレベルを保っている．尚，PCCOM は事前に共通暗号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既に保持していることを前提としている．

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おり，P2P 通信やホームネットワーク，イントラネットなどの環境に適した方式として有効と考えられる．PCCOM の考え方は IPv4/IPv6 のどちらにも適用可能である．本稿では，PCCOM を IPv6 に適用した場合について述べ，IPv4/IPv6 の混在環境での有効性を評価する．

以降，2 章で IPsec とその制約，3 章で PCCOM，4 章で IPv4/IPv6 の混在環境における考察，5 章でまとめと今後の課題について述べる．

2.　IPsec 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 IPv4，IPv6 それぞれにつき図 1 に示す．IPv6 では ESP ヘッダは IPv6 拡張ヘッダとして定義されており，IP ヘッダとペイロードの間に拡張ヘッダと終点オプションヘッダが挿入される場合は終点オプションヘッダの前に ESP ヘッダを挿入するが，基本的には IPv4 と相違はない．

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．ESP トレーラは，ブロック暗号のブロック

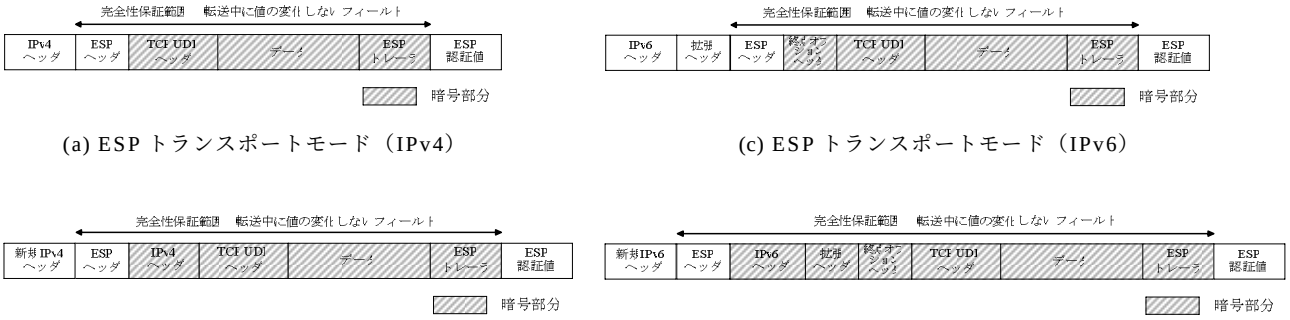


図 1　IPsec ESP のパケットフォーマット

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 認証値としてパケットの末尾に付加する．ESP は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 アドレスの変換を伴う NA(P)T 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．UDP ヘッダで ESP をカプセル化することで NA(P)T を通過させる方法（UDP Encapsulation of IPsec Packets）が提案されているが [9]，カプセル部分は完全性保証の範囲に含まれず，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課題がある．

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，ESP ヘッダから ESP トレーラまでのデータの完全性を保証する．しかし，トランスポートモードと同様にポート番号が暗号化されているため，ファイアウォールを通過しようとすると拒絶される場合が多い．トンネルモードにおいては，IP ペイロードにアドレスに依存したデータが存在しない場合には NAT を通過することは可能であるが，ポート番号の変換も伴う NAPT (IP マスカレード)は通過できない．更に，トンネルモードの場合

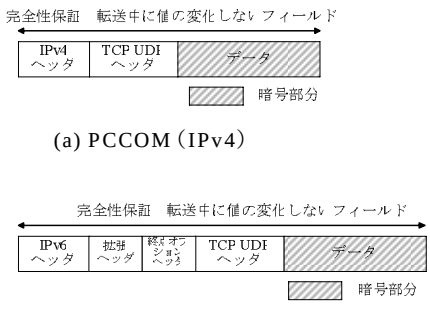


図 2　PCCOM のパケットフォーマット

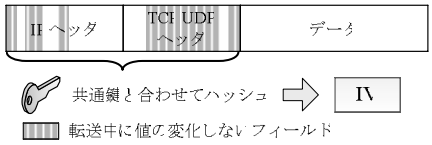


図 3　IV (Initialization Vector) の生成

は IP によるカプセル化を行うので，トランスポートモードに比べオーバヘッドが大きい．

また，いずれのモードも TCP/UDP ヘッダの情報は暗号化されるため，上位層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． IPsec のセキュリティ強度は強靭であるが，パケットフォーマットが変えられるため，新システムの設計・構築では IPsec との相性を考慮したり，IPsec を導入する際にスループットの低下を考慮したりする必要があるなどの弊害が生じる．

3.　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．

3.1.　実現方式

IPv4，IPv6 それぞれにおける PCCOM のパケットフォーマットを図 2 に示す．PCOOM 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全体の完全性保証を実現する．PCCOM では，共通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．尚，IPv6 では IP ヘッダとペイロードの間に拡張ヘッダと終点オプションヘッダが挿入される場合があるが，基本的には IPv4 と相違はない．

PCCOM では本人性確認と完全性保証を実現するために，まず IV（Initialization Vector）と呼ぶ初期値を定義する．図 3 に IV の生成方法を示す．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 の網掛け部分）と，事前に秘密裏に共有している共通鍵を含めた値からハッシュ値を求め，これを IV とする．IV の種として共通鍵を含

図 4　IV 生成に用いるフィールド

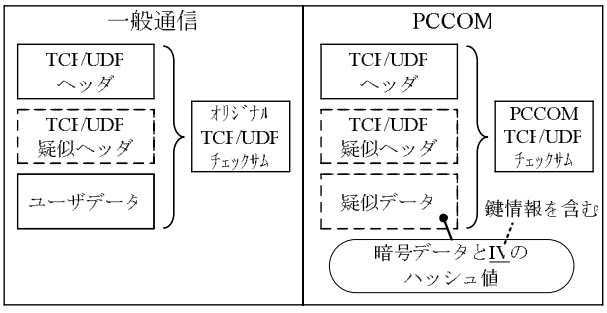


図 5　チェックサム計算範囲の違い

めているため，第三者に IV が知られることはない．更に，シーケンス番号のようにパケットごとに必ず値が変化するフィールドを含むため IV の値を第三者が推測するのは極めて困難である．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．

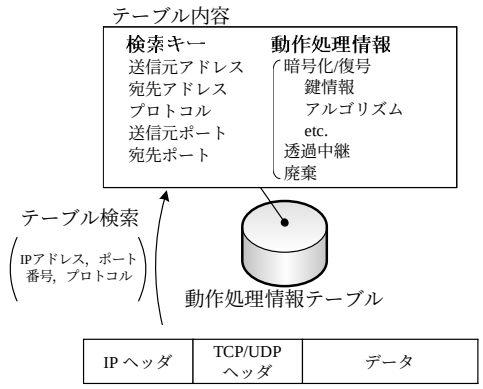


図 6　テーブル検索処理

オリジナルと PCCOM の，TCP/UDP チェックサムの計算範囲の違いを図 5 に示す．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が，PCCOM では IV をチェックサムの計算に含めて再計算する．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 5 において疑似データとは，暗号化後のデータと 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．尚，IP アドレスとポート番号は NA(P)T にて変換されるので IV 生成の範囲に含めない．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する．

上記の演算方式によると，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 [10]，受信側で行うチェックサムの検証には影響を与えない．ここで，パケットの暗号化範囲はユーザデータ部分のみとする．すなわち，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 ヘッダは平文のままとする．これは，PCCOM では本人性確認とパケットの完全性保証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と判断できるためである．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と考えられる．

PCCOM の暗号化では，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，IPsec などに見られるように暗号化によってパケット長が変化することがなく，フラグメントの発生を懸念する必要がない．

3.2. IP アドレス・ポート番号の保証

前節のように, IP アドレスとポート番号は NA(P)T を経由する際に値が変化するため 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 6 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．

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]などを流用する方式が考えられる．

4. IPv4/IPv6 の混在環境における考察

IPv4/IPv6 が混在する環境では，NA(P)T の存在は無視できない．本方式によると，IPv4 環境において NA(P)T によって IP アドレス，ポート番号の変換とチェックサムの書き換えが行われても，パケットの完全性を保証したまま通信を行うことができる．これは，IPv4/IPv6 の混在環境において有効と考えられる．また，パケットフォーマットを変えないため新たな技術の出現にも影響が少なく, IPv6 への移行に対応しやすいと考えられる．

このように，PCCOM は IPv4/IPv6 の混在環境と親和性が高く，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．

5. まとめ

本稿では実用暗号通信 PCCOM を IPv6 に適用した場合について述べ，IPv4/IPv6 の混在環境での有効性を評価した．PCCOM は NA(P)T などの既存システムに影響を与えず，新たな技術の出現にも影響が少ないため, IPv6 への移行に対応しやすいと考えられる．とりわけ企業ネットワークでは，IPv4 のインフラやアプリケーションが確立されており, IPv6 への移行には時間を要する上，部門ごとにファイアウォールが設置されている場合が多いことから，イントラネットのセキュリティ技術として有効な方式と考えられる．

今後は，リプレイ攻撃への対策などについて検討する予定である．

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) 白石 善明，福田 洋治，森井 昌克, “ ネットワークのサービス品質管理を容易化するセキュリティプロトコルの一方式 ”，信学論(D-I), vol.J85-D-I, no.7, pp.614-625, Jul 2002.
6) Y. Zhang and B. Singh, “A Multi-Layer IPsec Protocol”, Proc. 9th USENIX Security Symposium, Aug 2000.
7) 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.
8) 増田真也，渡邊晃, “ 実用暗号通信 PCCOM の実装と評価 ”，情処研法，2004-CSEC-28，pp.205-210，Mar. 2005.
9) A. Huttunen, B. Swander, V. Volpe, L. Diburro, and M. Stenberg, “UDP Encapsulation of IPsec Packets”, RFC3948, Jan. 2005.
10) K. Egevang and P. Francis, “The IP Network Address Translator (NAT)”, RFC1631 May. 1994”.

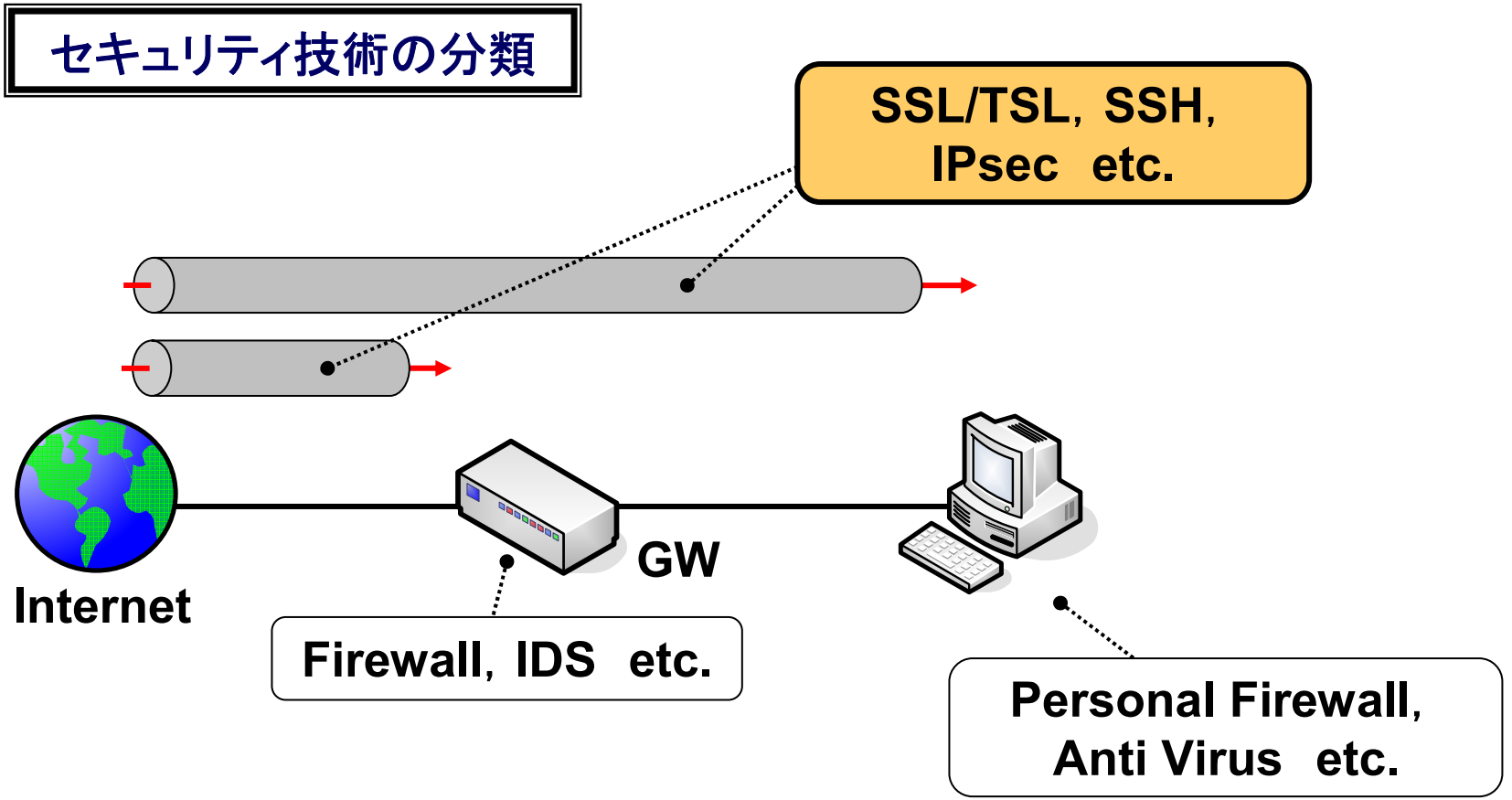
IPv4/IPv6混在環境における暗号通信方式の考察

名城大学大学院理工学研究科
増田 真也, 鈴木 秀和, 渡邊 晃

名城大学

はじめに

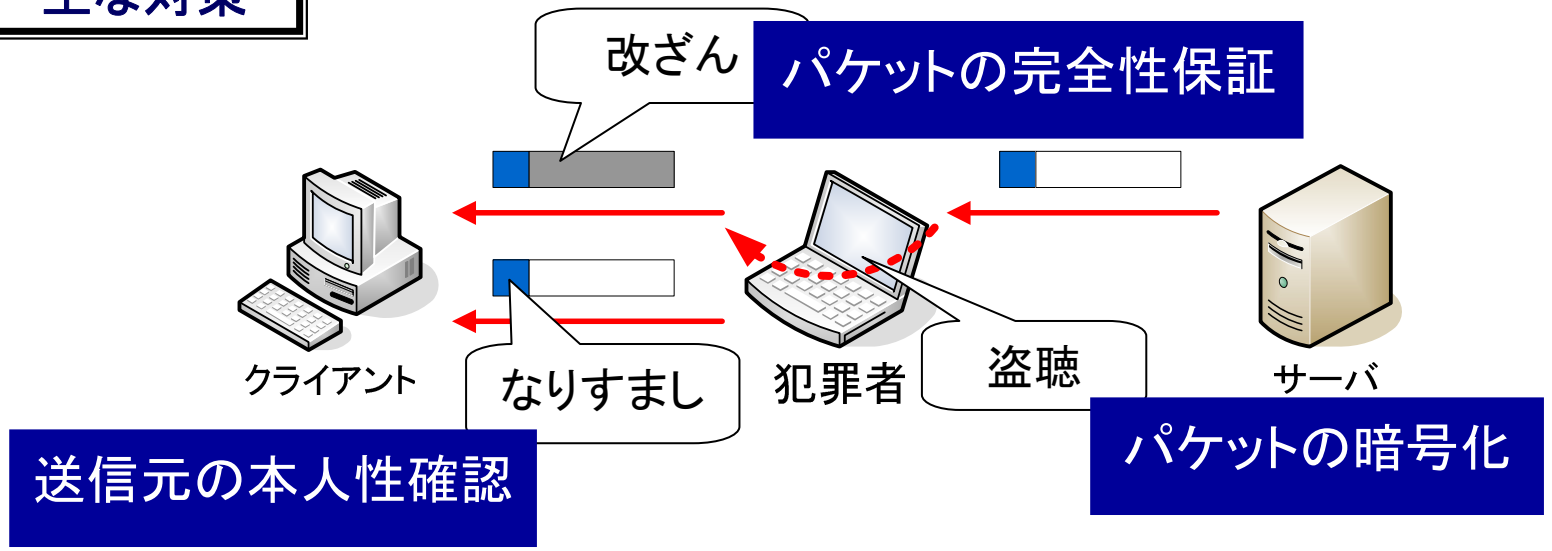
- ネットワークにおけるセキュリティ上の脅威
  → セキュリティ技術の重要性



はじめに

- 通信間を保護する技術

主な対策



分 類

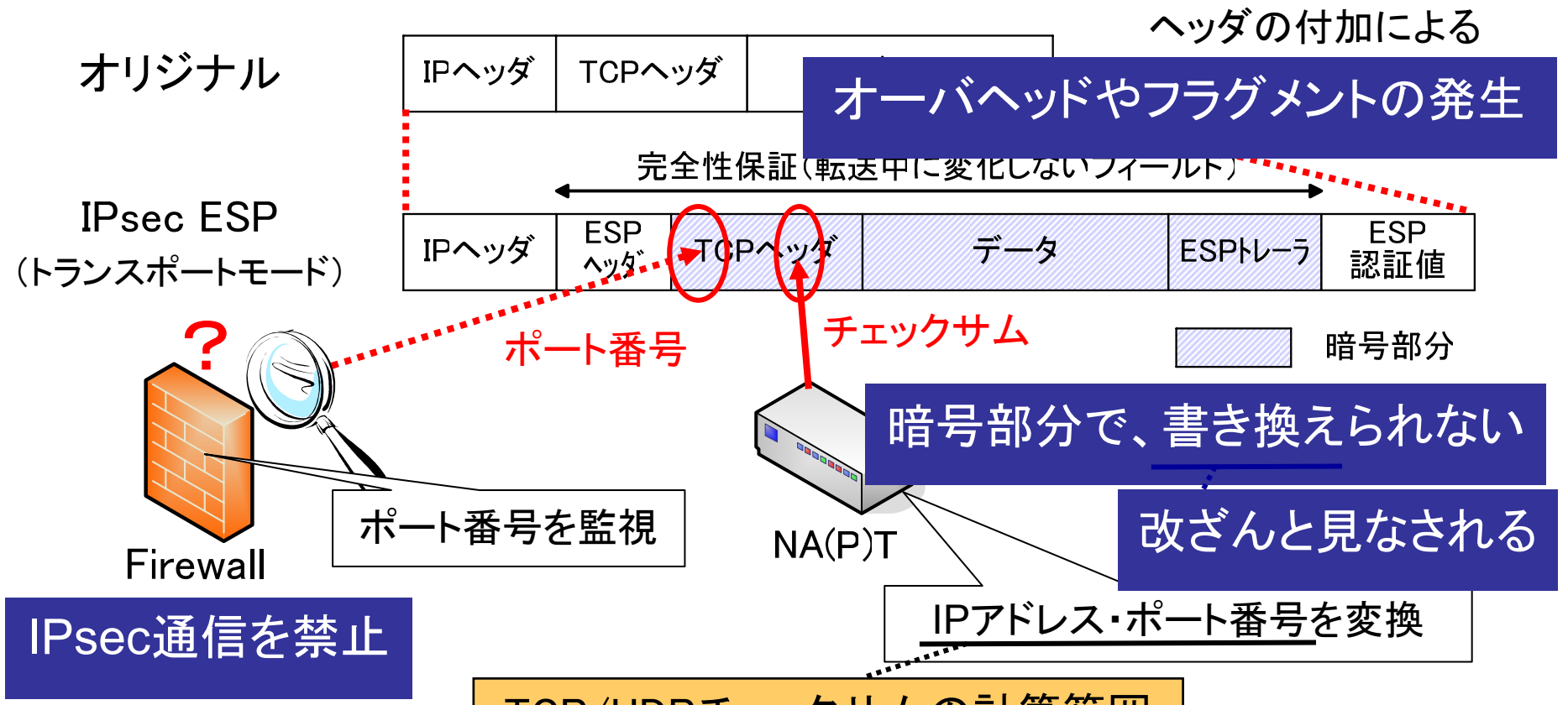
- SSL/TSL，SSH　etc.（レイヤ4以上）
- IPsec　etc.（レイヤ3）

アプリケーションに依存することなく安全を確保

IPsec ESP

既存技術

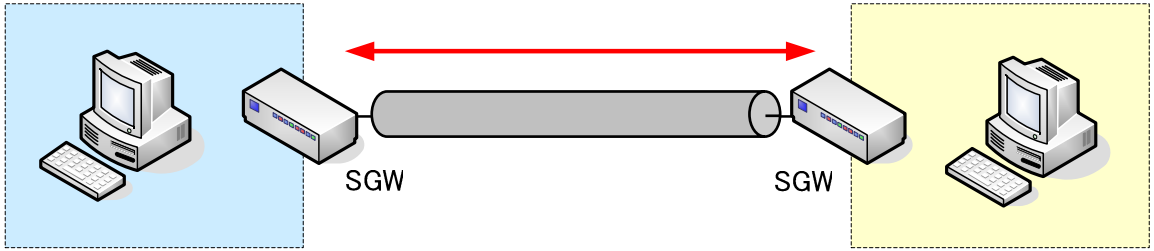
- 既存のネットワークセキュリティ技術
  - IPsec ・・・ IP層の技術で，強力なセキュリティを提供
    - IPsec ESP（Encapsulation Security Payload）・・・暗号通信方式について規定



→ 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

IPsec ESP

主な用途



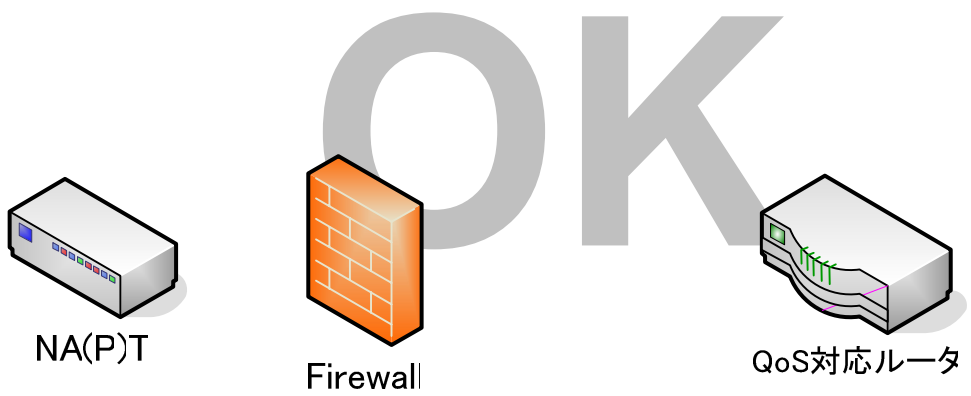
インターネットVPN

- インターネットVPN
  - Gateway-to-Gatewayでトンネルモードを適用

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相性の悪さに起因

補完技術の必要性



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

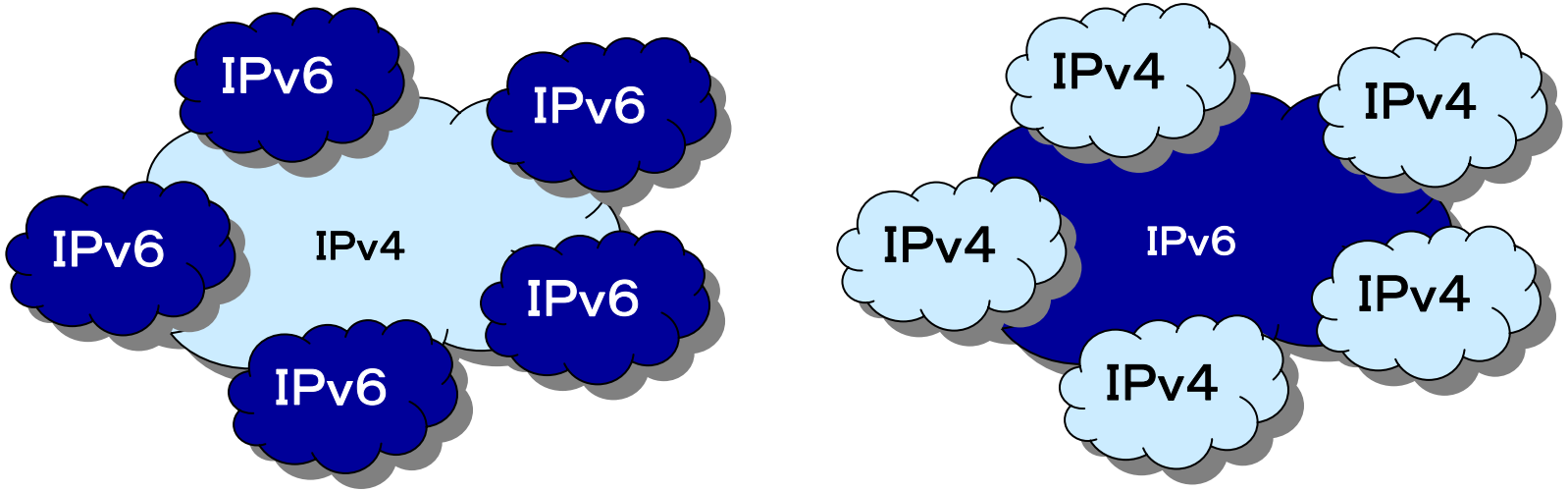
セキュリティ強度 ⟷ 実用度（柔軟性・利便性）

利用形態に適した方式を
検討することが重要

- ✓ 企業間を結ぶ通信
- ✓ 重要サーバとの通信
- ✓ 一般端末との通信　　etc.

IPv6化とNA(P)T

- IPv6への移行



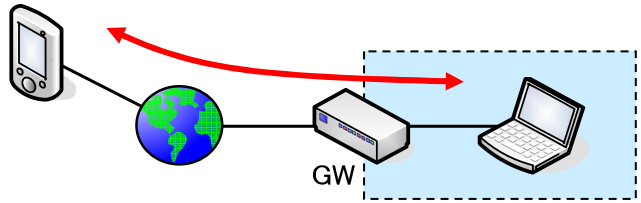
  - デュアルスタックによるIPv4/IPv6混在環境が暫く続く
    - → NA(P)Tの存在を無視できない
    - → NA(P)Tとの親和性は依然として重要な項目

PCCOM

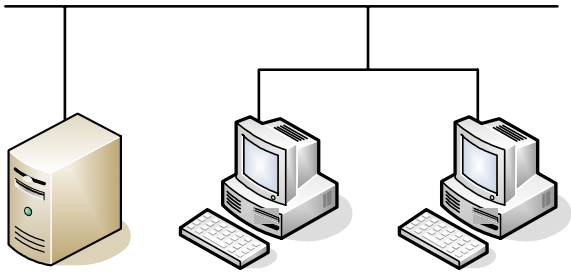
提案方式

- PCCOM（Practical Cipher COMmunication）
  - 必要最低限のセキュリティ
  - 既存システムにほとんど影響を与えない
  - 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

多様な利用形態への対応が求められる一般端末

本発表　・PCCOMのIPv6検討

・IPv4/IPv6混在環境での有効性を評価

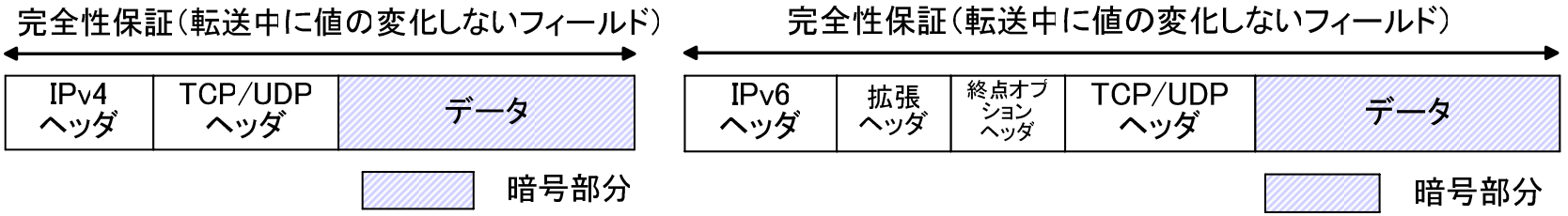
PCCOMの原理 ―特 徴―

特 徴

- パケットフォーマットを変えない
- 完全性保証・本人性確認

  IV情報を含めた疑似データと呼ぶ値を用いて実現

- ユーザデータのみを暗号化
  - Firewall 通過，従来どおりパケットフィルタリング可能
  - 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
- IPヘッダ，TCP/UDPヘッダは平文
  - 完全性保証・本人性確認により，不正パケットを廃棄



PCCOMの原理 ―完全性保証・本人性確認―

完全性保証・本人性確認

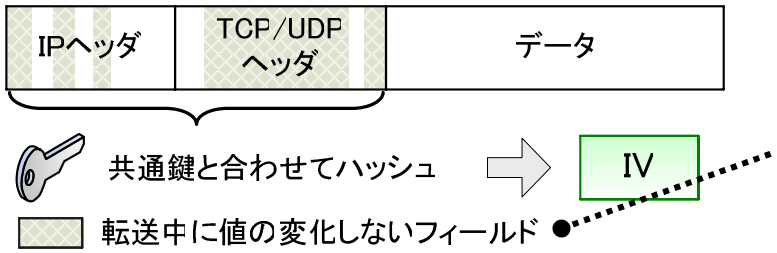
– 疑似データを用いたTCP/UDPチェックサムの独自計算により実現

暗号データとIVのハッシュ値

IV（Initialization Vector）:

暗号化/復号の際に，暗号鍵とは別に必要な初期値

IVの生成方法



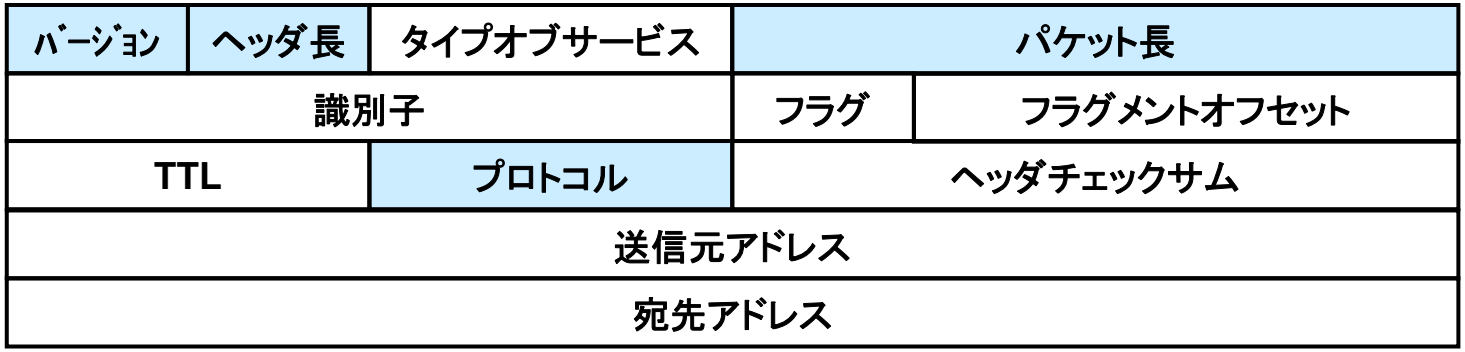
IPアドレス，ポート番号，
TCP/UDPチェックサムは除く

第三者に知られない値 （共通鍵を含むため）

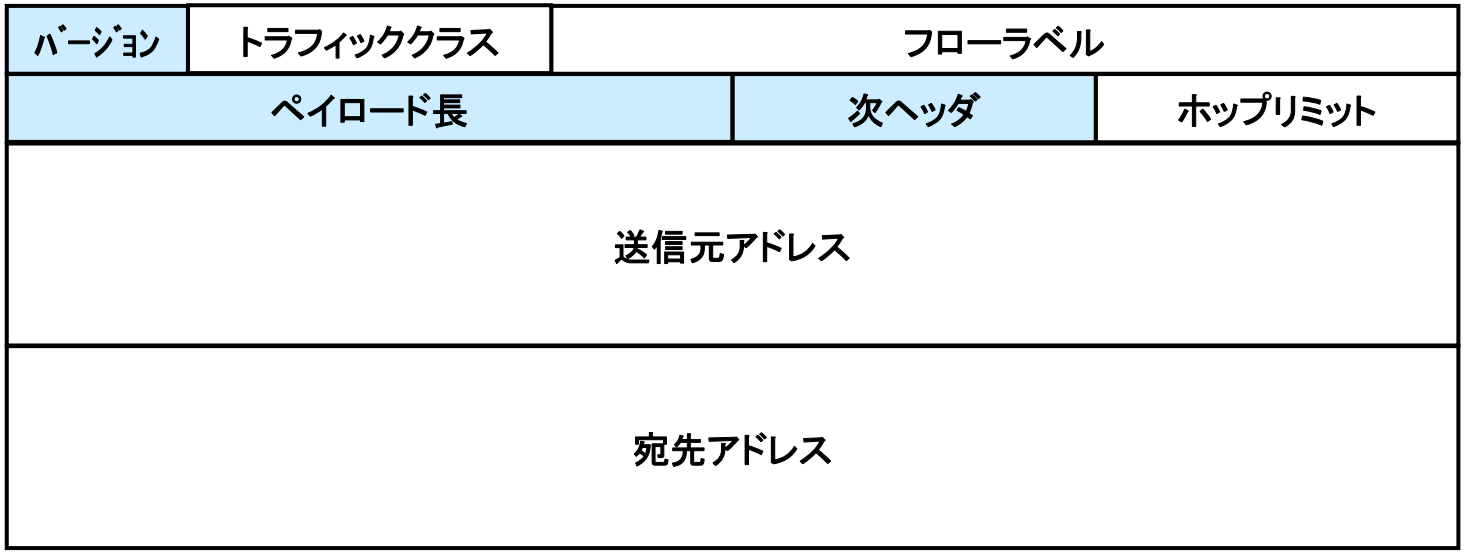
IVはランダムな値で推測は困難 （シーケンス番号などを含むため）

PCCOMの原理 ―完全性保証・本人性確認―

IPv4ヘッダ



IPv6ヘッダ



IV生成に用いるフィールド

PCCOMの原理 ー完全性保証・本人性確認ー

TCPヘッダ

送信元ポート番号			宛先ポート番号
シーケンス番号			
確認応答番号			
ﾃﾞｰﾀｵﾌｾｯﾄ	予約	ｺﾝﾄﾛｰﾙﾌﾗｸﾞ	ウィンドウサイズ
チェックサム			緊急ポインタ

UDPヘッダ

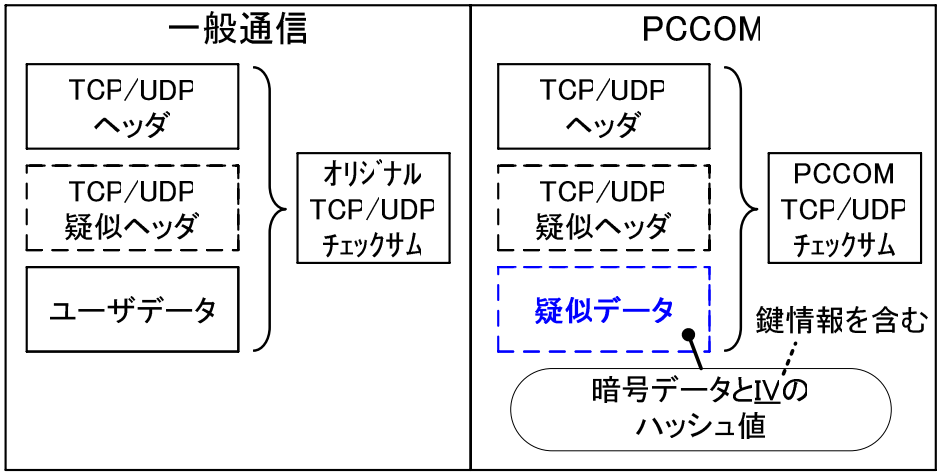
送信元ポート番号	宛先ポート番号
パケット長	チェックサム

IV生成に用いるフィールド

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，IV生成に用いたフィールド　の完全性を保証

– 疑似データは正当な（鍵を共有している）相手しか作れない

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

変換部分（IPアドレス，ポート番号）の差分計算

再計算ではない

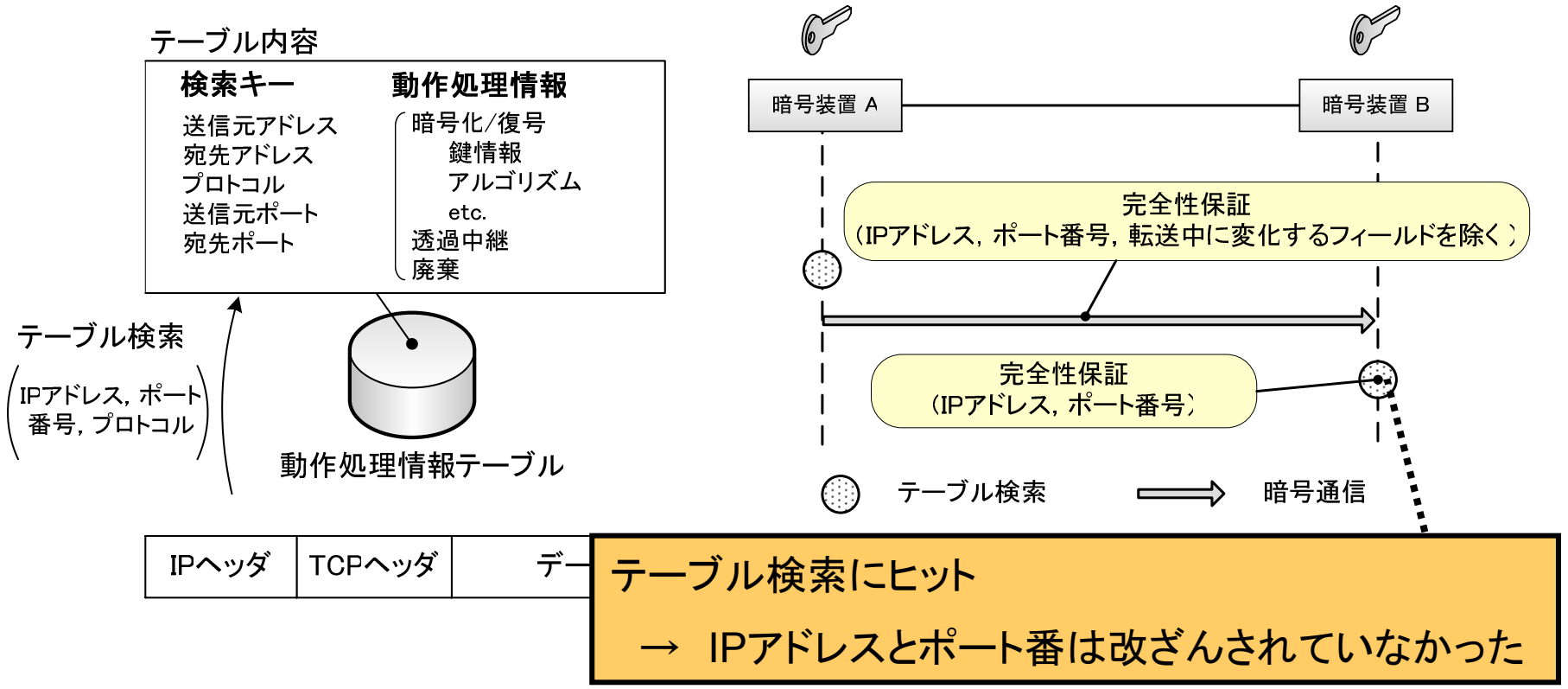
→ PCCOMのチェックサム検証には影響を与えない

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



– 正しいテーブルの生成を保証する方式：IKE　etc.

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
  - $1/2^{16}$ 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）
    - ウィンドウサイズの改竄によるパケットの取りこぼし （ $1/2^{16}$ の確率で成功）
    - ユーザデータの改竄 （意図した改竄は不可能）
  - リプレイ攻撃

IPv4/IPv6混在環境における考察

- IPv4/IPv6混在環境
  - NA(P)Tの存在は無視できない
- PCCOM
  - NA(P)Tとの親和性が高い
    - → IPv4/IPv6混在環境に対応
  - パケットフォーマットを変えず，既存システムや新技術の出現に影響が少ない
    - → 導入の敷居が低く，IPv6環境にも対応しやすい
- 企業ネットワーク
  - IPv4のインフラ，アプリケーション
    - IPv6への移行は時間を要する
  - 部門ごとにFirewallが設置されている場合が多い

イントラネットのセキュリティ技術として有効

まとめと今後の課題

- まとめ
  - PCCOMの説明，IPv6検討
  - IPv4/IPv6混在環境での有効性評価

    PCCOM

    - NA(P)Tと相性が良く，新技術にも対応しやすい

      → IPv4/IPv6混在環境に有効

- 今後の課題
  - リプレイ攻撃の対策

ご清聴ありがとうございました

名城大学