実用性を重視した暗号通信方式の提案

11300J125　増田真也
渡邊研究室

1. はじめに

近年，ネットワークにおける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いる．既存技術であるIPsecは，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（以下，FW）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．また，文献 1）において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が提案されているが，NA(P)Tを通過できないことや，本人性確認※1とパケットの完全性保証※2を考慮していないという課題がある．そこで本研究では，文献 1）の利点をそのまま継承し，既存システムに影響を与えず，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を提案する．

2. 提案方式

提案方式では，**図 1** のようにユーザデータ部分のみを暗号化の対象とすることで，NA(P)TやFWを通過できるようにする．暗号化には，パケット長を変えないためにブロック暗号のCFBモード※3を用いる．また，図 1 のように設定によってパケットの完全性保証に関わる処理を分ける．

図 1　提案方式のパケットフォーマット（TCP の場合）

①　NA(P)T なしの設定

暗号化/復号の際は，暗号鍵とは別に IV（Initialization Vector）をパラメータとして与える必要がある．提案方式では， 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の鍵付きハッシュ値を求めることで，パケットごとに異なる値となる IV を生成する．IV 生成には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，以下で述べる完全性保証の役割も果たす．

パケット長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ために，TCP/UDP チェックサムを用いる．すなわち，**図 2** のように暗号データと IV を合わせたハッシュ値をデータの一部と見なして（疑似データと呼ぶ）チェックサムの再計算/検証を行うことで，パケットの完全性を保証することができる．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できる．

②　NA(P)T ありの設定

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．NA(P)Tでは，チェックサムの書き換えが行われるが，変換部分の差分計算を行う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．この設定では，別の方法でIPアドレスとポート番号の完全性保証を行う必要がある．例えば，暗号通信に先立って行う DPRP（Dynamic Process Resolution Protocol）[2] 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．

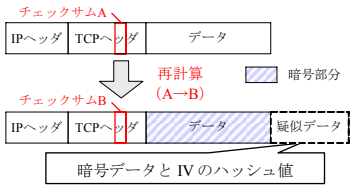


図 2　チェックサムの再計算（TCP の場合）

3. 既存技術との比較検討

IPsec ESP と提案方式を 6 つの項目において比較した表を以下に示す（**表 1**）．

表 1　IPsec ESP（トランスポートモード）との比較

	機密性	本人性確認	完全性保証	NA(P)T	FW	フラグメント
IPsec ESP	◎	◎	◎	△	△	×
提案方式	○	○	○	○	○	○

IPsec ESP（トランスポートモード）の場合，TCP/UDP ヘッダを暗号化・完全性保証の範囲に含めているため，特殊な処理・設定を行わないと NA(P)T や FW 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．

提案方式は，TCP/UDP ヘッダを暗号化範囲に含めない代わりに，NA(P)T や FW を通過できる．また，文献 1）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，提案方式によるフラグメントは発生せず，高スループットを実現できる．

4. むすび

本稿では，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について提案した．今後は提案方式を実装し，動作確認を行うと共に，既存技術との定量的な比較を行う予定である．

※1　正当な相手であることの保証
※2　パケットが改竄されていないことの保証
※3　任意長のデータを暗号化できるモード

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” 情報処理学会論文誌 Vol.38 No.04-025 Apr.1997
2）渡邊，井手口，笹瀬 “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” 電子情報通信学会論文誌 VOL.J84-D-I No.3

実用性を重視した暗号通信方式の提案

The proposal of practical cipher communication systems

名城大学理工学部情報科学科
渡邊研究室
11300J125　増田真也

はじめに

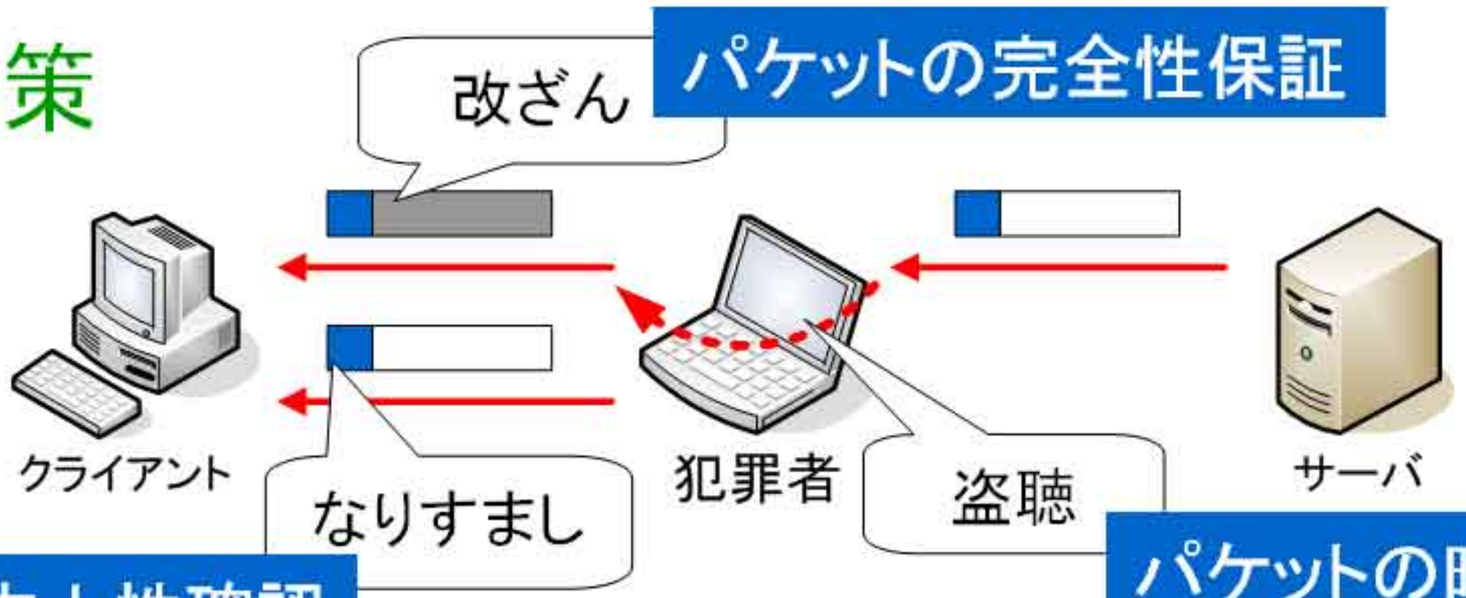
- ネットワークにおけるセキュリティ上の脅威

→ セキュリティ技術の必要性

- 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

NA(P)Tやファイアウォール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

セキュリティ対策の導入がゆえに・・・

別の新たな機器が必要

特殊な処理・設定が必要

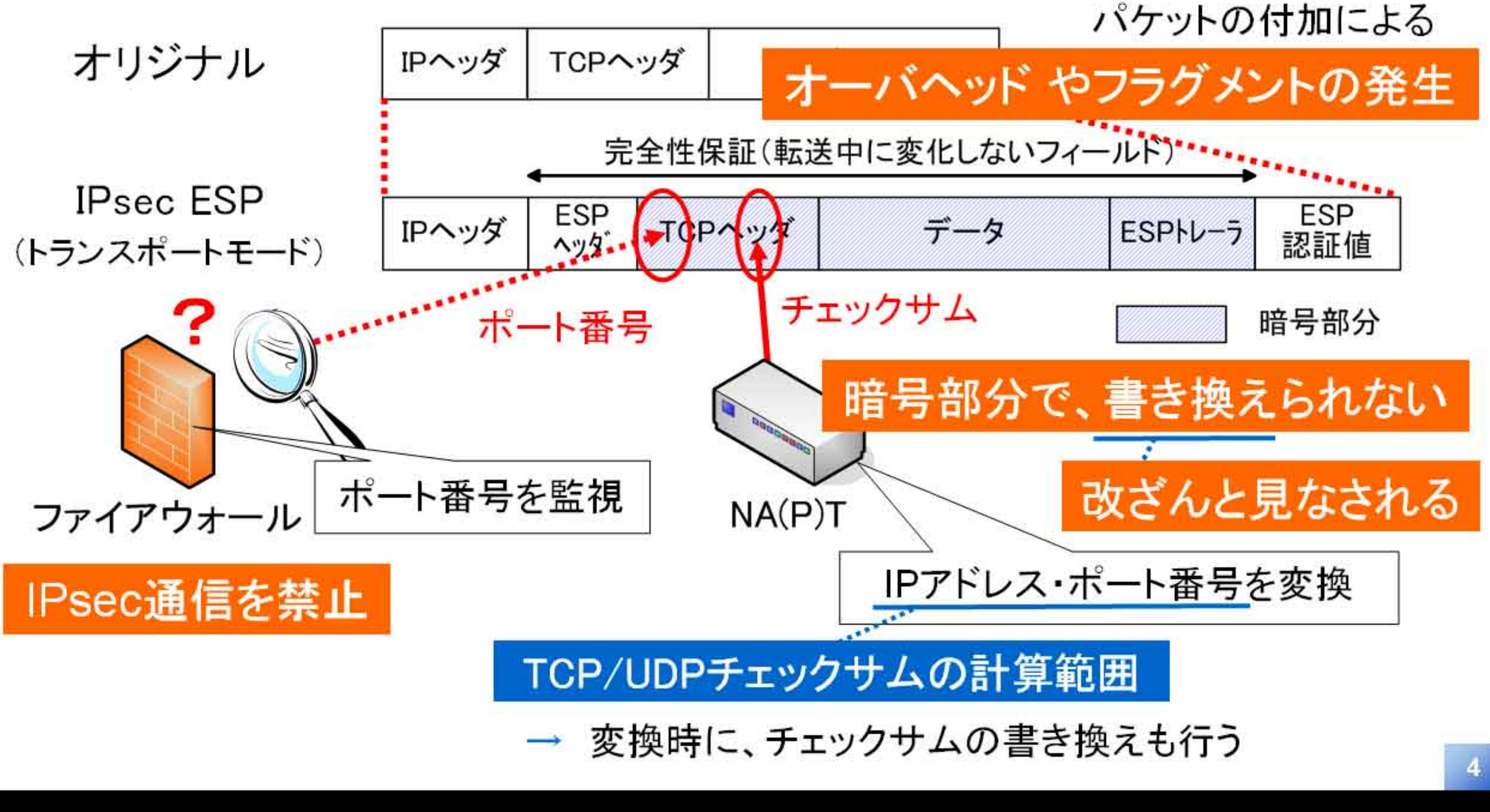
→ 導入の見送り

既存システムに影響を与えず、 容易に導入できる

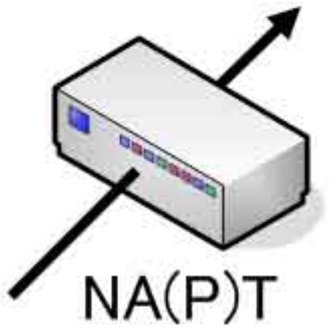
実用性を考える上で重要なポイント

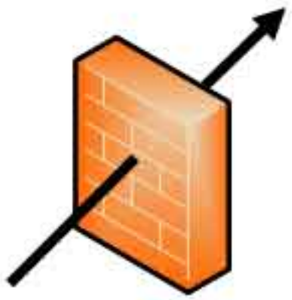
既存技術とその課題

- 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



提　案





NA(P)T、ファイアウォールが通過できる

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

提案方式

暗号化範囲をあえてユーザデータ部分のみとする

→ NA(P)T、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

→ 提案方式によるフラグメントは発生しない

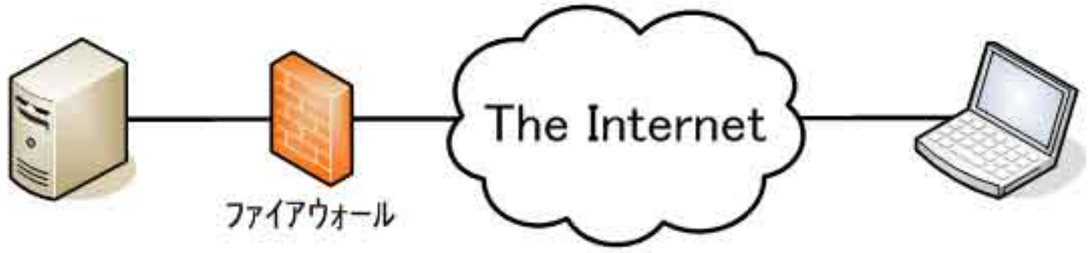
手段として・・・ 任意長のデータを暗号化できる、ブロック暗号のCFBモードを利用

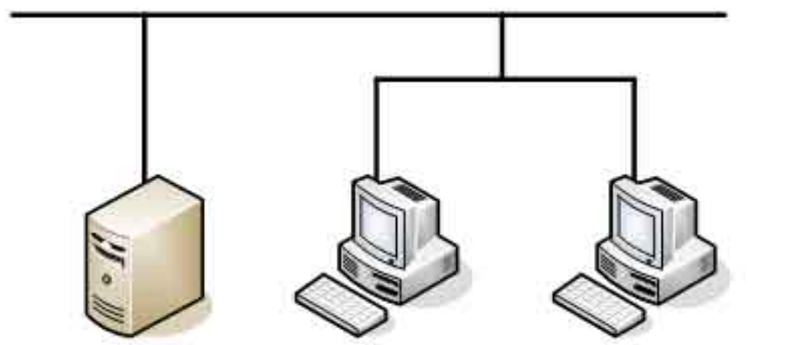
※ NA(P)Tなしの設定 IPアドレス・ポート番号を含む　　NA(P)Tありの設定 IPアドレス・ポート番号を含まない

設定によって、完全性保証に関わる処理を分ける

提案方式　設定例

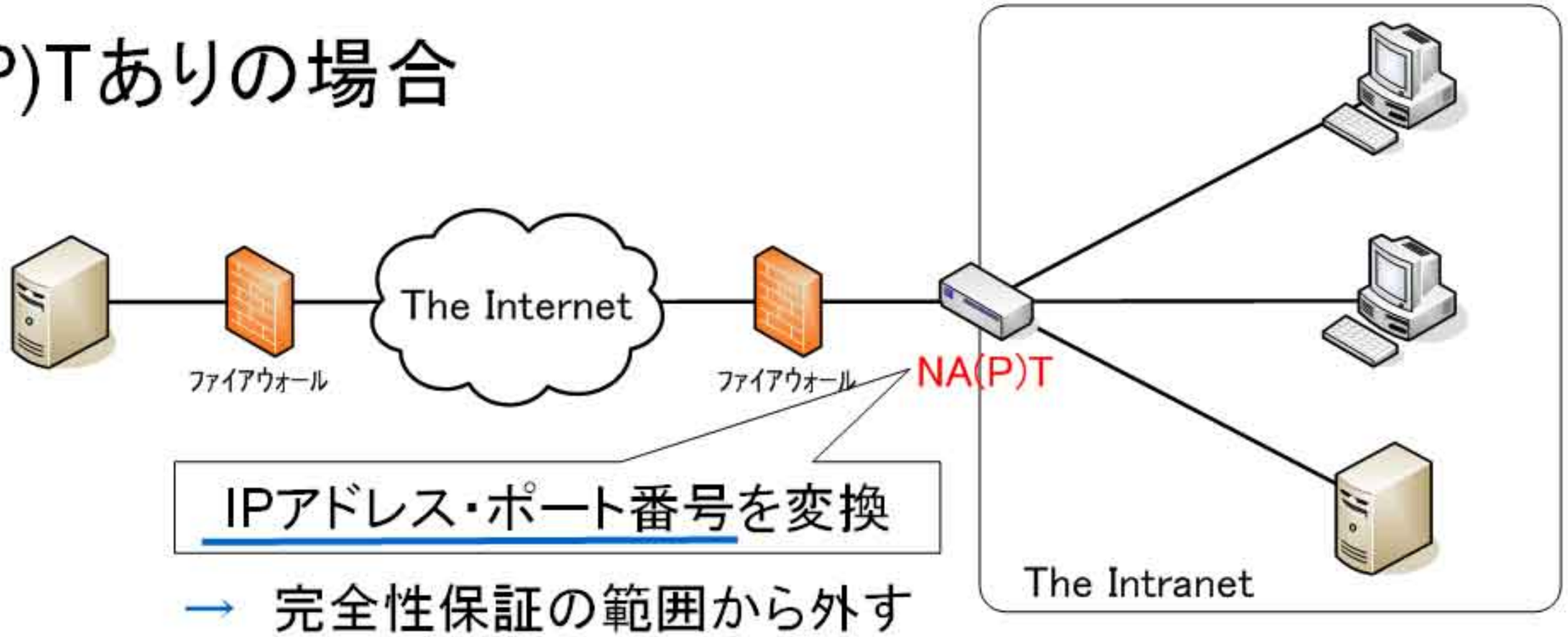
NA(P)Tなしの場合





本方式を独立して使用可能

NA(P)Tありの場合



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

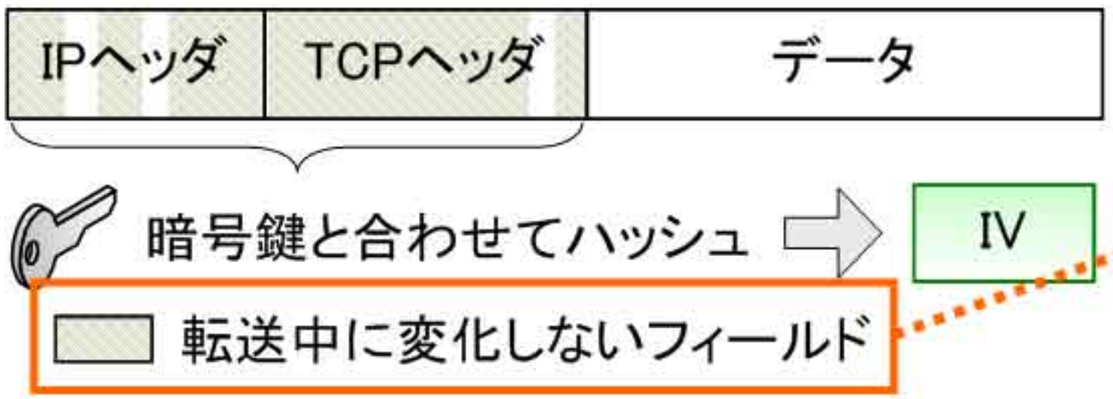
他の技術との組み合わせで保証

提案方式　NA(P)Tなしの設定

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

提案方式　NA(P)Tなしの設定

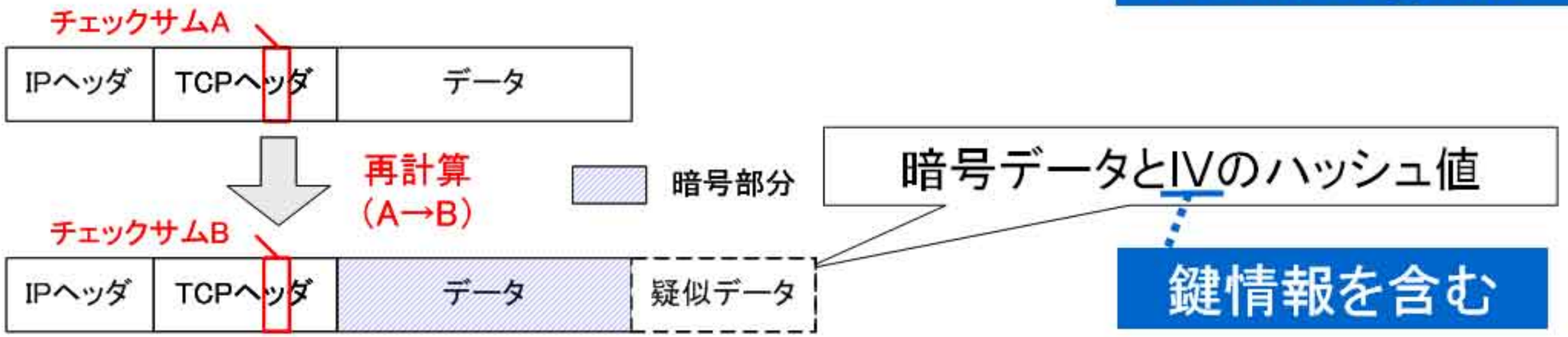
- 本人性確認とパケットの完全性保証
  - パケット長を変えないため、ヘッダの追加はしない
    → TCP/UDPチェックサムを用いる

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のハッシュ値をデータの一部の見なして、再計算/検証を行う

疑似データと呼ぶ

独自の計算方式

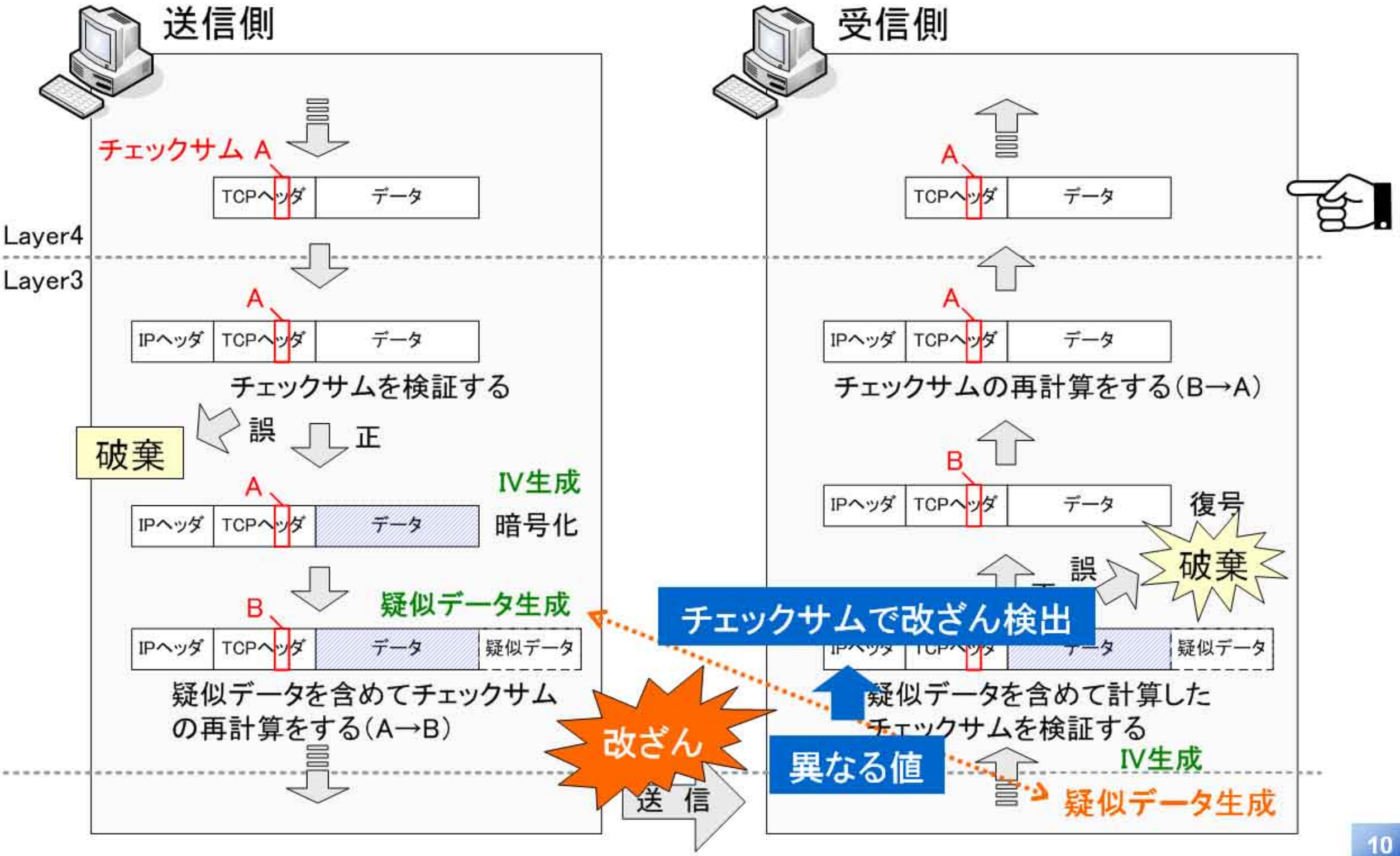


→ 暗号部分とIV生成に用いたフィールドの完全性を保証

- 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

提案方式　NA(P)Tなしの設定

- 改ざん検出の流れ



提案方式　NA(P)Tありの設定

- 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（疑似データを含めた再計算）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できる

例：　**提案方式**　＋　**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

比較検討

IPsec ESPと提案方式の比較

	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	◎	◎	◎	△	△	×
提案方式	○	○	○	○	○	○

- 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
      （特殊な処理・設定によって、通過できることもあるが困難）
  - 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
- 提案方式
  - 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、提案方式によるフラグメントは発生しない
    - → 高スループットを実現

む す び

- まとめ
  - 実用性を重視した暗号通信方式として
    - NA(P)T、ファイアウォールの通過ができる
    - 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

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

提案方式　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

- 現在の状況
  - 試作モジュールの開発完了（動作検証・処理性能を確認済み）
- 今後の課題
  - モジュールをカーネルに組み込む
    - システムの動作検証
    - 既存技術との定量的な比較

おわり