本資料について

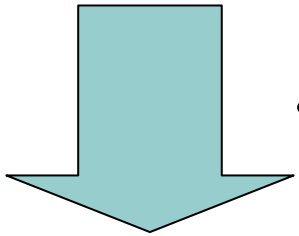
- 本資料は下記論文を基にして作成したものです．文書内容の正確性は保障できないため，正確な知識を求める方は原文を参照してください．
  - 著者：石川 大法　木村 成伴　海老原 義彦
  - 論文名： RSIPサーバにおけるポート番号によるパケットフィルタリングの提案とその性能検証
  - 出展：情報処理学会論文誌 Vol.45 No.2
  - 発表日：2004年2月

RSIPサーバにおけるポート番号による パケットフィルタリングの提案とその性能検証

名城大学理工学部情報科学科
030432057 佐本 章悟

はじめに

- 近年，インターネットの急速な普及により，インターネットを介した電子商取引などへの需要が増加してきている

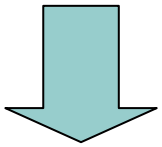


金銭，個人情報のやり取りがあるため，通信内容が改竄，盗聴があってはならない

SSH・SSL・IPsecなどの
暗号化通信プロトコルが開発されている

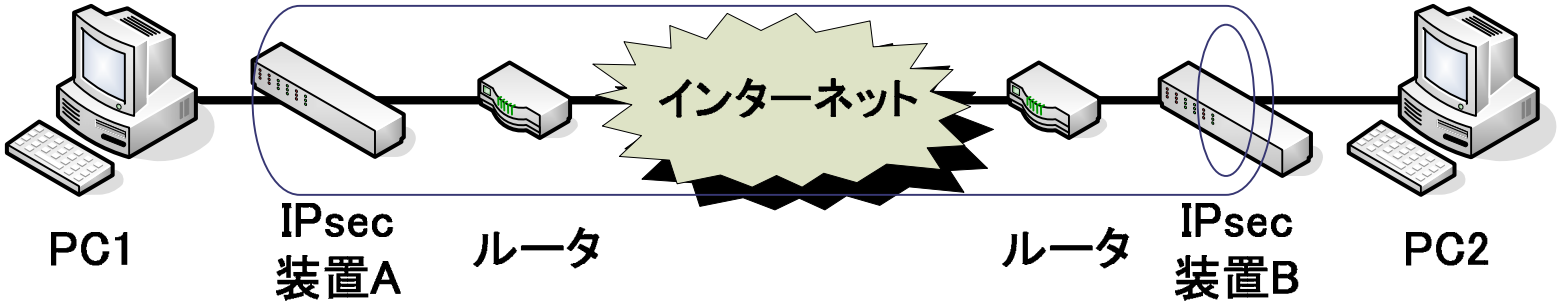
SSHとSSLとIPsec

- SSHとSSL
  - TCPのデータ領域を暗号化
  - 各アプリケーションがこれらのプロトコル利用するように実装
- IPsec
  - IPデータグラムのデータ領域の暗号化や送信者の署名を加える機能
  - アプリケーションを意識することはない



SSHやSSLをすべてのアプリケーションに実装することは事実上不可能
そこでアプリケーションが共通的に使用するIPレイヤで使用できるIPsecに注目

IPsecについて



IPsec装置同士でトンネリング

トンネリング ⇒SA（Security Association）

SA ・・・暗号化を行うための暗号化アルゴリズムやその鍵をまとめたもの

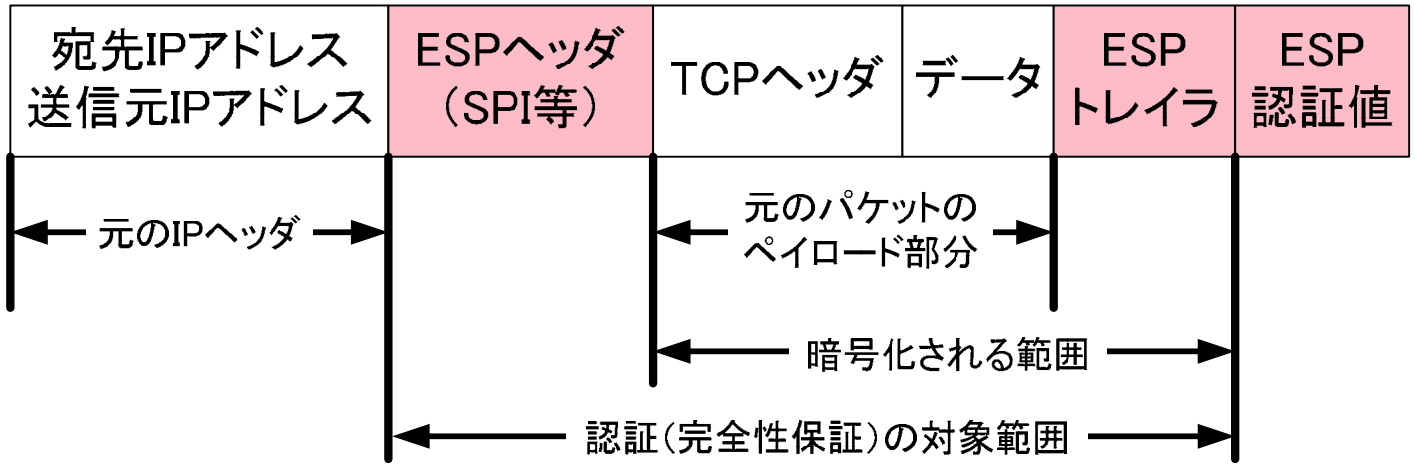
SPI・・・（Security Parameters Index）SAを識別するための識別子

受信側ホストはSPIから復号に必要なSAを特定している

またSAは暗号化や認証の方法にESPとAHを使用したものに分かれる

ESPとAH

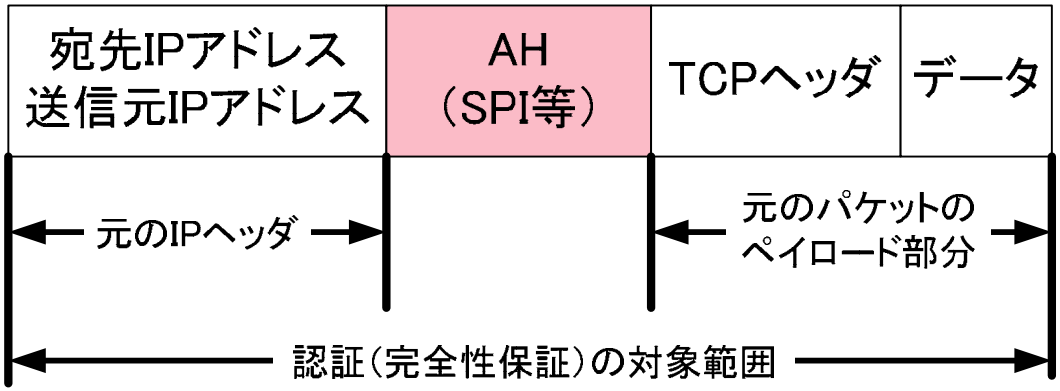
- ESP（Encapsulating Security Payload）
  - パケットの内容を暗号化し秘密にする.
  - 限定的な範囲（IPヘッダを除く）で認証を保証できる



※トランスポートモードの場合

ESPとAH

- AH（Authentication Header）
  - パケットは暗号化されない
  - IPヘッダを含めて認証できる



※トランスポートモードの場合

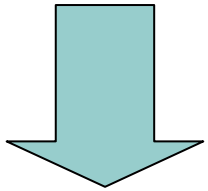
IPsecの問題点

- IPsecではTCPやUDPのヘッダも暗号化してしまうため，ポート番号を途中経路上で読み取ることが不可能．FW(Fire Wall)ではポート番号によるフィルタリングが，NAPTでは変換テーブルの作成ができなくなる
- AHでは，FWやNAPTでデータグラムに変更が加えられた場合，受信時に改竄がなされたと判断し破棄してしまう

既存技術

問題の解決

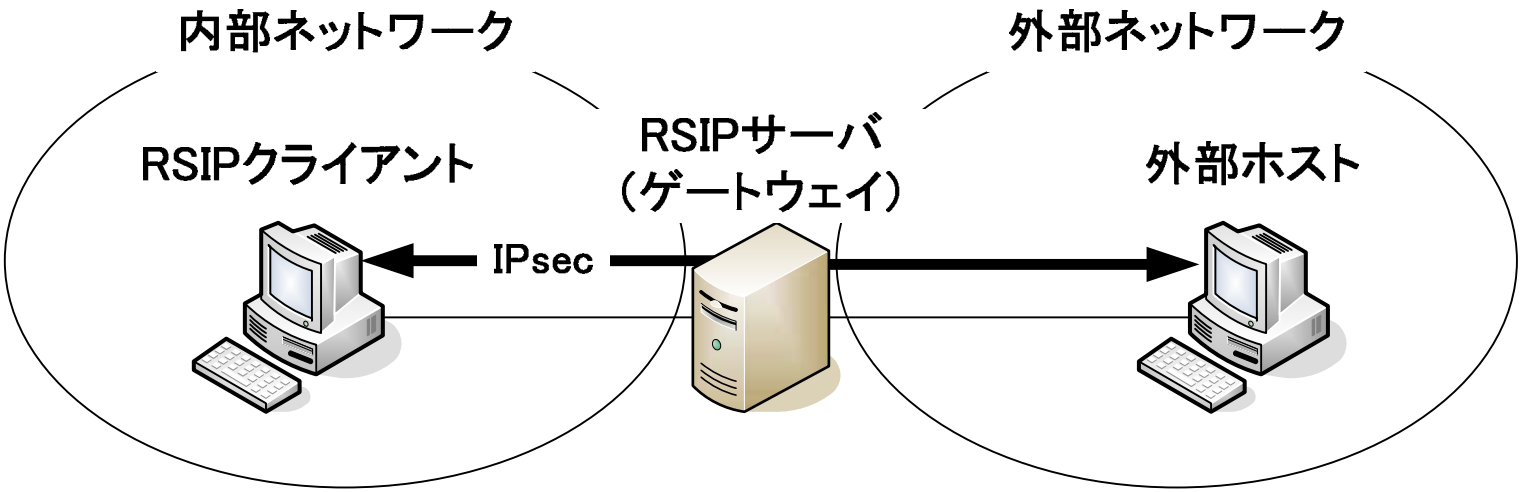
- 問題のうち，NAPTのサービスを受けられない問題とAHを使用できない問題を解決するために・・・



RSIP（Realm Specific IP）が提案されている

既存技術

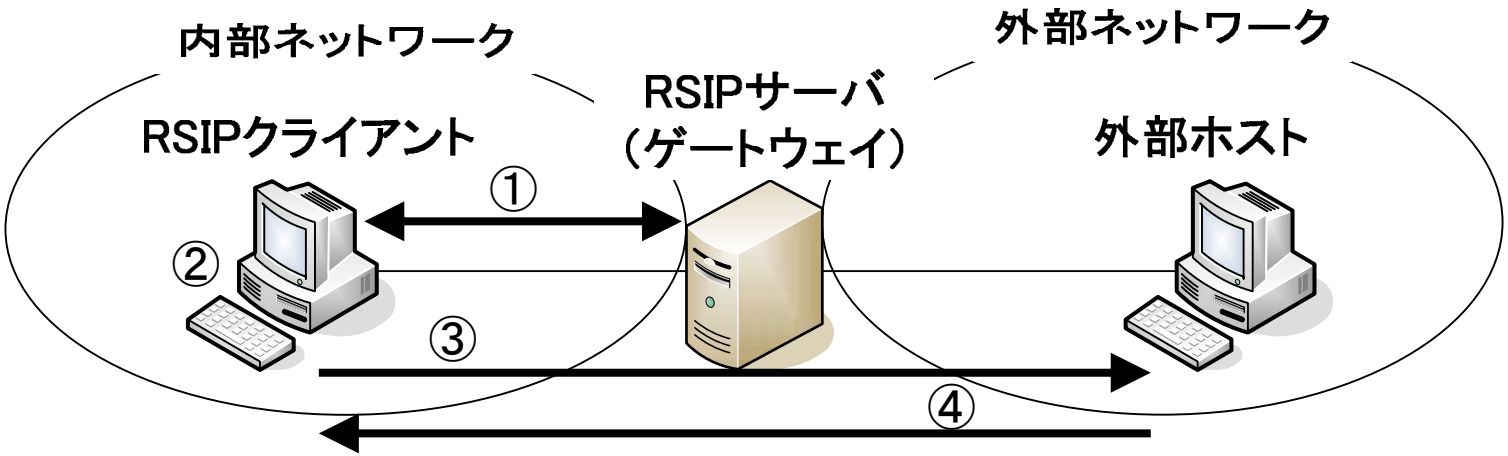
対象とするネットワーク



- 内部ネットワークにRSIPクライアント
- 外部ネットワークに外部ホスト
- 境界にRSIPサーバ（ゲートウェイ）

既存技術

RSIPの動作概要



RSIPクライアントが外部ホストにIPsecを用いた通信を開始する際・・・

① RSIPクライアントがあらかじめRSIPサーバに通信相手のIPアドレスやポート番号，SPIなどを通知
② RSIPクライアント自身がポート番号を使用したアドレス変換を行う
③ 外部ホストにRSIPサーバを経由してデータを送信

} 外向きの通信

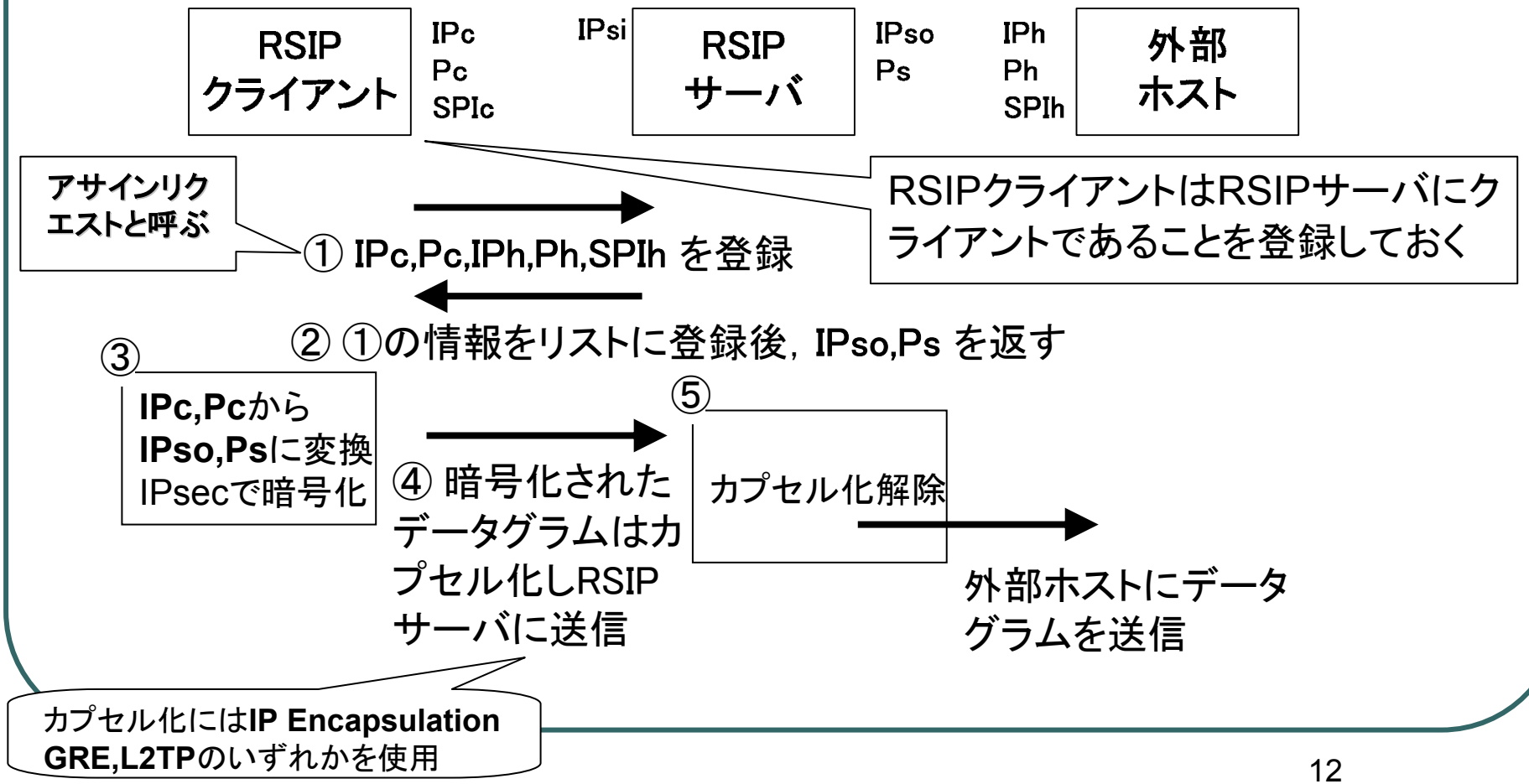
④ 外部ホストはRSIPサーバを経由しRSIPクライアントと通信

} 内向きの通信

既存技術

RSIPの動作詳細 ～外向きの通信～

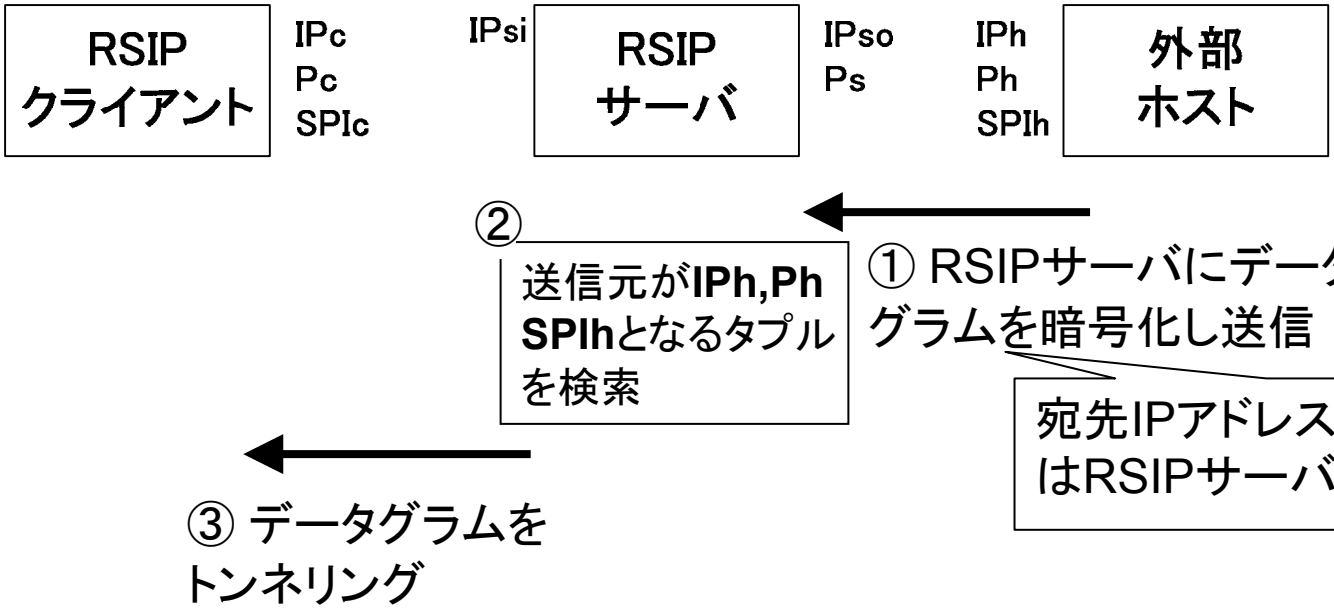
RSIPクライアントが外部ホストにIPsecを用いた通信をするとき



既存技術

RSIPの動作詳細 ～内向きの通信～

RSIPクライアントが外部ホストからデータグラムを受け取る場合

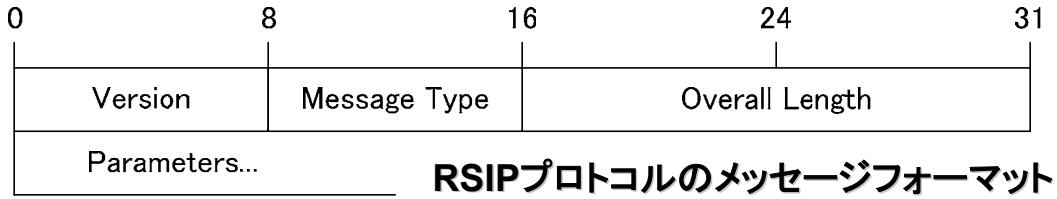


以上のように，送信元でアドレス変換を施すことでゲートウェイがポート番号を読み取る必要性をなくし，ゲートウェイがデータグラムを書き換えてしまうことによるAHが使用できないという問題を解決している

既存技術

RSIPプロトコルのメッセージフォーマット

RSIPクライアントがRSIPサーバにアサインリクエストを出し，
その結果を受け取るときなどにRSIPプロトコルが使用される



RSIPプロトコルのメッセージフォーマット

Versionにはプロトコルバージョン 現在は“1”

Message Typeにはメッセージタイプに関連付けられた値

Overall Lengthには送信するメッセージの全体長を指定

Parametersには**Message Type**で指定したメッセージタイプに必要なパラメータが設定される

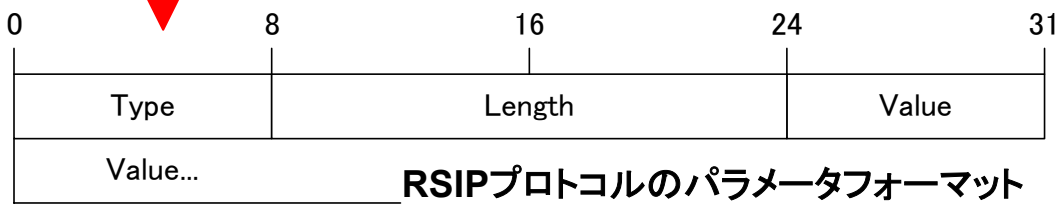
RSIPプロトコルのメッセージタイプ

Value	Message
1	ERROR_RESPONSE
2	REGESTER_REQUEST
3	REGESTER_RESPONSE
4	DE_REGISTER_REQUEST
5	DE_REGISTER_RESPONSE
6	ASSIGN_REQUEST_RSA_IP
7	ASSIGN_RESPONSE_RSA_IP
8	ASSIGN_REQUEST_RSAP_IP
9	ASSIGN_RESPONSE_RSAP_IP
10	EXTEND_REQUEST
11	EXTEND_RESPONSE
12	FREE_REQUEST
13	FREE_RESPONSE
14	QUERY_REQUEST
15	QUERY_RESPONSE
16	LISTEN_REQUEST
17	LISTEN_RESPONSE
22	ASSIGN_REQUEST_RSIPSEC
23	ASSIGN_RESPONSE_RSIPSEC

既存技術

RSIPプロトコルのメッセージフォーマット

RSIPプロトコルのメッセージフォーマット



RSIPプロトコルのパラメータフォーマット

Typeにはパラメータのタイプ 例えばアドレスは1，ポート番号は2など

Lengthには**Value**の長さをバイト単位で指定

RSIPの問題点と解決

RSIPにより，IPsecで暗号化されたデータグラムをRSIPサーバを経由して通信ができた・・・

しかし途中経路上でポート番号を読み取れないため，依然としてファイアウォールのサービス（ポート番号によるフィルタリング）を受けられないという問題が残っている

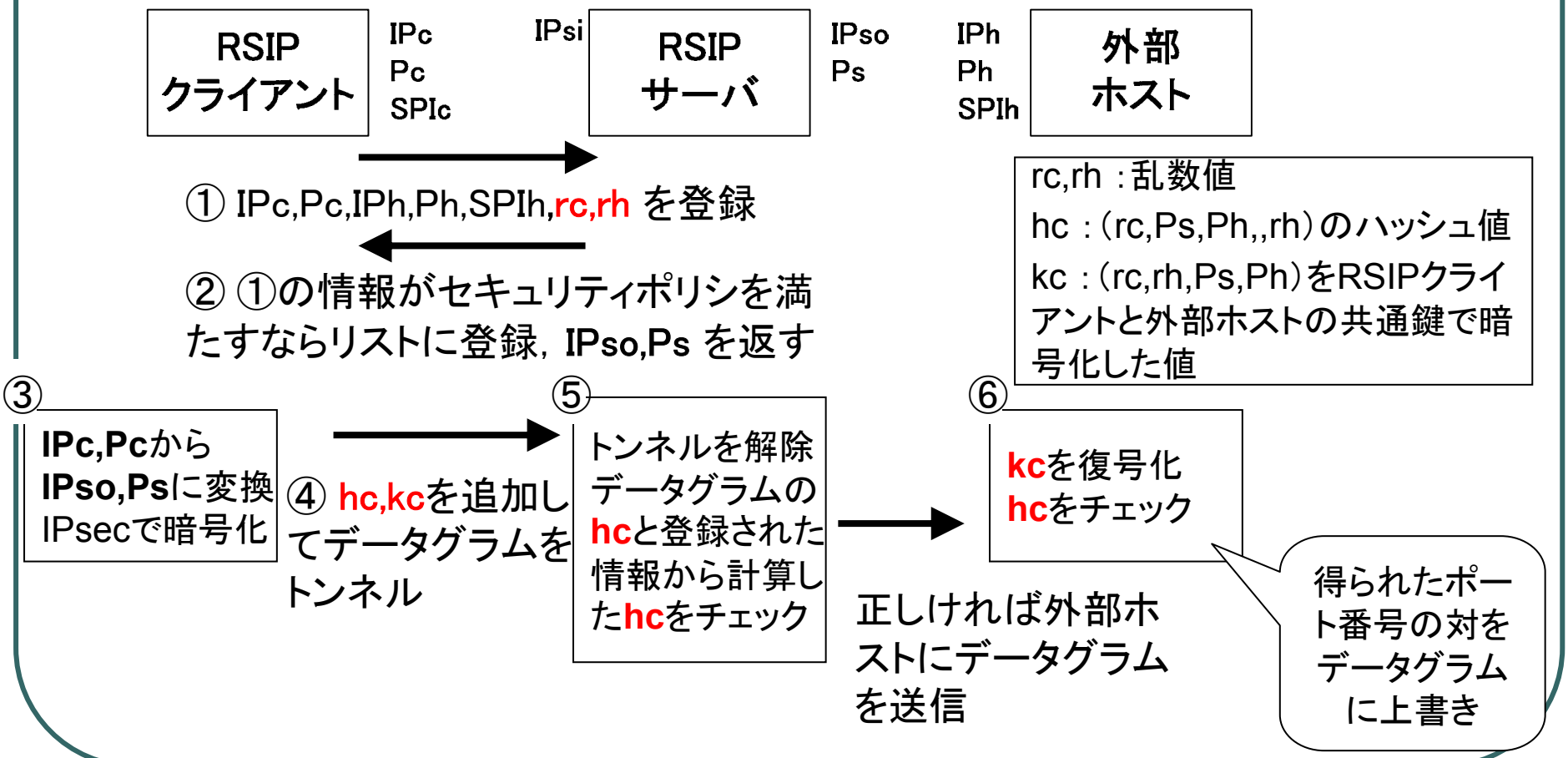
そこで本発表ではRSIPプロトコルを改良することでこの問題を解決する

従来のRSIPと提案方式の違い

- 従来のRSIPと提案方式の違いは，登録されたポート番号であるか否かを識別する2つの値をデータグラムに添付することにある．これらの値を用い，RSIPサーバと外部ホストが協力することでRSIPサーバに登録されていないポート番号をもつパケットのフィルタリングを実現する

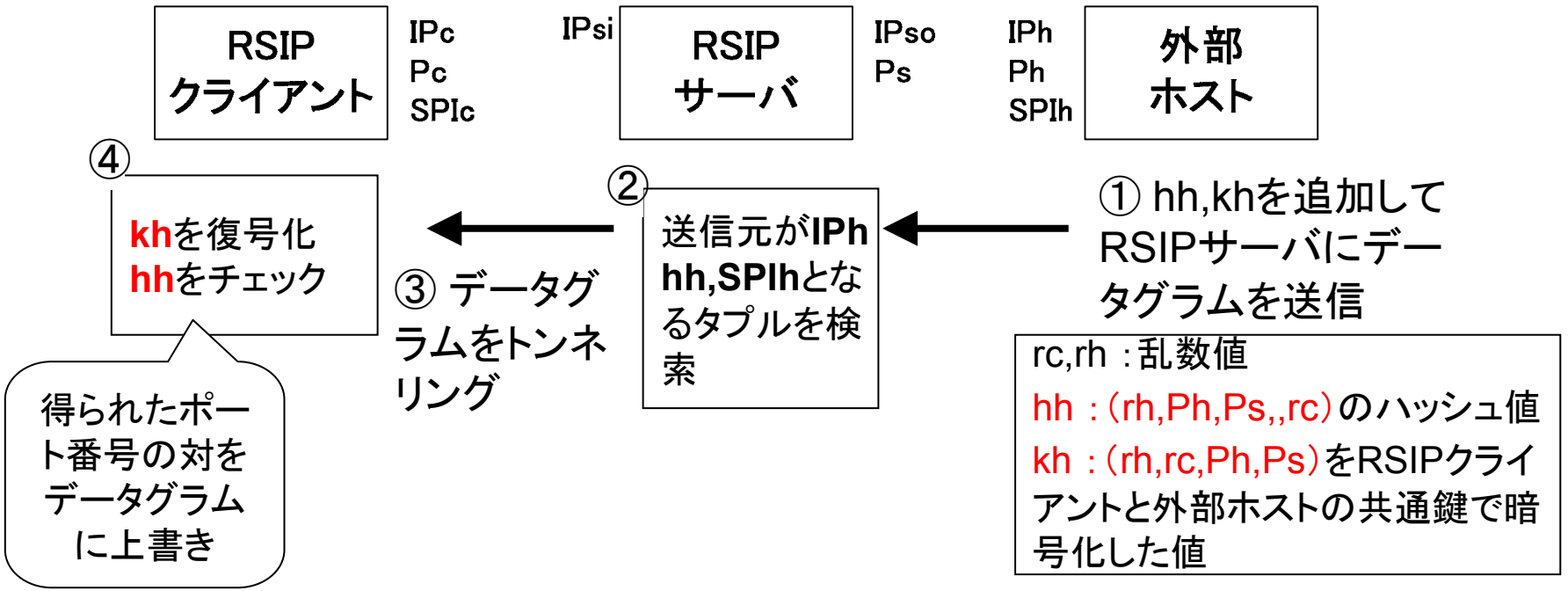
提案技術

RSIPの動作詳細 ～外向きの通信～



提案技術

RSIPの動作詳細 ～内向きの通信～



以上のような手順を用いることで，経路上のRSIPサーバ以外のホストにポート番号を知られることなく，登録されたポート番号の使用を強制することができる

提案方式の実装　～追加メッセージ～

- 提案システムでは追加したメッセージを運ぶのに必要となる，メッセージタイプ，パラメータ，IPオプションがある

追加するメッセージタイプ

Value	Message
18	ASSIGN_REQUEST_RSE_IP
19	ASSIGN_RESPONSE_RSE_IP

RSIPクライアントからRSIPサーバに提案方式での外部ホストとの通信を要求するものとその返答

追加するパラメータ

ASSIGN_REQUEST_RSE_IP, ASSIGN_RESPONSE_RSE_IPはrc,rhなどをパラメータに持つがrc,rhは定義されていないので定義する必要がある

追加するIPオプション

hcなどのハッシュ値やkcなどの暗号化された値を求めるため，ポート番号と乱数をまとめたフォーマットが新たに作られる．

ハッシュ値生成にはMD5が，暗号化した値を求めるにはDESが使われる．

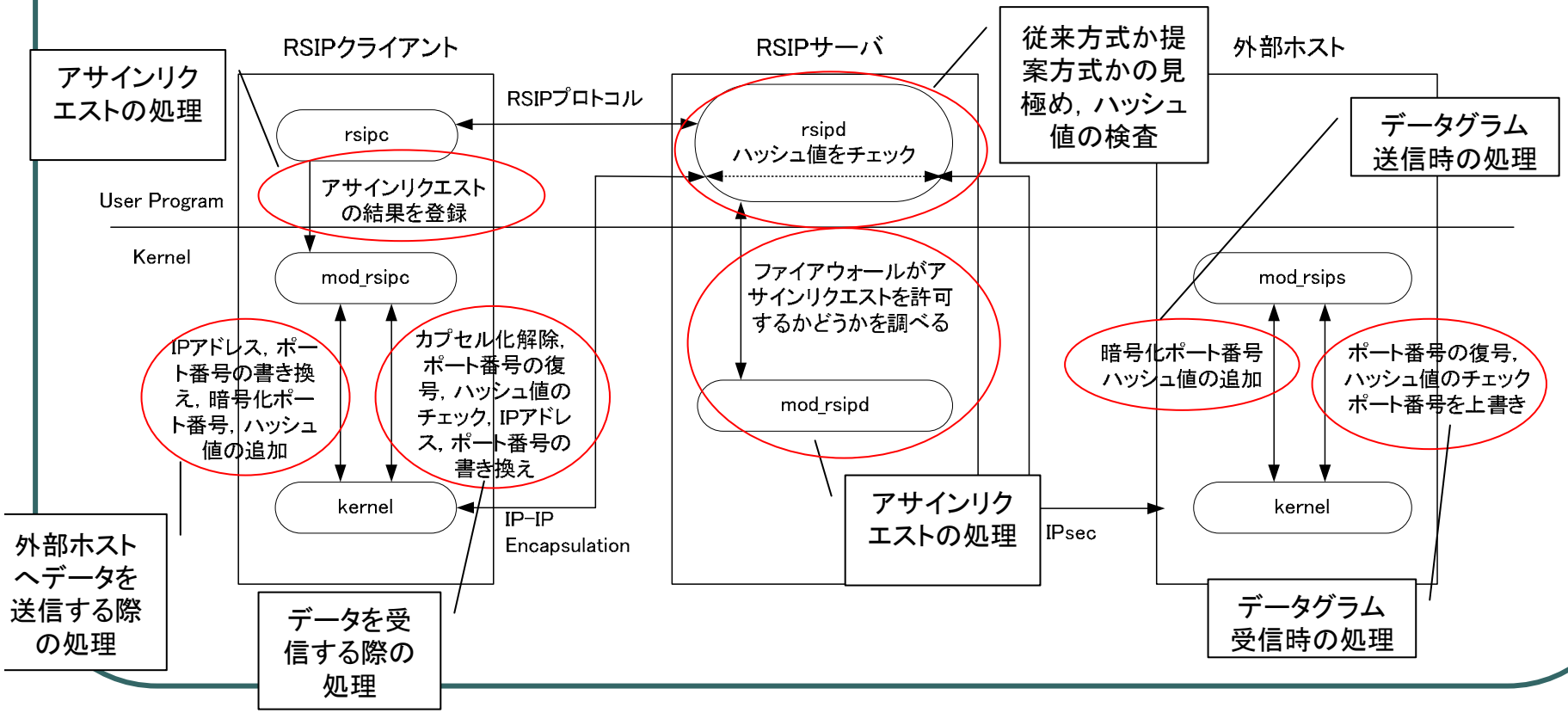
提案方式の実装～FreeBSDへの実装～

- 環境構成

RSIPクライアント
FreeBSD4.6.2_RELEASE-p2

RSIPサーバ
FreeBSD4.6_RELEASE-p2

外部ホスト
FreeBSD4.7_RELEASE-p1



実装システムの検証 ～機能の検証～

- 提案方式によるアサインリクエストがRSIPサーバに受理された後，RSIPクライアントから以下の不正データを外部ホストに送信
  - (1)IPオプションを付けないデータグラム
  - (2)不正なハッシュ値をIPオプションに含むデータグラム
  - (3)不正なポート番号を暗号化した値をIPオプションに含むデータグラム
  - (4)ESPデータ内のポート番号を不正なポート番号に書き換えたデータグラム

結果

RSIPサーバでは

(1)と(2)のデータグラムは破棄され，それ以外は通過させている．RSIPサーバではハッシュ値のチェックのみを行うため，この動作は正常である．

外部サーバでは

(1)と(2)のデータグラムはRSIPサーバで破棄されるため，(3)と(4)の検証を行う．(3)ではデータグラムを破棄し，(4)ではポート番号を上書きすることを確認した．外部ホストの動作も正常であることが示された．

実装システムの検証 ～性能の検証～

- 提案方式の実装は，従来の暗号化されたデータグラムを送受信するRSIPSECにハッシュなどの処理を加えたものである．そこで提案方式とRSIPSECについて性能を比較する

検証環境

外部ホストに構築したwebサーバからRSIPクライアントが100MBのファイルをダウンロード

	平均スループット	ラウンドトリップタイム
RSIPSEC	5.28MB/s	0.237m
提案方式	5.10MB/s	0.673m

平均スループットの低下はほとんど見られない．しかしラウンドトリップタイムは約3倍となった．これは提案方式によりメモリ上での値の読み取り，比較，書き込みなどが増加したことが原因とおもわれる．しかしこの増加は，データグラムが1ホップ程度の経路を通過する時間に相当するため，実用では大きな障害とならない

まとめ

- 本発表ではRSIPサーバにおけるポート番号によるパケットフィルタリングを提案
- システムを実装し評価したところ，平均スループットの低下がほとんどみられることなく，登録されたポート番号で通信を行うことを強制できることが示された