USAGI IPv6

神田　充
mk@linux-ipv6.org
USAGI/ 東芝研究開発センター

Contents

- USAGI Project 紹介
- Linux kernel IPv6 の歴史
- USAGI Project の状況
- 適合試験
- IPsec 概略
- Linux IPsec
- USAGI IPsec

USAGI Project

USAGI Project 紹介

- UniverSAl playGround for Ipv6
- 設立 2000 年 9 月
- コアメンバー
  - 現在 7 名
- 週 3 日新川崎 K2 タウンキャンパスに棲息
- KAME(http://www.kame.net/) チームと同棲

USAGI Project 紹介 (続き)

- 目標
  - Linux Kernel の IPv6 の改善
  - Linux における IPv6 API 環境の改善
  - Linux IPv6 アプリケーション対応
- 開発ポリシー
  - 成果物は GPL2 にて配布
  - ディストリビューション非依存

Linux kernel IPv6 の歴史

- Pedro Roque により実装(kernel 2.1.8)
- 現在、 netdev のコアメンバーによりほそぼそとメンテナンスされている
- 最新仕様(RFC) に準拠していない部分が多々ある
  - インターオペラビリティに難あり
- あまり使われていないためか、あまりメンテナンスが良くない

Linux kernel IPv6 の歴史 (続き)

- Mainline kernel において含まれていない機能
  - MobileIPv6
  - IPsec for IPv6
  - Anycast Support
  - Privacy Extensions(RFC3041)
  - Source Address Selection
  - Etc.

USAGI Projectの成果

- Neighbor Discovery Protocolの改善
  - 状態遷移処理の正確化
- Source Address Selection
  - Longest Prefix Match
- ICMP node information query
  - 例) ping6 -W ff02::1%eth0
- Privacy Extensions
  - IPv6アドレスのID部の乱数化

USAGI Projectの成果(続き)

- SNMPv6
- bind(2)の挙動改善
- HUT MobileIPv6の統合
- IPsec
- libinet6の提供
- IPv6化された基本的なアプリケーションの提供

最近の状況

- 2002 年 9 月末に 4 回目の Stable release 作成予定
  - 初めて IPsec(IPv6) が含まれる

適合試験

- 主に TAHI テストを実施することにより確認
  - TAHI Project により作成されているテストツール
- IPv6 の相互接続試験に随時参加
- IPsec の相互接続試験に随時参加

TAHI テスト結果

テスト項目	Vanilla 2.4.19	USAGI
基本仕様	Fail(0)/Warn(0)/86	Fail(0)/Warn(0)/86
ICMPv6	Fail(0)/Warn(0)/22	Fail(0)/Warn(0)/22
Neighbor Discovery	Fail(28)/Warn(1)/81	Fail(9)/Warn(3)/81
Stateless Address Autoconf	Fail(11)/Warn(1)/57	Fail(1)/Warn(1)/57
Path MTU Discovery	Fail(2)/Warn(0)/5	Fail(1)/Warn(0)/5
IPsec	無し	Fail(5)/Warn(2)/118
IPv6 Over IPv4 Tunnel	Fail(1)/Warn(0)/4	Fail(0)/Warn(0)/4
Robustness	Fail(0)/Warn(0)/22	Fail(0)/Warn(0)/4

IPsec 仕様概要 (その 1)

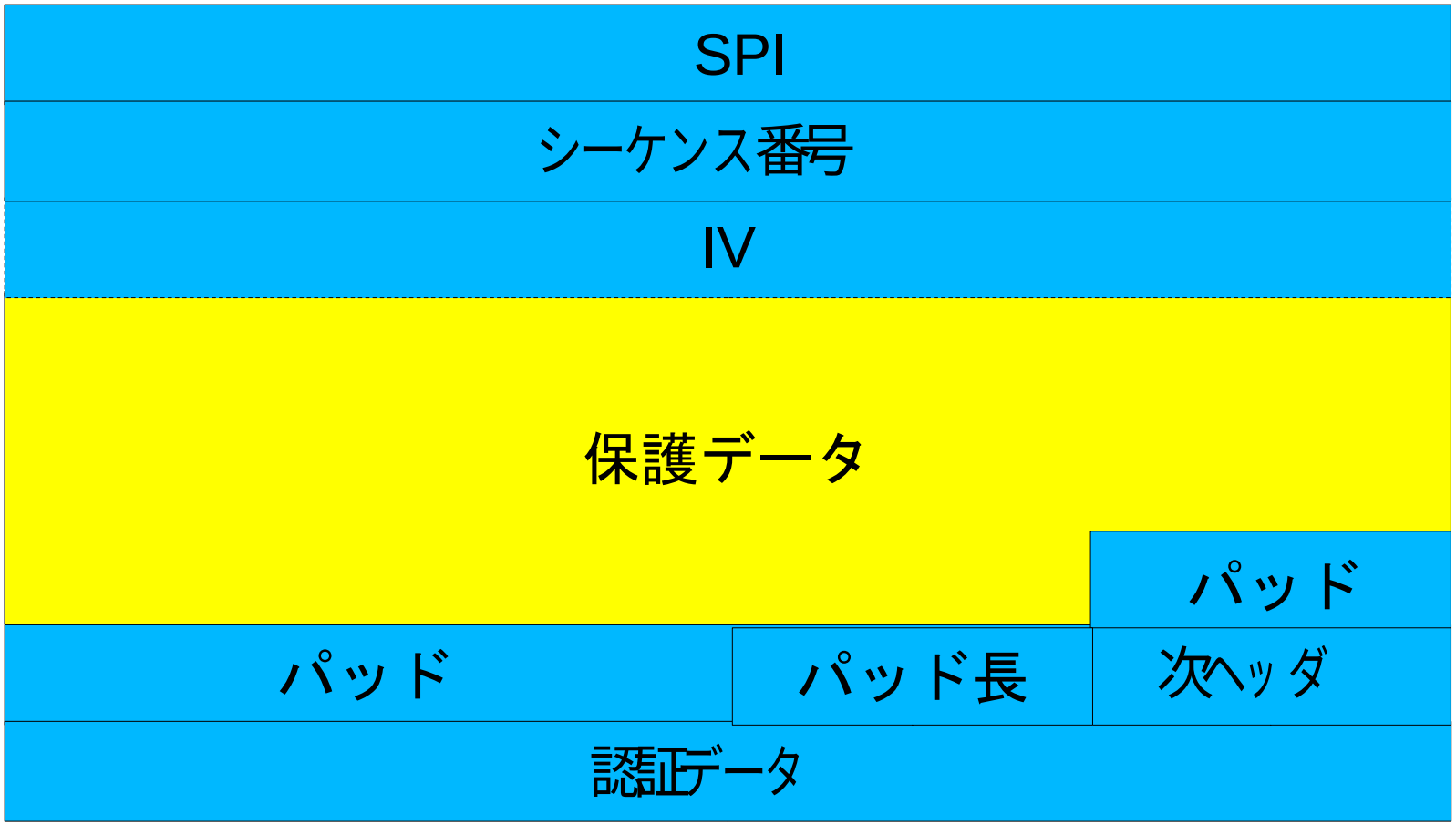
- IP 層に暗号化、認証、完全性チェックなどのセキュリティ機能の枠組みを提供
  - RFC2401
  - IPv6 においては標準機能
- AH ヘッダ
  - データ完全性
  - IP パケット発信元の認証
  - リプレイアタック防止

IPsec 仕様概要 (その 2)

- ESP ヘッダ
  - データの暗号化
  - データの完全性
  - リプレイアタック防止
- ２つのモード
  - トランスポート (Transport) モード
  - トンネル (Tunnel) モード

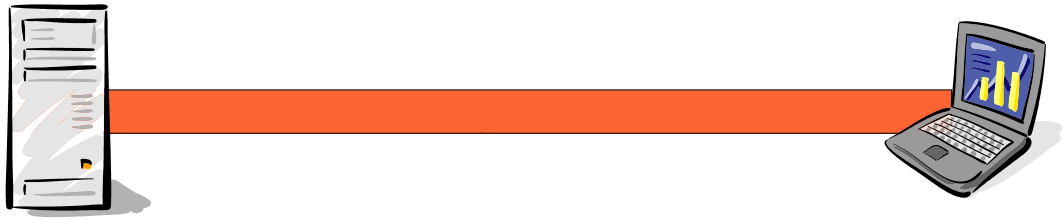
AH ヘッダ

ESP ヘッダ



トランスポートモード

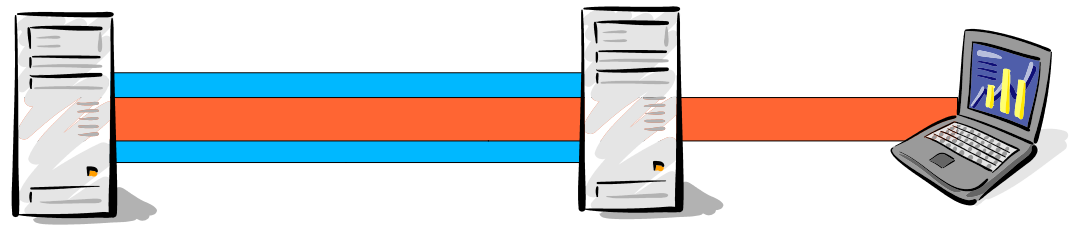
IP	AH	ESP	ペイロード



上位層 (TCP,UDP) を保護するために使

トンネルモード

IP	AH	ESP	IP	ペイロード



SG　　SG

内側 IP パケット全体を保

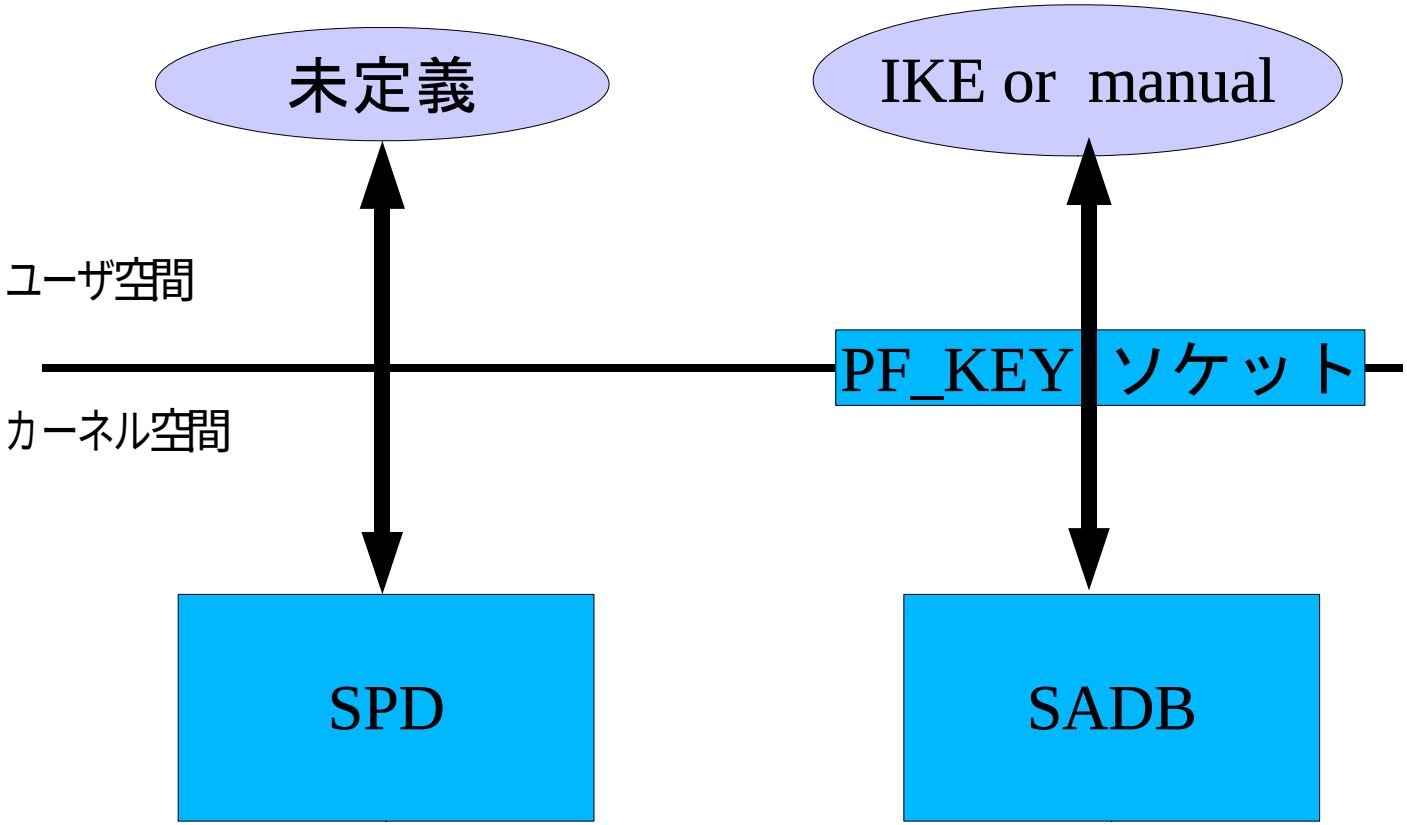
Security Association, Security Policy

- Security Association(SA)
  - 実際に IPsec を適用するためのパラメータ
  - Security Association Database(SPDB) に格納
  - 片方向ずつ設定
  - 宛先アドレス、 IPsec プロトコル、 SPI で識別
- Security Policy(SP)
  - どのパケットに IPsec を適用するかの方針
  - Security Policy Database(SPD) に格納
  - IPsec を適用、通過、破棄

PF_KEYv2

- RFC2367 に定められている、 SA を設定するためのインターフェース
  - 各実装で独自拡張がされていて互換性をとるのが難しい
  - 多くの実装では、 SP も独自拡張によって設定している

PF_KEYv2(続き)



鍵の自動交換

- IPsec においては IKE(Internet Key Exchange) を使用
  - RFC2408, RFC2409
- もちろん、 IKE を使用せずに手動で鍵を設定することも可能

Linux の IPsec 実装

- Mainline kernelの中には存在せず
- Free/SWAN(http://www.freeswan.org/)
  - IPv4 用の IPsec を提供、構造は IPv4 に強く依存
  - 仮想 IPsec デバイスにより kernel 内の IP 層より下に実装
- IABG(http://www.ipv6.iabg.de/)
  - FreeS/WAN を基に IPv6 用の IPsec を実装
  - FreeS/WAN に対するパッチ
  - PF_KEYv2 のインターフェースは、 FreeS/WAN と同じだが内部では IPv6 用に別個に処理
  - 開発は止まっている

USAGI IPsec

- 当初 IABG の実装を基に開発をスタート
- 現在は、ほぼ全面的に書き直された
  - FreeS/WAN のコードは PF_KEYv2 のインターフェース用に一部使用している
- SADB, SPD は IPv4 と IPv6 で共通
- PF_KEYv2 のインターフェースは FreeS/WAN と互換性と保つように努力している

USAGI IPsec(続き)

- IP スタック内に実装
- Security Policy の粒度を細かくとれる
  - 上位プロトコル、ポート
- CryptoAPI を使用 (http://www.kerneli.org/)
  - 汎用的な暗号 / 認証アルゴリズムの枠組み
  - 関数が抽象化されている
  - 多数のアルゴリズムが選択可能

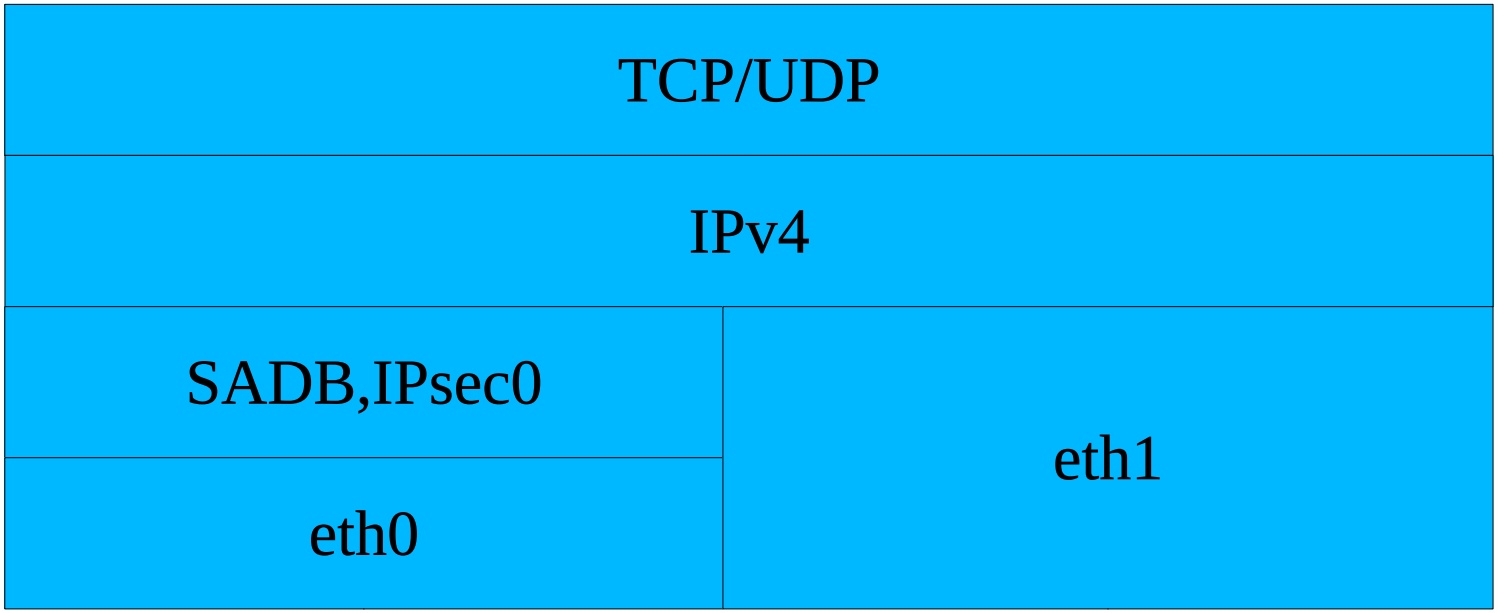
USAGI IPsec(続き)

- 現在サポートしているアルゴリズム
  - 暗号アルゴリズム
    - DES, 3DES, AES
  - 認証アルゴリズム
    - MD5,SHA1
- モード
  - トランスポート、トンネルモード両方サポート
    - トンネルモードは IPv6 over IPv6 トンネルデバイスを流用
    - IPv4 は現在のところトランスポートモードのみ

USAGI IPsec(続き)

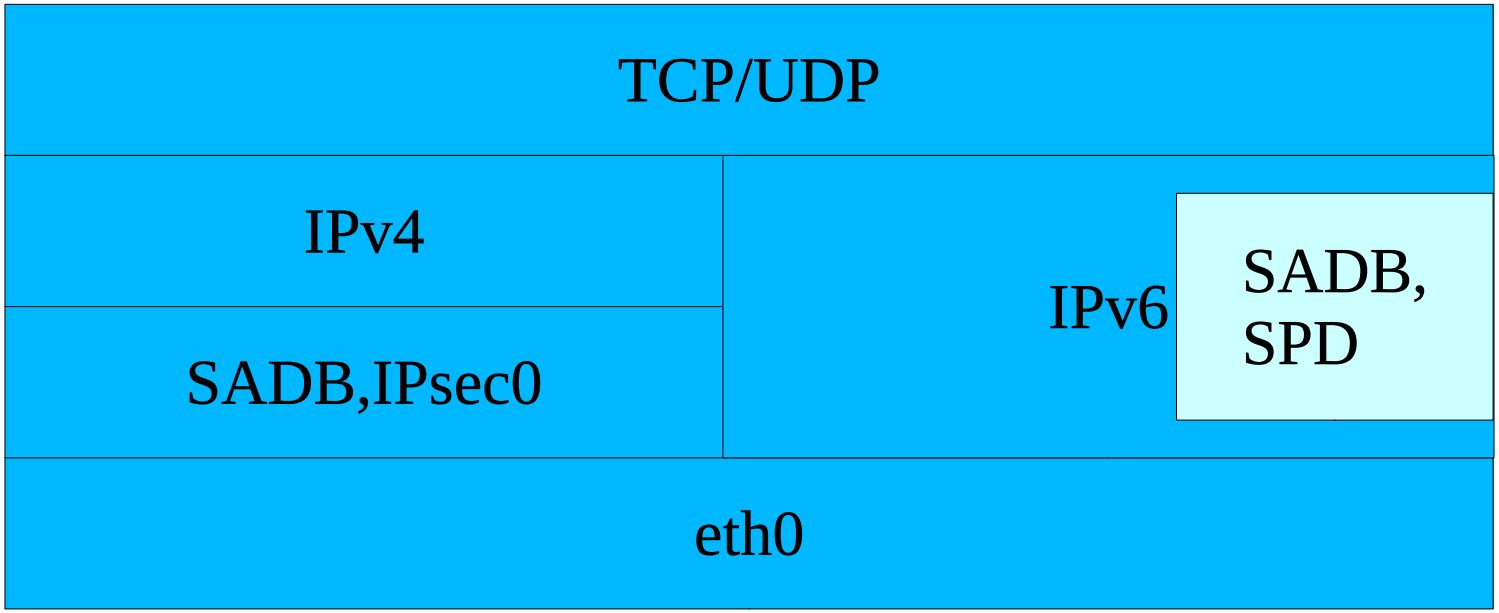
- SA, SP の手動設定
  - pfkey コマンドを提供
  - ipsec-conf スクリプトにより設定の保存、ロードが可能
- IKE
  - FreeS/WAN の IKE デーモン (Pluto) を改造し使用

FreeS/WAN の実装



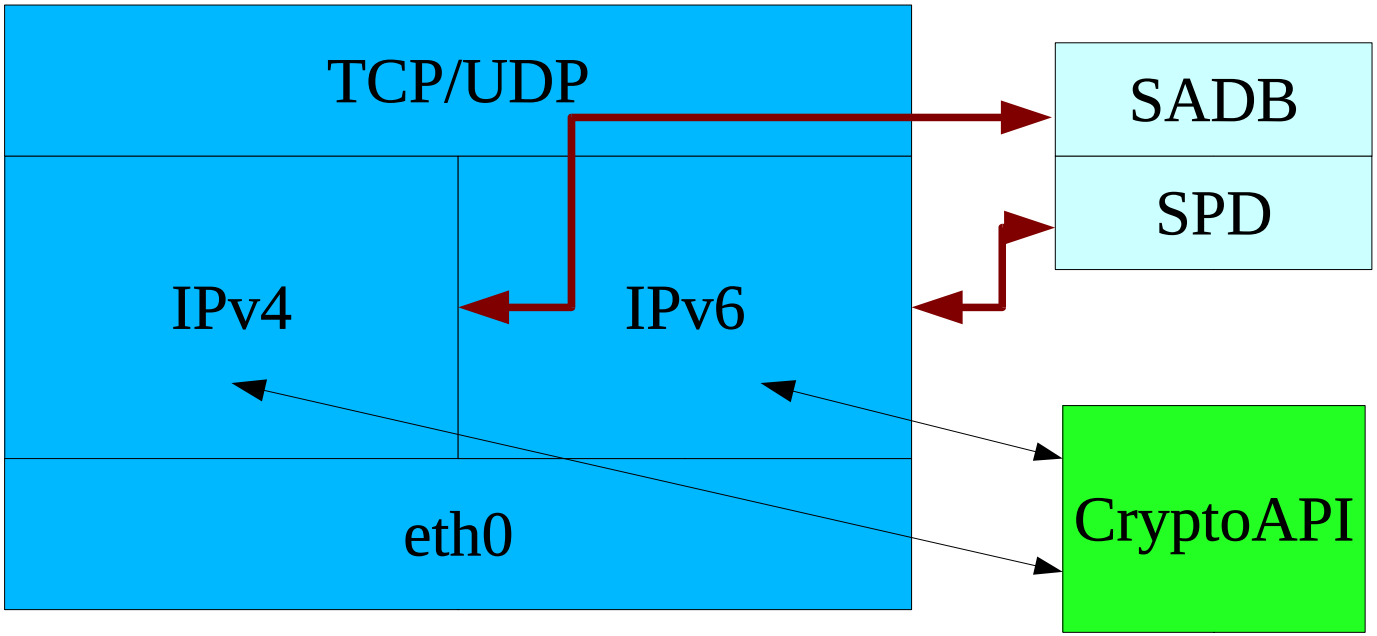
Security Policy は routing と IPsec デバイスにより決定

IADB の実装



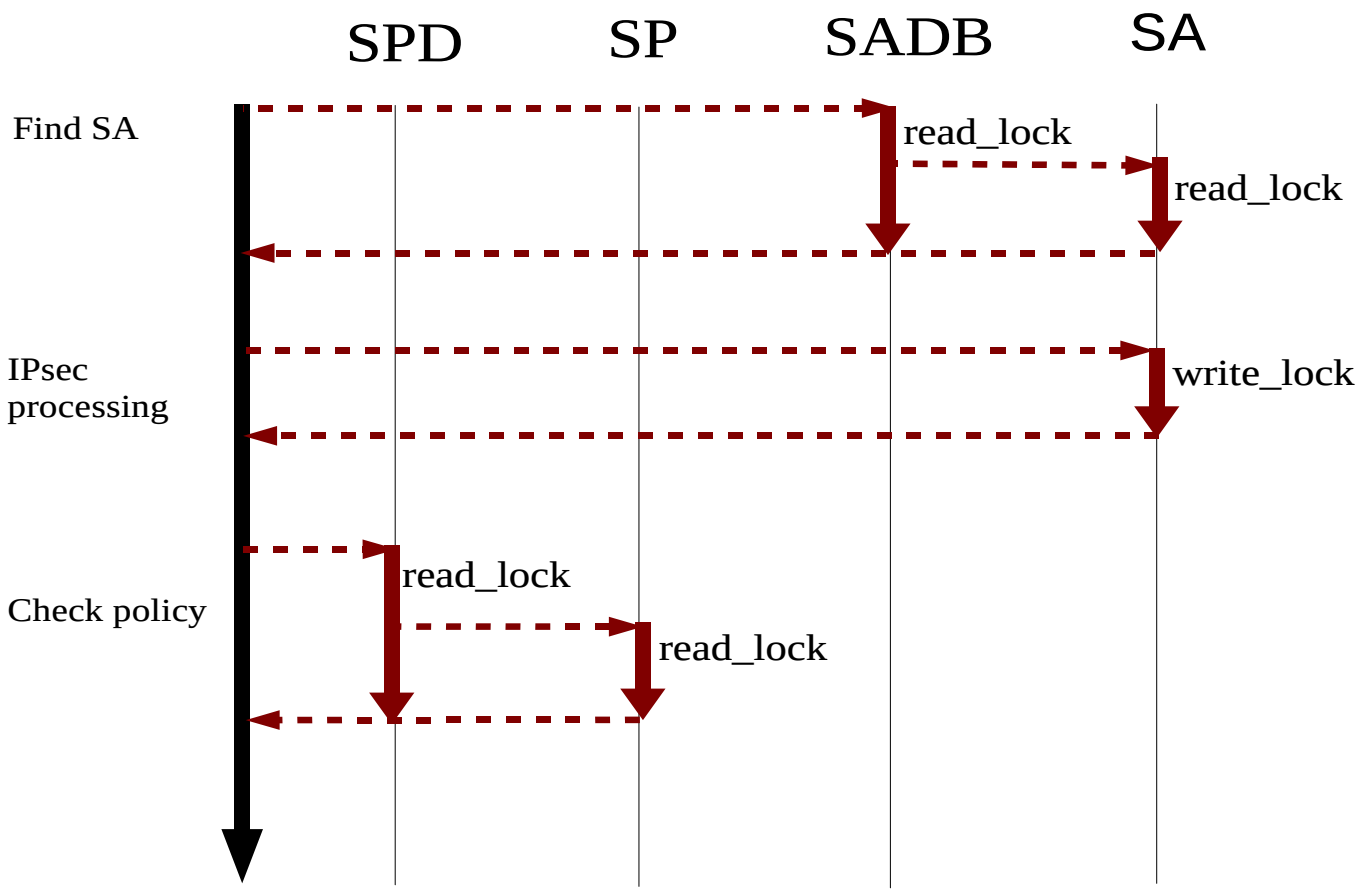
SADB,SPD は IPv6,IPv4 で別

USAGIの実装



IPのバージョンに極力依存しない作り

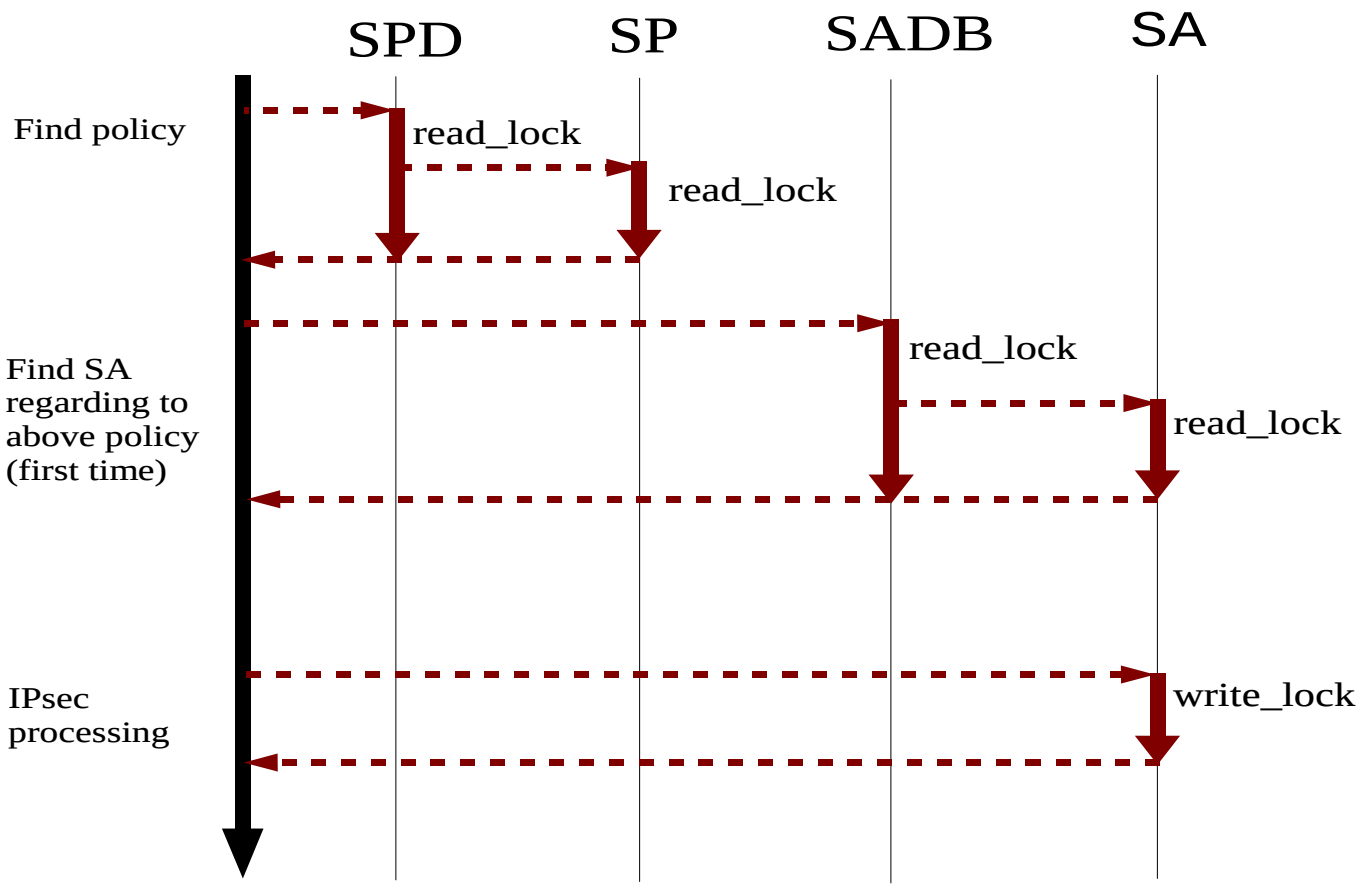
USAGI IPsec input 処理



USAGI IPsec input 処理 (続き)

1. パケット受信
2. AH/ESP ヘッダの SPI 値より SA の検索
3. AH ヘッダの場合完全性のチェック、 ESP ヘッダ場合復号化を行う
4. Policy のチェック

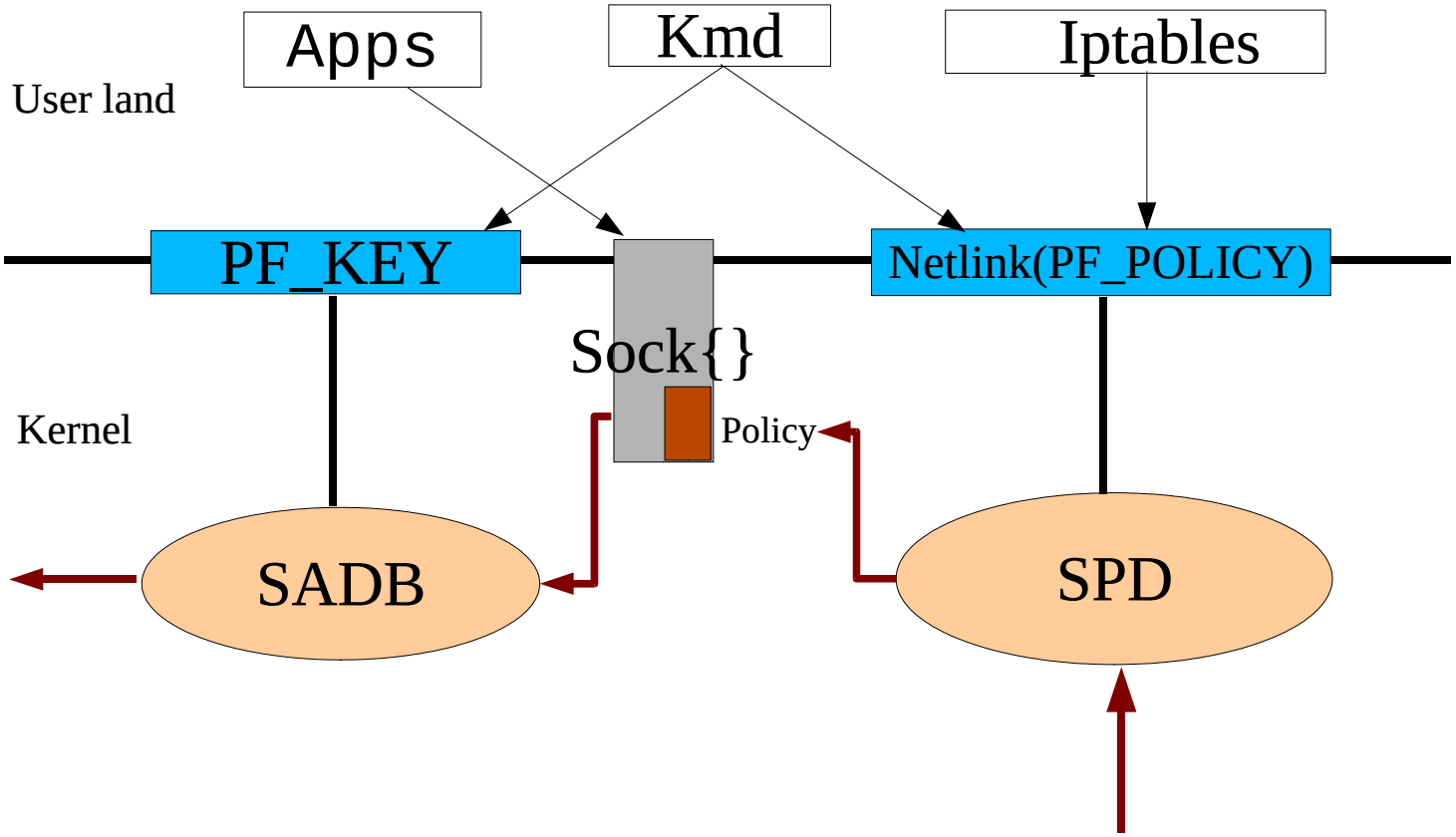
USAGI IPsec output 処理



USAGI IPsec output 処理 (続き)

1. Policy のチェック
2. SA の検索
3. IPsec の適用 (暗号化処理など)
4. パケット送出

USAGI IPsec 将来構想



Mainline kernelへのマージ

- 2002年10末にkernel2.5の新機能導入期限設定された
- 現在マージされたものは、バグフィックス関連のみ
- これから上記の期限までに機能毎の小さいパッチを作成しnetdev/linux-kernelメーリングリストへ投げる
- もちろんどれだけ受け入れられるかは不明

まとめ

- 2002 年 9 月末に 4 回目の Stable release
- これからマージへの活動を活発化
- http://www.linux-ipv6.org/
- ftp://ftp.linux-ipv6.org
- メーリングリスト
  - usagi-users@linux-ipv6.org （英語）
  - users@jp.ipv6.org （日本語）