

第4回 Admintech.jp 勉強会
新しくなったIPsec
～IPsec v3とIKE v2～

2007/06/09

宮本 久仁男 a.k.a wakatono
wakatono@todo.gr.jp



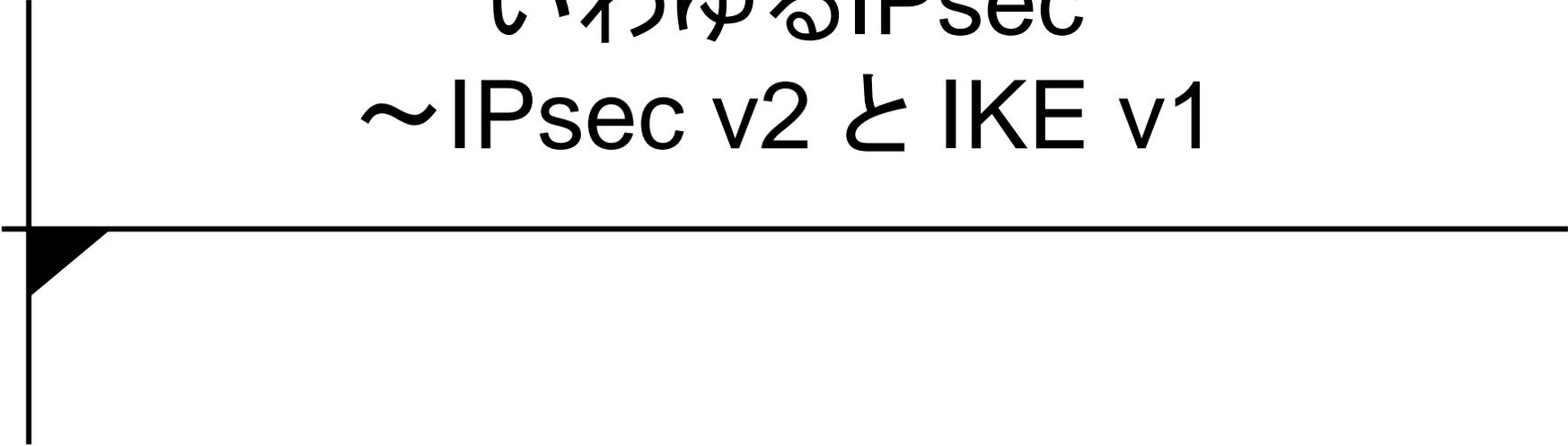
wakatonohakonnana

- Microsoft MVP(Windows – Security)
 - 2004年10月～2007年9月
- Slashdot Japan (<http://slashdot.jp/>) の編集者の顔も
 - かれこれ7年目？
 - 現状、時間が...orz
- セキュリティキャンプ(2004,2005,2006)講師
- あちこちに寄稿してる人
 - インフラ(基盤)まわりの技術に興味があるんで、そっち方面の寄稿活動もやってます
- フツーに会社員
 - 実はこれでも普通に会社に勤めてます(笑)
 - 入社してからOS,ネットワークシステム,社内サポセン,管理系業務,etc...
- フツーに大学生(現在D2)
 - ...ホントに大丈夫かな...(汗

Contents.

- いわゆるIPsec～IPsec v2 と IKE v1
- 従来のIPsecの問題点
- 改善されたIPsec～IPsec v3とIKE v2
- 改善されたIPsec～使える実装は？
- Windowsでの実装は？
- 参考文献

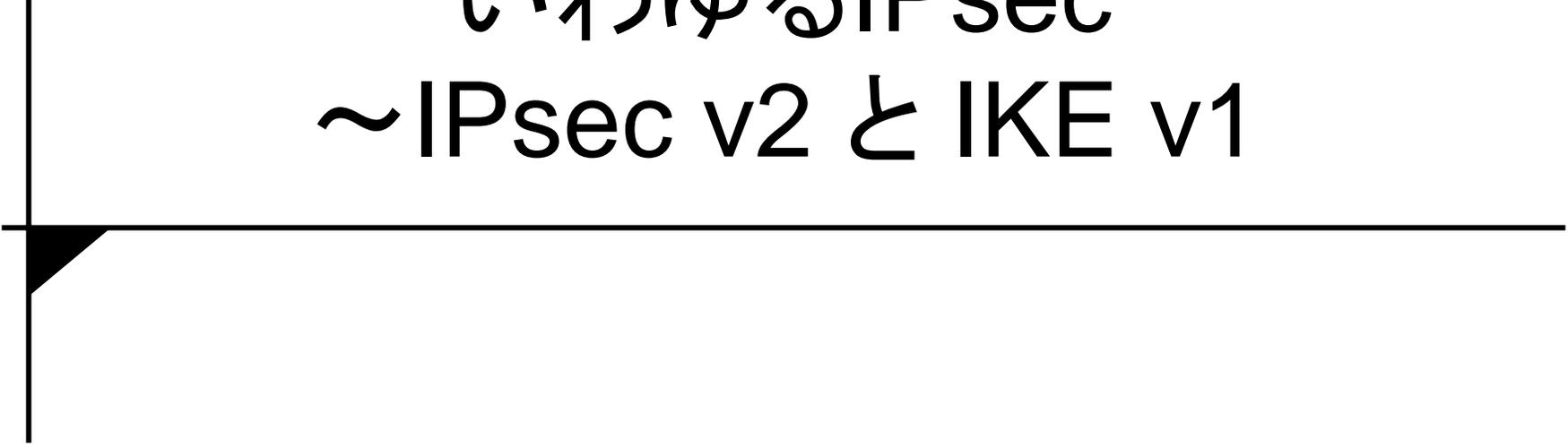
いわゆるIPsec
~IPsec v2 と IKE v1



IPsecの基本的な構造

- 1つの規約で全てを決めない
 - それでも最低限の要求条件は決定する
- 基本的な仕様を「実装可能なレベル」で規定
- 暗号化通信と、暗号化通信のための鍵の交換は別々に規定
 - IPsecとIKEを別々に規定
- 必要に応じて規約を追加

いわゆるIPsec
~ IPsec v2 と IKE v1

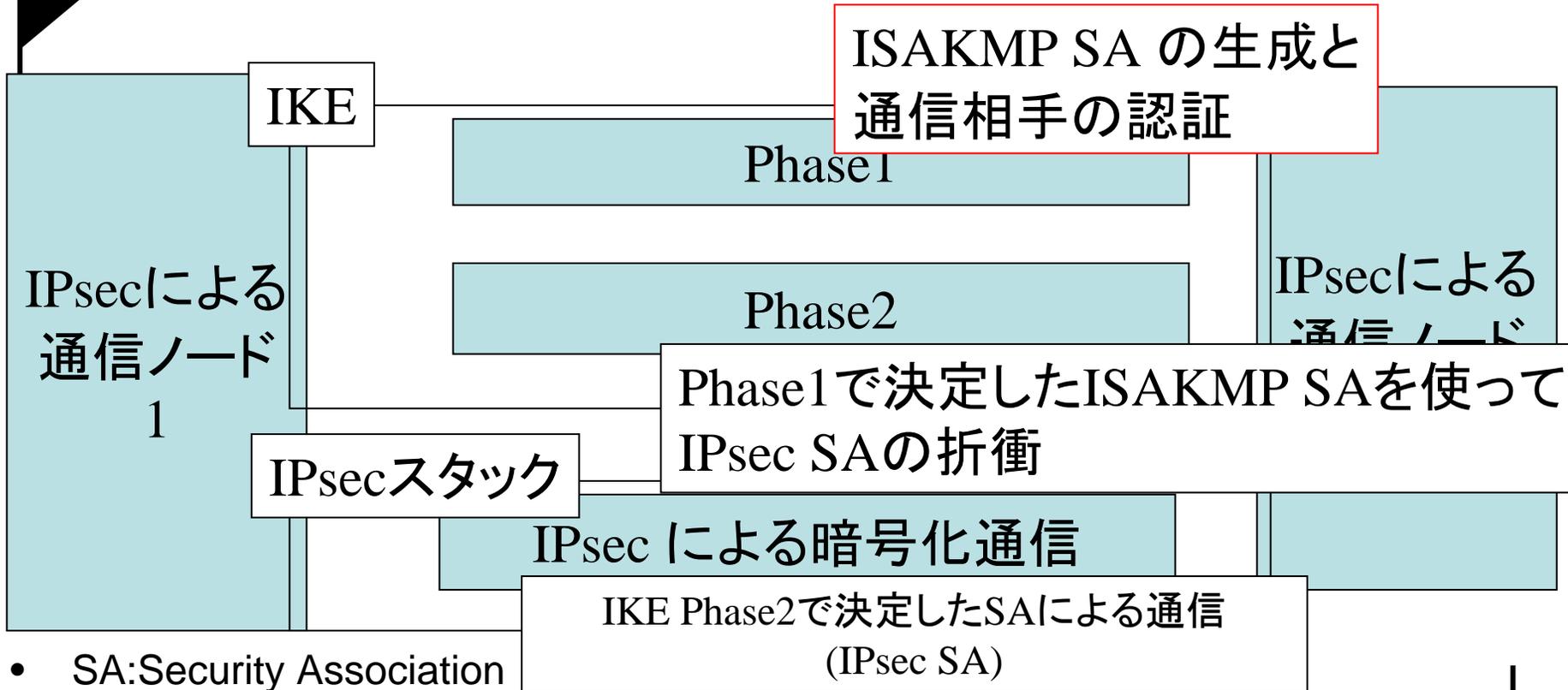




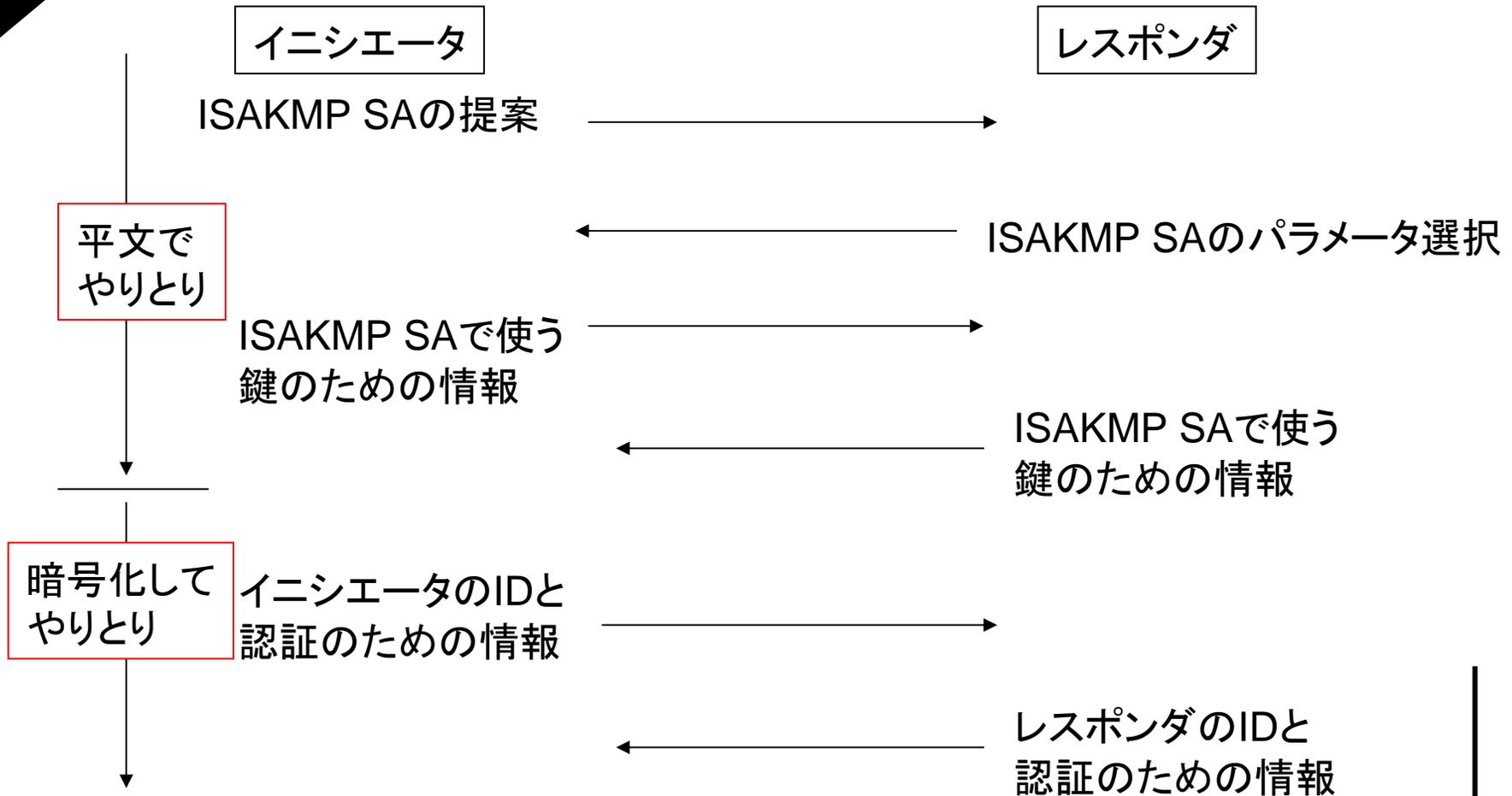
IPsec v2とIKE v1

- 現在のIPsec VPNに対応した機器や、IPsec対応の通信スタック等に実装されている
 - Checkpoint VPN-1、NetScreen、YAMAHA製ルータ、etc...
 - Windows 2000以降、Linux, Solaris, etc...
 - 数千円で売られているブロードバンドルータにも実装されていることも

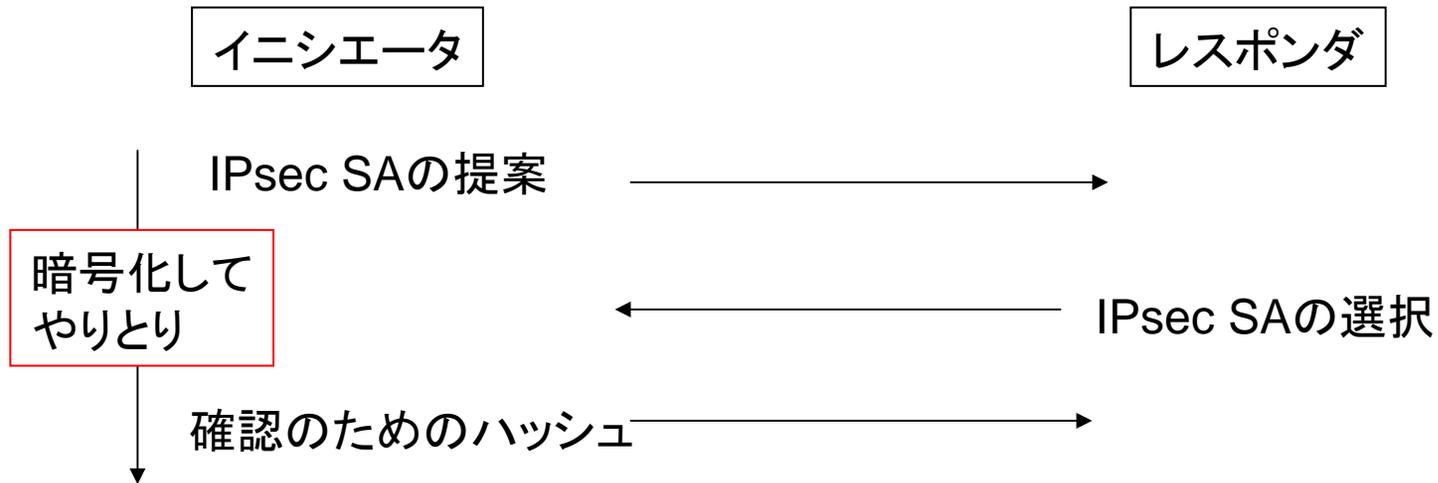
IKE v1とIPsec



Phase1 (ISAKMP SAの開設)

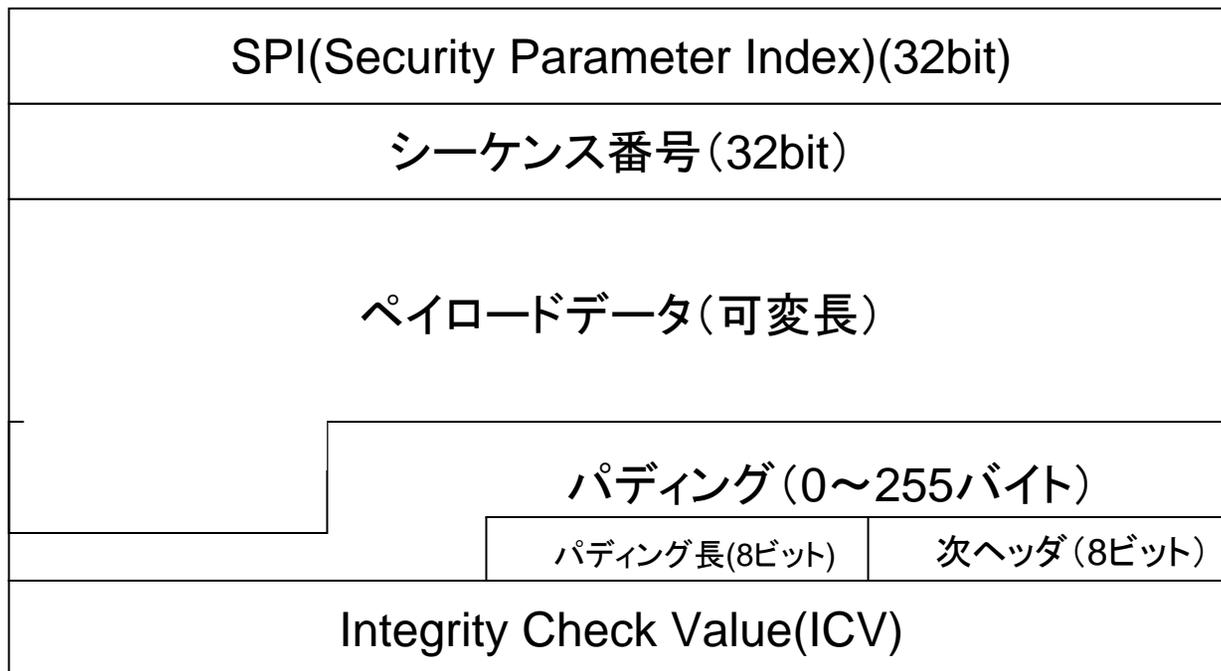


Phase2(IPsec SAの決定)



- Phase1で相手の認証、Phase2でIPsecのためのパラメータ交換を実施する

IPsec v2のパケット形式



- ペイロードの中には暗号化されないこともある
 - パケット認証のみを目的とする場合

従来のIPsecの問題点

これで何が問題なのか

IKE v1の問題点

- 仕様があいまい
- プロトコルインタラクションが複雑
 - 上記2点は相互接続性の欠如に一役買っている
- must要件であるCIPHERアルゴリズムがすでに危殆化
 - 暗号として役に立たないレベル(特にDESやMD5)

IPsec v2の問題点

- IKEほど深刻ではないが...
- カウンタのサイズがすでに小さい
 - 32bitのリプレイ防止用のカウンタがすでに小さい
- must要件になっているCIPHERアルゴリズムが危殆化
 - ここはIKEと同様
- 通信データのサイズまで隠蔽できない
 - 暗号化／圧縮はするが、サイズの調整などはしない

改善されたIPsec ～IPsec v3とIKE v2

変わったところを見よう

IKE v2とIPsec v3

- かわってないところ
 - IKEヘッダの形式
- かわったところ
 - IKEのプロトコルインタラクション
 - IPsecパケットのフォーマット
 - 各種呼称
 - mustとなる暗号化アルゴリズム
 - etc...

IPsec v3で必須の暗号化・ 認証アルゴリズム



- IPsec v2
 - DESとMD5、SHA1、そしてNULLが必須(RFC2403~2405、2410)
- IPsec v3
 - 暗号化アルゴリズムはNULLとTriple DES
 - 認証アルゴリズムはNULLとSHA1
 - 強く推奨されている暗号化アルゴリズムはAES
 - 強く推奨されている認証アルゴリズムはAES
 - 具体的には、RFC4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) で規定
 - RFC4305では、“MUST”や“SHOULD”だけでなく“MUST-”や“SHOULD+”などという表記も見られる
 - “MUST-”は、「今は必須だが、いずれ必須ではなくなる」
 - “SHOULD+”は「今は推奨にとどめておくが、将来は“MUST”になる」
 - IPsec v2で必須だったDESは、“SHOULD NOT”になっている

IKEヘッダ (v1, v2共通)

IKE_SA Initiator's SPI(64ビット)

IKE_SA Responder's SPI(64ビット)

v1、v2の間でこの部分に入る値が変わってくる

Next Payload (8ビット)	Major Version (4ビット)	Minor Version (4ビット)	Exchange Type (8ビット)	Flags (8ビット)
------------------------	----------------------------	----------------------------	-------------------------	-----------------

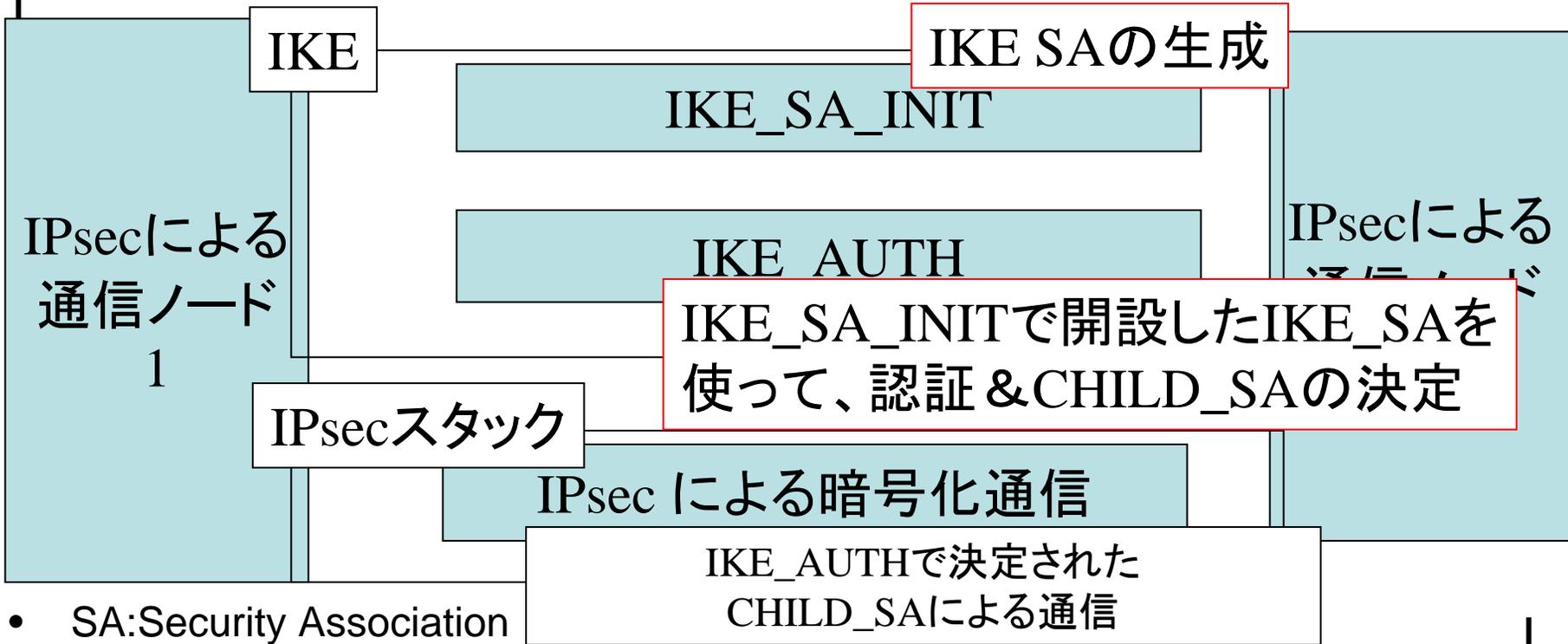
Message ID(32ビット)

Message Length(32ビット)

ヘッダは共通でも

- Next Payloadフィールドに入る値は異なる
 - KE v1の場合は0～32が割り当てられる
 - IKE v2の場合は0および33～127が割り当てられる
 - 0は、Next Payloadはないという意味なので、IKE v1、v2ともに使われる
- Exchange Typeフィールドに入る値も異なる
 - IKE v1の場合は0～33が割り当てられる
 - IKE v2の場合は34～37が割り当てられる
 - それ以降239までは予約
 - RFC2408でDOI Specific Useとされていた範囲のうち、IKE v1ですでに使われている32と33以外の部分をIKE v2で使う
- IKEv1とIKEv2の両方をサポートするIKEを実装する場合には、Major Version, Minor Version, Next Payload, Exchange Typeの値を見て、その後の処理を決める必要がある

IKE v2とIPsec



- SA: Security Association
- IKE: Internet Key Exchange

IKEv1とIKEv2の対応

- Phase 1(IKE v1)
 - ISAKMP SAのパラメータ合意および、パラメータ合意を行った相手の認証を実施
 - パラメータ合意までは、IKE_SA_INIT(IKE v2)に対応
 - IKE_SAとISAKMP SAは、双方向の暗号化通信路であることは変わらない
 - 認証以降は、IKE_AUTH(IKE v2)に対応
- Phase 2(IKE v1)
 - IPsec SAのパラメータ合意
 - IKE_AUTH(IKE v2)に対応
 - IKE_AUTHで交換されるパラメータの一部としてCHILD_SAのパラメータがある
 - IKE v2では、IPsec SAという言い方はせず、CHILD_SAという言い方になっている
 - » IPsec SAとCHILD_SAは、片方向のSAであることは変わらない(行きと帰りで異なる鍵を用いて暗号化・署名されている)

IKE_SA_INITでのやりとり

イニシエータ

IKE SAの提案と、
IKE SAで使う鍵の
ための情報

レスポнда

IKE SAの選択と、
IKE SAで使う鍵の
ための情報

- この時点でまだ、イニシエータとレスポндаの間での認証は行わない
 - あくまでIKEが用いるSA(暗号化通信路)のパラメータを握るまで

IKE_AUTHでのやりとり

イニシエータ

レスポнда

イニシエータのID
認証情報
提案するCHILD_SA
提案するプロトコルセレクタ

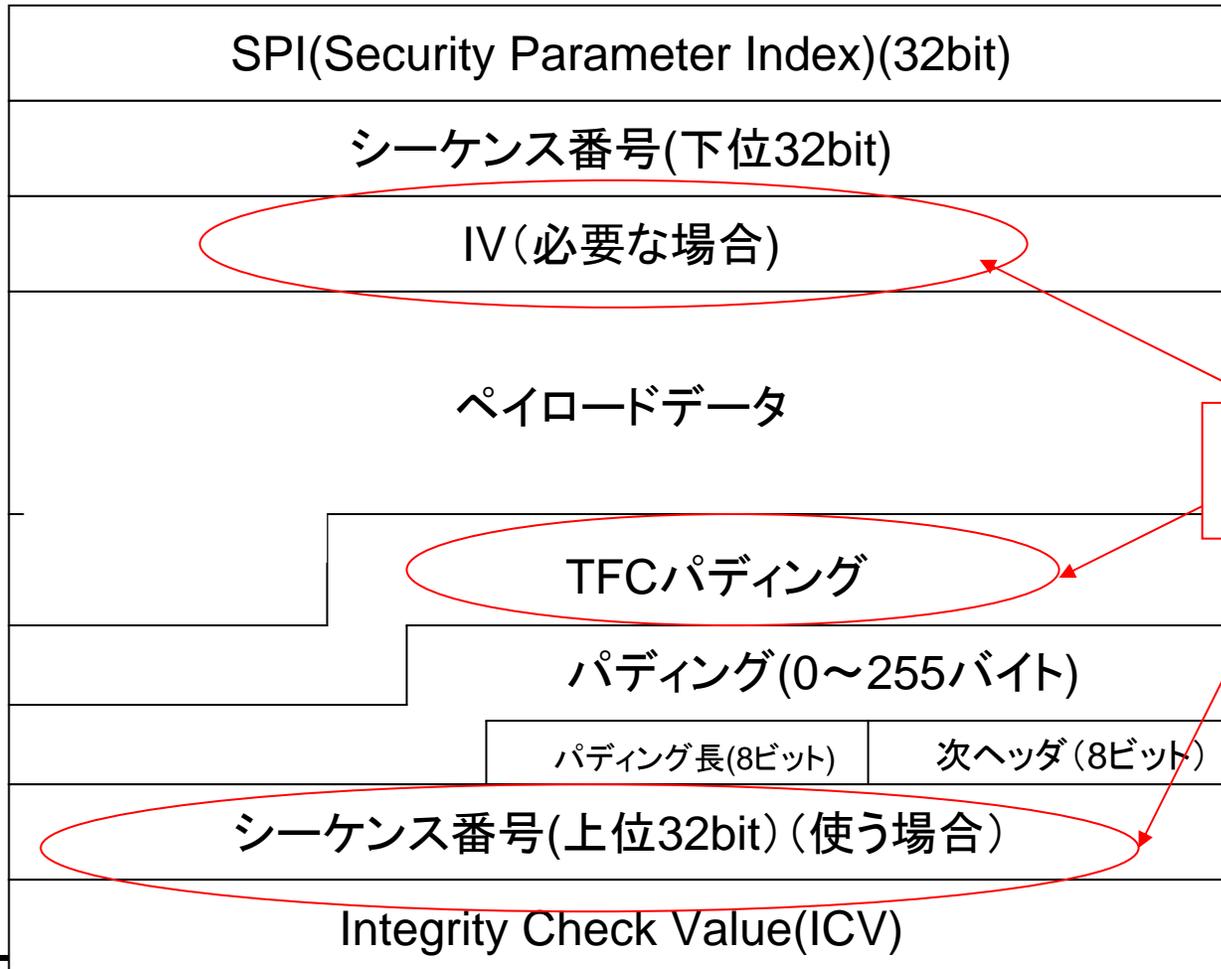


レスポндаのID
認証情報
選択するCHILD_SA
選択するプロトコルセレクタ

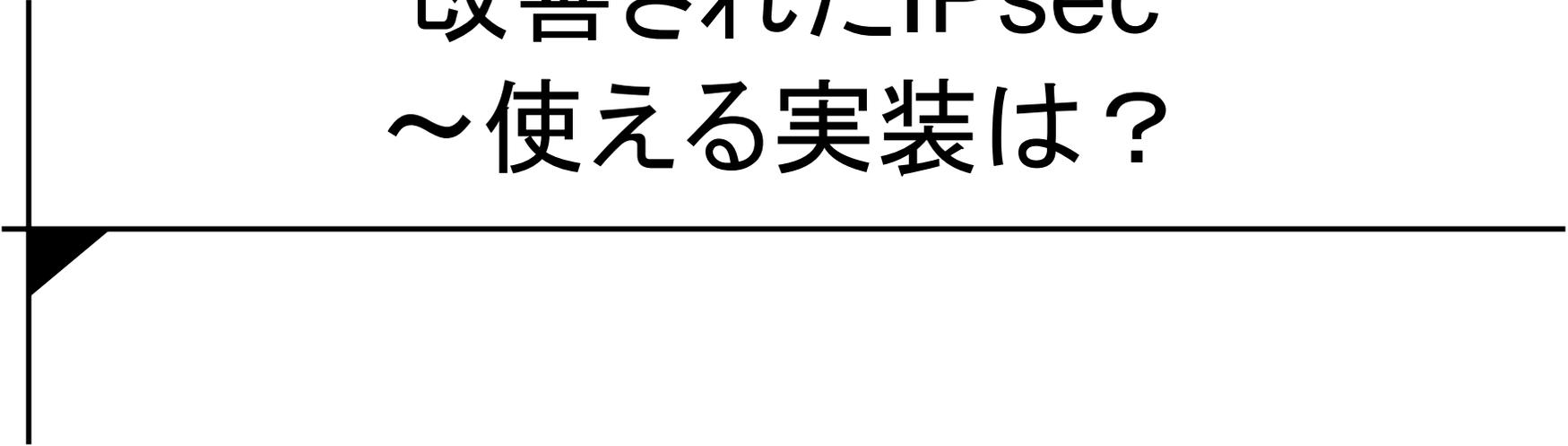


- 相互認証と、IPsec通信のためのパラメータの合意を一度に実施する

IPsec v3の packets 形式



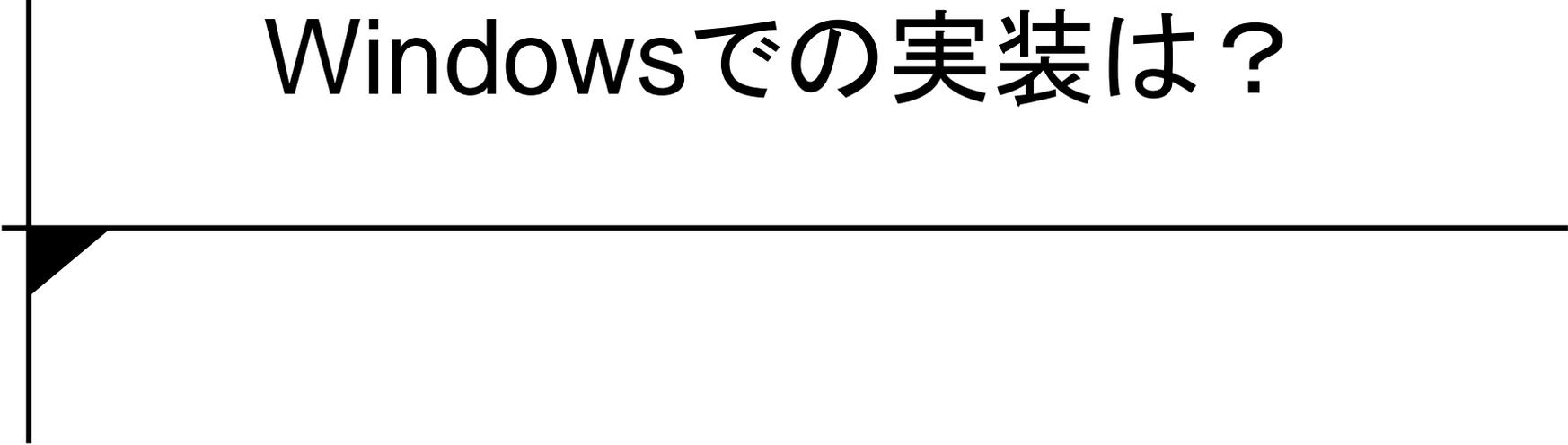
改善されたIPsec
～使える実装は？



実際に探して試せたもの

- IKEv2ではracoon2が使えるがIPsec v3はまだ見当たらない
 - IKEv2をサポートする実装として、WIDE Projectの坂根昌一氏によるracoon2がある
 - IPsec v3を実装しているものは見当たらない
 - プロトコルがFIXされたのが比較的最近であることが大きいと推測
- 試すには？
 - IPsec通信が行える環境で、racoon2をbuild、設定してやるだけ
 - **IKEの仕様とIPsecの仕様が独立のため**、IKE v2 + IPsec v2という組み合わせでも普通に動作する(確認済み)
- TheRacoon2Project
<http://www.racoon2.wide.ad.jp/w/>

Windowsでの実装は？

A decorative L-shaped line is positioned on the left side of the slide. It consists of a vertical line segment on the left and a horizontal line segment extending to the right. At the bottom-left corner where the two lines meet, there is a small black right-angled triangle pointing towards the top-right.

Windowsでの実装は？

- 残念ながら、ありませんorz
 - Vistaの実装ですらも、IKE v1とIPsec v2の組み合わせ
- 作れば試せます（但しVista以降）
 - Vistaでは、IKEとIPsecが実装上分離されている
 - IPsecスタックでの鍵設定のためのAPIがある
 - IKE v2だけ試すというのも可能
 - Windows Server 2003R2までは、IPsecスタックとIKEが不可分だったため、試そうとするとまるごと全部入れ替える必要があった

課題

- racoon2のコードがUNIX系OSに依存したものである
– 当然といえば当然
– 鍵設定のAPIまわりは、Windowsにあわせる必要がある
– 通信ポリシーの部分の互換をどうやって取るか
 - 未調査
- 試すための環境を作るのに一苦労
 - まず相互接続のための環境を組める必要がある
 - これがちょっと大変かも

参考文献





参考文献(1/2)

- マスタリングIPsec 第2版(オライリー)
- 『マスタリングIPsec』サポートページ
 - <http://www.tatsuyababa.com/MasteringIPsec/>
 - 第1版のPDF(IKEv1やIPsec v2に関連する部分)がダウンロード可能
- Software Design 2007年6月号
特集 VPN徹底攻略 2007
 - Appendix 1: IPsec最前線(拙著)
- TheRacoon2Project
 - <http://www.racoon2.wide.ad.jp/w/>

参考文献(2/2)

- IPsec v3およびIKE v2に関連したRFC
 - RFC4301 Security Architecture for the Internet Protocol
 - RFC4302 IP Authentication Header
 - RFC4303 IP Encapsulating Security Payload (ESP)
 - RFC4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
 - RFC4306 Internet Key Exchange (IKEv2) Protocol
 - RFC4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- IPsec v2およびIKE v1に関連したRFC
 - RFC2406 IP Encapsulating Security Payload (ESP)
 - RFC2408 Internet Security Association and Key Management Protocol (ISAKMP)
 - RFC2409 The Internet Key Exchange (IKE)
 - The ISAKMP Configuration Method
 - <http://tools.ietf.org/html/draft-dukes-ike-mode-cfg-00>



Let's Enjoy Encrypted and Tunneled Communication 😊