Understanding IKEv2 Tutorial, and rational decisions

渡邊研究室
00J120　保母雅敏

1. Introduction

- IKEとは
  - IPsecのために相互認証を行い、SAを確立するプロトコル
  - かつてはISAKMP/OAKLEYと呼ばれていた
- IKEv1
  - RFC2407,2408,2409がベース
  - NAT-Traversal、Legacy Authentication、リモートアドレスの取得などの機能を追加

- IKEv2
  - IKEv1での身元隠匿、PFS、2つのフェイズ、 暗号交渉などを継承
  - IKEv1での問題を、不要な変更を行わないで修正することが目的

2. Overview of IKEv2

①暗号化アルゴリズムの取り決め

②双方の認証

③セッションキーの作成

①の暗号化を使用

IKE-SAの確立

- **追加要求**
  - Information Message
    - peerの生存を確認するnullメッセージ
    - SAを削除するようなメッセージ

    など
  - Child-SA Request
    - 任意のDiffie-Hellman exchange、ノンス、アドレス、ポート、プロトコルの種類を指示するトラフィックセレクター値の取り決め

3. Two Phases

- First Phase
  - IKE-SAの確立
- Second Phase
  - IPsec-SA(Child-SA)の確立

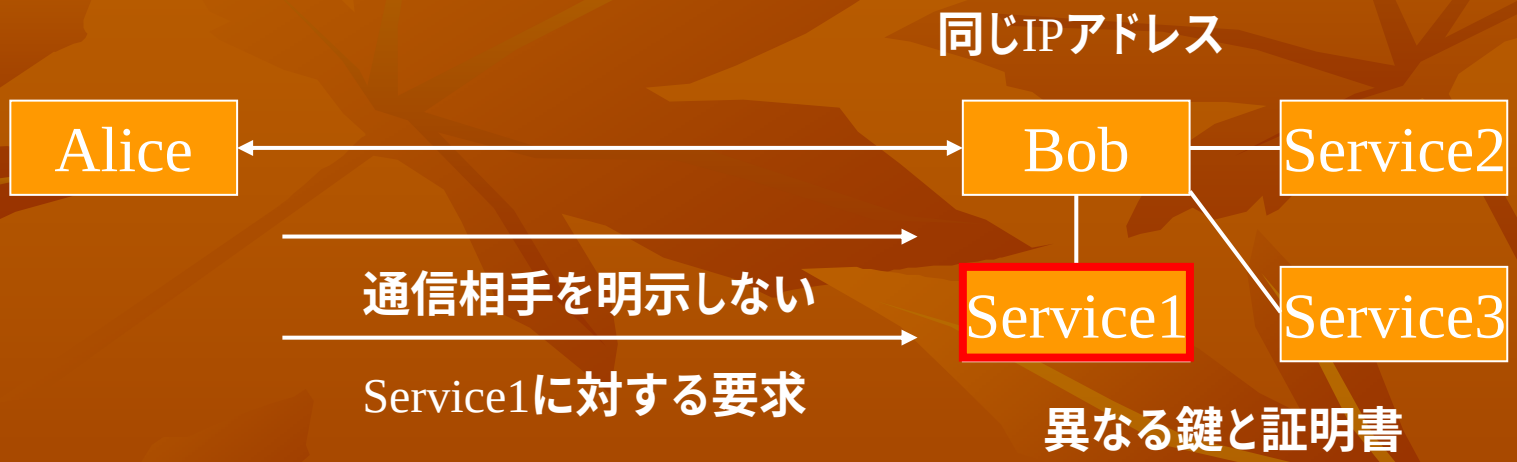
IKEv2では、フェイズの概念を削除

- 任意数のIPsec-SAを作成することの有用性
  - 同じSA以外への多重送信の防止
  - 異なるフローのセキュリティプロパティへの対応
  - 異なるサービスクラスのためのSAへの対応

4. Perfect Forward Secrecy /Computation Tradeoff

- ある鍵を知られても、その鍵で暗号化したメッセージ以外には被害が及ばないこと
- IKEv2では
  - ノンス（セッション毎に異なる乱数）
  - Diffie-Hellman Number（再利用の可能性有り）

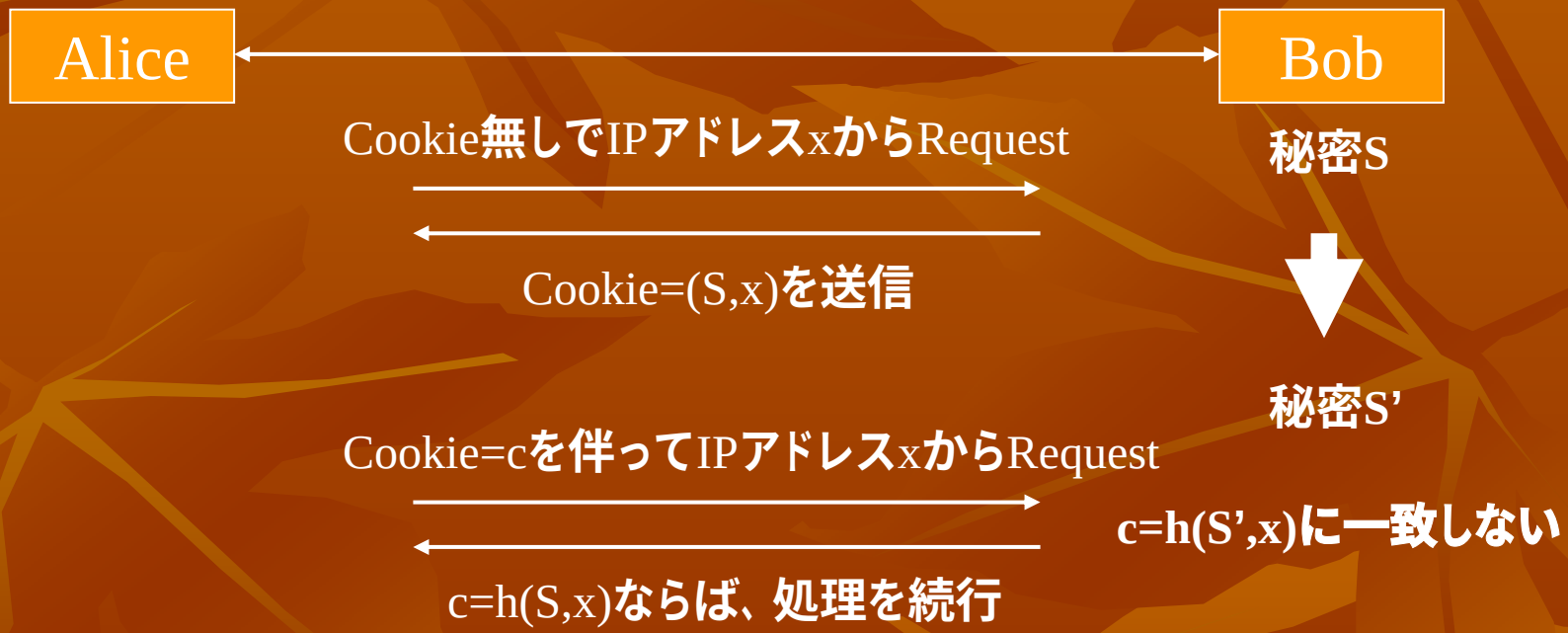
5. Colocated Services



- 明細な証明書の記述
  - 特定の身元を要求することが可能

6. DOS protection

- Stateless Cookie



- IKEv2におけるStateless Cookieの扱い
  - Stateless CookieはRound Tripとして扱う(OAKLEYスタイル)
    - 特別なRound Tripなしで提供できる
    - Under Attackを強制的に決定するのを回避する
    - Initial Pre-exchange後はStatelessではなくなる簡単なプロトコル
    - Fragmentation Attackからの防御を容易にする
      - IKE-exchangeメッセージ3から証明書が含まれるため、メッセージは分割して送信される

7. Cryptographic Negotiation

- IKEv1では”a la carte”
  - それぞれのアルゴリズムが独立してネゴシエーション可能
  - アルゴリズムは指数関数的に拡大
- IKEv2では
  - 基本的には”a la carte”を継承
  - Suitesを組み込むことを許可

- Suites
  - 全ての要素は単一のSuiteに符号化される
  - ネゴシエーションではひとつ以上のSuiteを提供
  - 相手から提供されたSuiteを所持することも可能
- “a la carte”と比較した利点
  - アルゴリズムの増加を抑制
  - 簡単でよりコンパクトな符号化が可能
- “a la carte”と比較した欠点
  - IKEv1からの変更は面倒
  - 柔軟性に欠ける

8. Acquiring an IP address

FWを通した通信

①内部ネットワークに属するIPアドレスのみを所持

→インターネットに属するIPアドレスを与える

②インターネットに属するIPアドレスのみを所持

→内部ネットワークに属するIPアドレスを与える

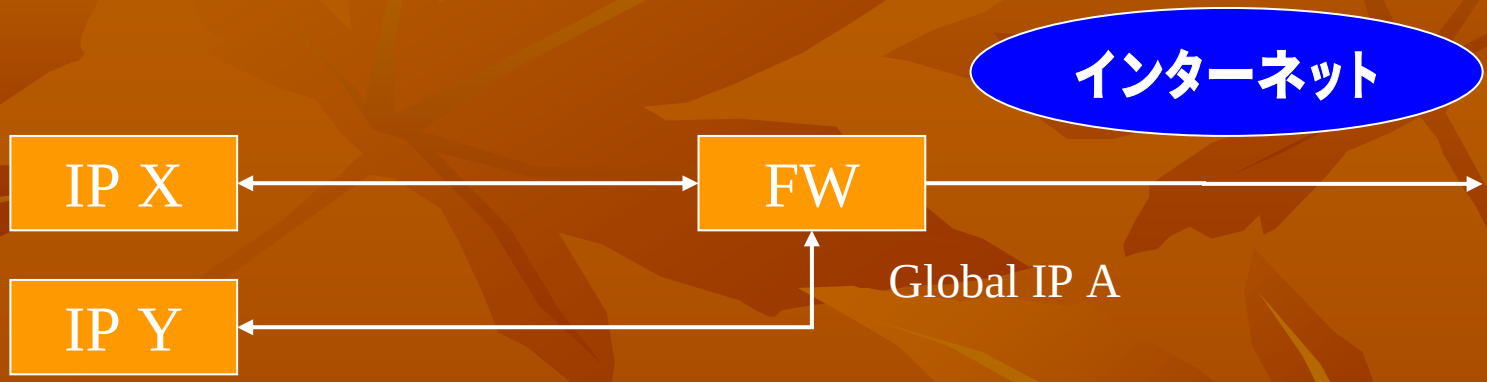
- MODECFG
  - IPアドレスを教える際にIKE exchangeのフィールドを含む
    - IPsecセッション設定で、メッセージ数や暗号化作業を最小化することが可能
    - IPアドレスをリースする以外の目的でトンネルされたDHCPを排除しない
    - 一般的に必要とされている機能を提供できるため、IKEv2ではこちらを使う事が多い
- DHCP-relay
  - IKE上またはESP上に特殊なコネクションを設置する
    - MODECFGよりも柔軟性がある
    - IKEの仕様から独立して作成することが可能
    - クライアント-サーバ間の認証で使われる

9. NAT-Traversal

NAT Mapping Table	
Private IP	Global IP
X	A
Y	B
・・・	・・・

- 内部ノードに対して十分なGlobal IPがある場合に有効

- NAPT（IP masquerade）
  - TCPやUDPポートを基にアドレス変換を行うもの



コネクションの確立

送信パケット

送信元アドレスをIP A、Port αに変更

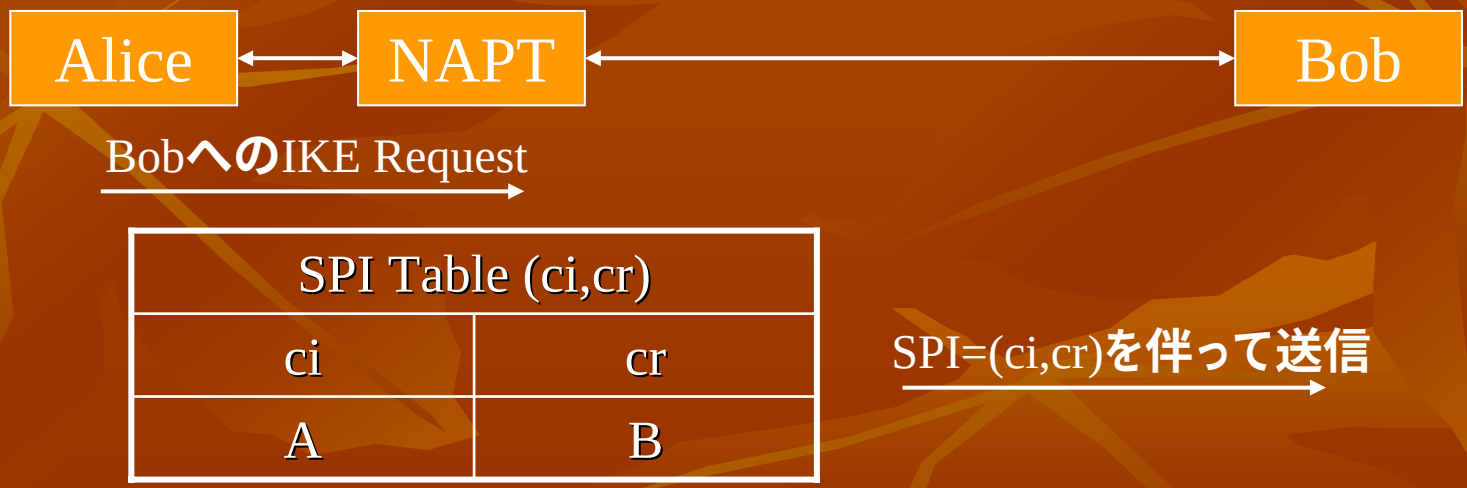
受信パケット

Mapping Tableを元に
IP Xに転送

NAPT Mapping Table		
Private IP	Global IP	Port
X	A	α
Y	A	β
・・・	・・・	・・・

- IKEとNAT
  - IKEメッセージはUDP　port=500を必要とする

- IKE SPI
  - UDP　port=500に対して特別なmappingを行う



10. Identity Hiding

- IKEv2では受動的攻撃者からの隠蔽は容易
- 能動的攻撃者からの隠蔽
  - IKEv2では、公開署名鍵と予め共有した鍵をサポート
- 公開署名鍵の欠点
  - 片方が最初に身元を明らかにする必要がある

  - 開始者の身元を守る必要性

11. Legacy Authentication

- Legacy Authenticationに対して提案された機能
  - XAUTH、EAP、CRACKなど
- IKEv2ではEAPが採用

- 主なLegacy Authenticationの種類
  - MD5チャレンジ
    - クライアントはハッシュを計算する必要がある
    - テキスト文字列を再現することは出来ない
  - OTP
    - Human-with-paperかclient-computed-hashを選択
  - トークンカード
    - 応答する側にテキスト文字列を表示
    - 表示された文字列を打ち込みサーバに送り返す