Library

KASAGO IPv6(Dual)オプション: IPsecセキュリティプロトコル

KASAGO® IPsec IKEv1, KASAGO® IPsec IKEv1 /IKEv2

KASAGO IPsec IKEv1、KASAGO IPsec IKEv1/IKEv2は、図研エルミックのTCP/IPプロトコルミドルウェア「KASAGO IPv6(Dual)」の高機能オプションです。
IPsec技術を使い、インターネット上でやりとりされるデータを暗号化するセキュリティプロトコルです。

KASAGO IPsec IKEv1はIPsecセキュア通信のSA(通信ごとの設定情報)を確立するための鍵交換プロトコル"IKE"の、バージョン1に対応しています。KASAGO IPsec IKEv1/IKEv2はバージョン1と2の両方をサポートしています。
IKEv2は、リモートアクセス、EAP(拡張認証)やCOOKIEなどの機能が新たに加わり、より高度で幅広い認証方式、相互接続性の向上を実現し、将来は現在の主流であるIKEv1に置き換わる規格です。

特長

共通

- AH、ESP、IKEをサポート
- 各アルゴリズムをモジュール化。ユーザー独自モジュール(ソフト/ハード)の使用も可能
- NAT-T対応
- 自社開発製品。開発スタッフによるサポート、カスタマイズサービスを提供
- サンプルアプリケーションを提供

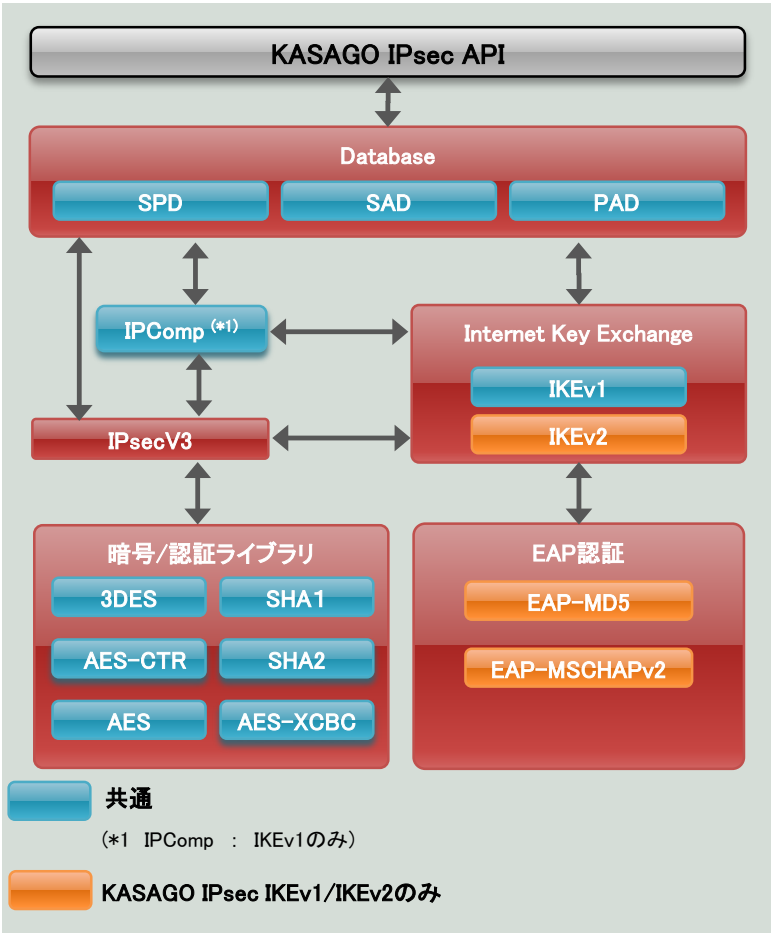
KASAGO IPsec IKEv1独自機能

- IPComp対応

KASAGO IPsec IKEv1/IKEv2独自機能

- EAPをサポート
  ユーザ名を使用した認証が可能
- COOKIE をサポート
  IKE 連続接続攻撃に対抗
- リモートアクセス機能
  仮想IP の割り当てによってIPsec で保護されたリモートネットワークへのアクセスが可能
- マルチプロポーザル (AH + ESP)

サポートアルゴリズムの詳細は裏面をご参照ください。



サポートする機能

IPsec機能

IPsecプロトコル	AH, ESP(認証あり), IPComp
暗号アルゴリズム	トランスポートモード, トンネルモード
カプセル化モード	DES, 3DES, CAST128, BLOWFISH, AES(128, 192, 256ビット), AES-CTR, NULL暗号
認証アルゴリズム	MD5, SHA, RIPEMD, SHA2(256, 384, 512), AES-XCBC ※AH及びESPでサポート
	DEFLATE
	IPsec, Bypass, Discard
拡張機能	64ビット拡張シーケンス番号(ESN), TFCパディング, ESPパケットのUDPカプセル化

IKEv1機能

Phase-1換　モード	メインモード, アグレッシブモード
Phase-2換　モード	クイックモード
暗号アルゴリズム	DES, 3DES, CAST128, BLOWFISH, AES (128, 192, 256ビット), NULL暗号
ハッシュアルゴリズム	MD5, SHA, SHA2(256, 384, 512)
認証方式	既知共鍵　, デジタル署名認証(RSA/DSA)
Diffie-Hellman	Group 1, 2, 5, 14
拡張機能	NAT-T, マルチプロポーザル(AH + ESP, ESP + IPComp , AH + ESP + IPComp)

IKEv2機能 （IPsec/IKEv2のみ）

IKE換　タイプ	IKE_SA_INIT換　, IKE_AUTH換　, CREATE_CHILD_SA換　, INFORMATIONAL換
暗号アルゴリズム	DES, 3DES, CAST128, BLOWFISH, AES(128, 192, 256ビット), NULL暗号
ハッシュアルゴリズム	MD5, SHA, SHA2(256, 384, 512)
認証方式	既知共鍵　, デジタル署名認証(RSA), EAP-MD5, EAP-MS-CHAPv2
Diffie-Hellman	Group 1, 2, 5, 14
拡張機能	NAT-T, マルチプロポーザル(AH + ESP)

Elmic

図研エルミック株式会社

URL:https://www.elwsc.co.jp　　e-mail: info@elwsc.co.jp

横 浜 本 社 〒222-8505　横浜市港北区新横浜3-1-1　図研新横浜ビル2F
Tel:045-624-8002 ／ Fax:045-476-1102
大阪営業所　〒532-0011　大阪市淀川区西中島4-3-22　新大阪長谷ビル8F
Tel:06-4396-8430 ／ Fax:06-4396-8431

2019/7/2