日本ネットワークセキュリティ協会
Japan Network Security Association

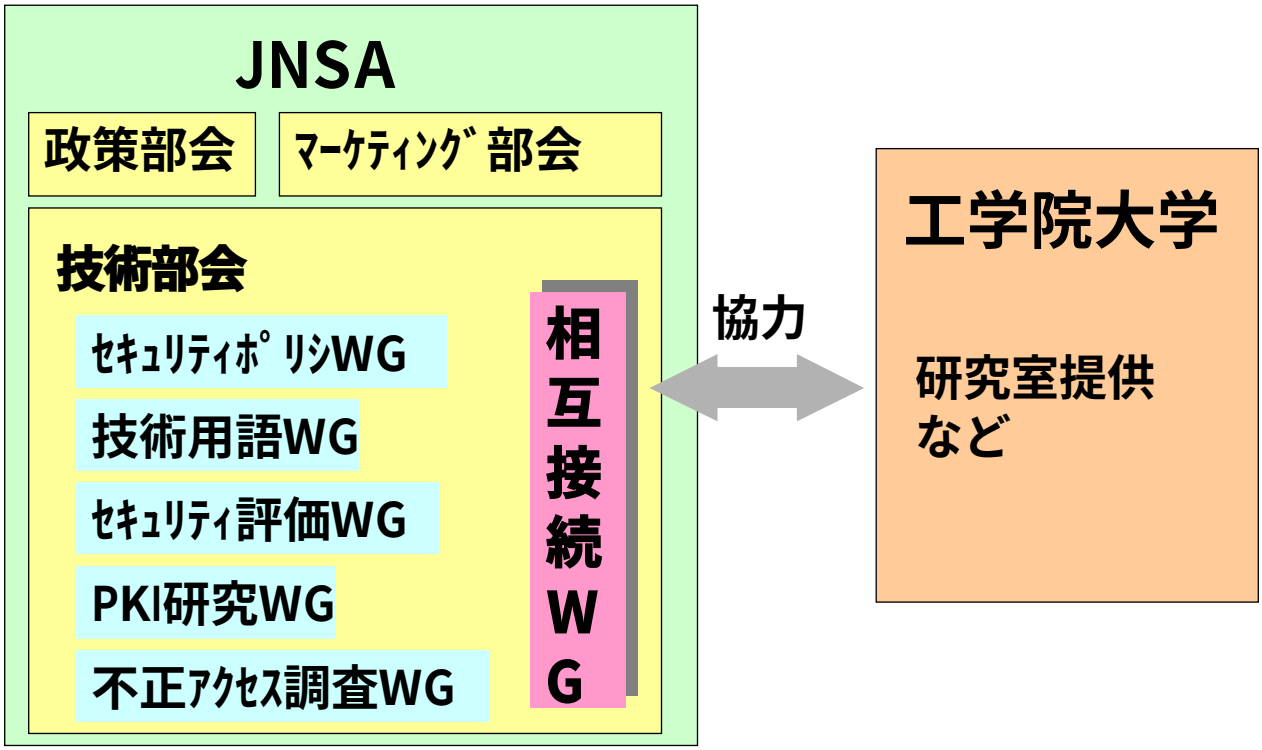
JNSA

相互接続ワーキンググループ

活動結果発表

2001 年 5 月 17 日

相互接続ワーキンググループ



相互接続Working Groupの目的

JNSA

- セキュリティプロダクトの技術要件検証のための評価試験環境を提供する。
- 試験で得られた情報は一般公開する。

第一回 IPSec相互接続試験目的

- 目的
  - IPSec機器の接続性の確認
  - IPSec機器の運用性の確認
  - 試験結果をメーカにフィードバックする事による、IPSecプロダクト全体の接続性の向上

第一回 IPSec相互接続試験

JNSA

- **期間**
  - 平成12年11月28日～平成13年2月28日
- **試験会場**
  - 工学院大学新宿キャンパス 1611研究室
- **参加企業および参加機器**
  - 24社 34製品 (詳細は別紙参照)
    - IPSecGateway製品　24製品
    - IPSec Client製品　6製品
    - CA局　3製品
    - アナライザ　1製品

試験参加機器一覧

第一回 JNSA相互接続実験参加機器

2001/2/2

1．Ｇａｔｅｗａｙ製品

1) LAN Gateway

	製造メーカ	製品名	Version	参加メンバー
1	Nortel Networks	Contivity Extranet Switch	V2.61	ネットワンシステムズ(株)
2	Ａｌｃａｔｅｌ	PERMIT/Gateシリーズ	v.3.10.010	(株)ディアイティ/(株)CRC総合研究所
3	Ｃｈｅｃｋpoint	VPN-1 (Solaris版)	v4.1 sp2	(株)フォーバルクリエーティブ/新日鉄ソリューションズ(株)
4	Ｃｈｅｃｋpoint	VPN-1 (WinNT版)	v4.1 sp2	(株)フォーバルクリエーティブ/新日鉄ソリューションズ(株)
5	Checkpoint	VPN-1 (Linux版)	v4.1 sp2	(株)フォーバルクリエーティブ/新日鉄ソリューションズ(株)
6	Nokia	Nokia IPシリーズ	v4.1 sp2	(株)ネットマークス/新日鉄ソリューションズ(株)
7	AlliedTelesis	AR720	2.0.2-01	アライドテレシス(株)
8	Microsoft	Windows 2000	sp1	(株)インターネット総合研究所/マイクロソフト(株)
9	WatchGuard	FireboxII	v4.5	(株)ヒューコム
10	Intel	Shiva VPN Gateway	v6.8p3	(株)ヒューコム
11	Cisco systems	VPN3005	2.5.2	シスコシステムズ(株)/ネットワンシステムズ(株)
12	Cisco systems	Cisco7100	v12.1	シスコシステムズ(株)
13	古河電工	INFONET-VP100	v02.01	古河電工(株)
14	VPNet	VSUシリーズ	v3.0.52	(株)ネットマークス
15	SSH	IPSEC Express Toolkit	v4.0	ＳＳＨコミュニケーションズ・セキュリティ(株)
16	RadGurad	clPro	v4.47	(株)東陽テクニカ
17	AXENT	PowerVPN	v6.5	(株)シマンテック/日新電機(株)
18	RedCreek	RAVLIN	3.4	日新電機(株)
19	フジクラ	FNX0531	v2.1.03	(株)フジクラ
20	Cisco systems	PIX		シスコシステムズ(株)
21	富士通	NetShelter	E11L10	(株)ピーエフユー/(株)富士通北陸システムズ

2) Dialup Gateway

	製造メーカ	製品名	Version	参加メンバー
22	古河電工	MUCHO-EV	v30.0	古河電工(株)
23	古河電工	MUCHO-EV/PK	v40.0	古河電工(株)
24	フジクラ	FNX0510	v2.1.01	(株)フジクラ

提供機器一覧

IPSec相互接続試験 提供機器一覧

2001/2/2

3．CA局

	製造メーカ	製品名	Version	協力ベンダー
1	Baltimore	UniCERT	v3.0.1	日本ボルチモアテクノロジーズ(株)
2	SSH	Certifier	v1.0.2	ＳＳＨ コミュニケーションズ・セキュリティ(株)
3	Entrust	Entrust	v4.0v5.0	セコムトラストネット(株)

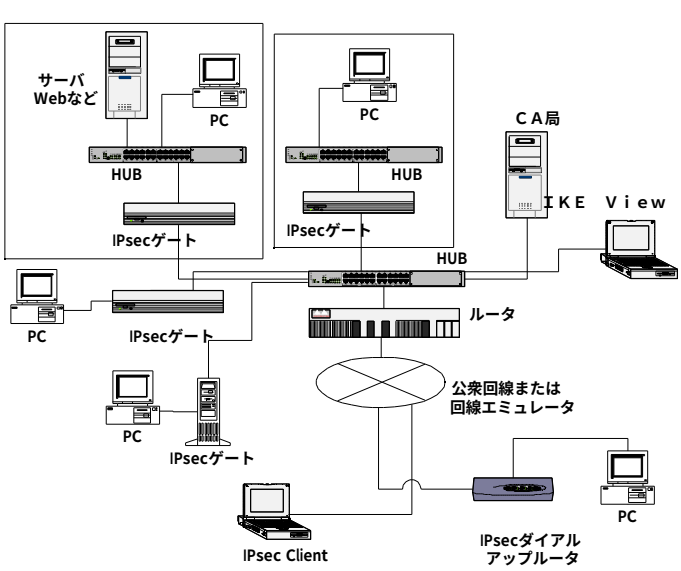
4．アナライザ

	製造メーカ	製品名	Version	協力ベンダー
1	松下電工	IKEVIEW	v1.5	松下電工(株)

5．設備

		協力ベンダー
1	1611研究室	学校法人 工学院大学
2	OCN回線	エヌ・ティ・ティ・コミュニケーションズ(株)

試験環境



- 基本的にはローカルネットワークで試験を実施する。
- Dialupルータや、クライアント接続試験時にダイアルアップ環境や、リモート接続環境が必要な場合は、回線シュミレータを使用し試験を実施する。

試験項目

- **基本試験**
  - **相互接続性確認試験**
    - **各製品の基本的な接続性を確認**
      - Pre-Shard**相互認証方式の接続確認**
      - Phase2 ID**ペイロードタイプ確認試験**
      - **通信中の**Re-key**動作確認**
  - **運用性確認試験**
    - IPSec**機器の機種や機能に関わらず、**IPSec**機器を運用する際に確認が必要な項目**
      - IP**フラグメンテーション発生時の通信試験**
      - SA**消失に関する試験**
      - End to End**通信試験（ｱﾌﾟﾘｹｰｼｮﾝ動作試験)**
      - SA LifeTime**の確認**

試験項目

- オプション試験
  - 相互接続性確認試験
    - デジタル署名による相互認証など、RFCで実装必須となっていない項目を使用した際の接続性を確認
      - デジタル署名相互認証方式の接続性確認
      - Public-key相互認証方式の接続性確認
      - NAT Traversal接続試験
  - 運用性確認試験
    - IPSec機器の機能や機種に関係する運用性の確認
    - IPSec機器を運用する際に有益となる情報取得の為の試験
      - NAT動作確認試験(NAT使用時のIPSec通信)
      - CAに関する試験(証明書の取得方法やCRLの参照方式)
      - 性能試験
      - 回線障害試験

試験結果(基本試験/相互接続性確認)

- Pre-Shard相互認証方式の接続確認
  - パラメータ
    - 暗号方式：DES
    - ハッシュ：MD5、SHA1
    - 鍵素材：DH Group1
    - 認証方式：HMAC-MD5、HMAC-SHA1
    - PFS

試験結果(基本試験/相互接続性確認)

- Pre-Shard相互認証方式の接続確認

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ	◎																			
3	VPN-1 (Solaris版)		◎																		
4	VPN-1 (WinNT版)	◎	◎																		
5	VPN-1 (Linux版)		◎																		
7	Nokia IPシリーズ	◎	○																		
8	AR720	◎	◎	○																	
9	Windows 2000	○	◎				◎	◎													
10	Fireboxll	●P					●P		●P												
11	Shiva VPN Gateway	◎	◎				◎	◎	◎	●P											
14	VPN3005	○	◎	◎	◎	◎			○	●P	◎										
15	Cisco IOS	◎	◎	◎	◎	◎			◎	●P	◎	◎									
16	INFONET-VP100	◎		◎	◎	◎	◎	◎	◎	●P	◎	◎	◎								
17	VSUシリーズ	◎	◎					◎	◎	●P	◎	◎	◎	◎							
18	IPSEC Express Toolkit	◎	◎	◎			◎	◎		●P	◎	◎	◎	◎	◎						
19	CIPro	◎	◎	◎		◎		◎	◎	●P	◎	◎	◎	◎	◎	◎					
20	PowerVPN	◎	◎	◎		◎	◎	◎	◎	●P	◎	◎	◎	◎	◎	◎P	◎				
21	RAVLIN	◎	◎		◎		◎	◎	◎	●P	◎	◎	◎	◎	◎	◎	◎	◎			
22	FNX0531	◎P	◎P	◎P	◎P	◎P		◎P		●P	◎P	◎P	◎P	◎P	◎P	◎P	◎P	◎P	◎P		
25	NetShelter		◎							●P	◎	◎	◎	◎	◎	◎	◎		◎	◎	

◎：ハッシュを MD5、SHA-1で指定して接続できたもの

○：MD5 のみで接続確認できたもの

●：SHA-1 のみで接続確認できたもの

P ：PFS を OFF

試験結果(基本試験/相互接続性確認)

- Pre-Shard相互認証方式の接続確認
  - 試験結果
    - 試験を実施した組合せのすべてについて接続を確認。
    - 機器間ごとにネゴシエーションからIPSec通信が開始されるまでの所要時間に差がでた。

試験結果(基本試験/相互接続性確認)

- Phase2 IDペイロードタイプ確認試験
  - Phase2 ID Payload Type
    ⇒ IPsecによる通信保護の対象
  - 「Host」単位、「Subnet」単位、相互異なるPayload Typeを指定した場合のSA確立の可否を確認。

試験結果(基本試験/相互接続性確認)

- Phase2 IDペイロードタイプ確認試験

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ																				
3	VPN-1 (Solaris版)		◎																		
4	VPN-1 (WinNT版)																				
5	VPN-1 (Linux版)																				
7	Nokia IPシリーズ																				
8	AR720																				
9	Windows 2000						○														
10	Fireboxll		◎				○														
11	Shiva VPN Gateway		◎				○	◎													
14	VPN3005	◎	◎	○	○																
15	Cisco IOS	◎	◎	○	○	○			◎	◎	◎	◎									
16	INFONET-VP100		◎			○	○		◎		○		◎								
17	VSUシリーズ		◎					◎	◎	○	○		◎	◎							
18	IPSEC Express Toolkit	◎	◎	○		○	○		○	○	◎	◎	◎	◎	◎						
19	CIPro		○			○	○		◎				◎		◎	◎					
20	PowerVPN		◎			○	○	○	○		◎	◎	◎		◎	○	◎				
21	RAVLIN		◎		○				○	○	○		○		○	◎	◎				
22	FNX0531	◎	◎							○	○	◎	◎	○	◎	○			◎		
25	NetShelter		◎							◎	◎	◎	◎	◎	◎	◎	◎		◎		

◎：すべての組み合わせで接続

○：subnet同士、 host同士の組み合わせで接続

試験結果(基本試験/相互接続性確認)

- Phase2 IDペイロードタイプ確認試験
  - 試験結果
    - 異なるPayload Typeでの組み合わせでも接続可能なケースが多く見受けられた。
      ⇒本来は拒否するべき。
      ⇒確立されたSAの確認が必要。

試験結果(基本試験/相互接続性確認)

- **通信中の**Re-key**動作確認**
  - **一方向から、継続的な通信を発生させ、通信が継続して行えることを確認。**
  - Initiator**、**Responder**の入れ替え。**
  - **相互異なる** LifeTime**を指定。**

  - **通信は途絶えていないか？**
  - Re-key **が問題無く行えているか？**
  - **どちらが、**Re-key**を開始しているか？**

試験結果(基本試験/相互接続性確認)

- 通信中のRe-key動作確認

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ																				
3	VPN-1 (Solaris版)		◎																		
4	VPN-1 (WinNT版)		◎																		
5	VPN-1 (Linux版)		◎																		
7	Nokia IPシリーズ																				
8	AR720			○																	
9	Windows 2000																				
10	Fireboxll						○														
11	Shiva VPN Gateway	◎	○				◎	○	○	◎											
14	VPN3005	◎	○	○	○	◎				○											
15	Cisco IOS	○	○	○	○	○			○	○	◎	○									
16	INFONET-VP100	○	○		◎			○	○	○	◎		◎								
17	VSUシリーズ	○	◎					○	○	○	◎	○	○	◎							
18	IPSEC Express Toolkit	○	○	○	○	○	○	○	◎		◎		○	○							
19	CIPro	○	○			○	◎	○		○	◎	○	○	○	◎	◎					
20	PowerVPN	○	○	○		○		○	○	○	○		○		○		◎				
21	RAVLIN	○	○		○	◎	◎	◎	○	○	◎	○	○	○	×	◎	◎	○			
22	FNX0531	◎	○	◎	◎	◎		○		○	◎	◎	◎	◎	○	○	×#1	○	◎		
25	NetShelter		○							○	◎	○	○	○	○	○	○	○	×	○	

◎：双方向で re-key 動作を確認
○：一方向のみ re-keyを確認
×：re-key に失敗した項目を持つもの
#1:Rekeyは完了したが途中で 30秒ほどの通信不能な期間あり。

試験結果(基本試験/相互接続性確認)

- 通信中のRe-key動作確認
  - 試験結果
    - InitiateがOKでも、Re-keyで、NGの場合があった。

    - ◎、○だからと言って、必ずOKとは限らない。
    - ×だからと言って、必ずNGとは限らない。

      ⇒LifeTime の組合わせによって、Re-keyの成否が左右される場合がある。

      ⇒各社製品の実装を確認する必要がある。

試験結果(基本試験/相互接続性確認)

- **通信中の**Re-key**動作確認**
  - Re-key**を成功させるためのヒント（各社製品の実装を確認）**
    - Re-key**タイミングの確認**
      - SA Life Time **に対して一定の割合が経過した時。**
      - SA Life Time **までの残り時間が規定の秒数に達した時。**

        ⇩
      - SA**が存在。**
      - SA**が存在かつトラフィックが発生。**
    - Responder **側の** LifeTime **通知**
      - RESPONDER LIFETIME
    - **削除ペイロード**(Delete Payload)
      - ISAKMP SA Delete
      - IPSec SA Delete

試験結果(基本試験/運用性確認)

- IPフラグメンテーション発生時の通信試験
  - ESPヘッダの増加によるパケットサイズの増大
    ⇒フラグメント要
  - DF(Don't flagment)ビット = ON or OFF の場合について
    IPSec装置がどう振舞うかを確認。

試験結果(基本試験/運用性確認)

JNSA

- IPフラグメンテーション発生時の通信試験

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ																				
3	VPN-1 (Solaris版)		○																		
4	VPN-1 (WinNT版)		○																		
5	VPN-1 (Linux版)																				
7	Nokia IPシリーズ																				
8	AR720		●																		
9	Windows 2000																				
10	Fireboxll																				
11	Shiva VPN Gateway	●	●	○	○			●													
14	VPN3005	●	●																		
15	Cisco IOS	○	○							○	○										
16	INFONET-VP100	○	○	○	○					○		○									
17	VSUシリーズ							●		○	○			○							
18	IPSEC Express Toolkit			○		○				○				○							
19	CIPro		○								○	○		○		○					
20	PowerVPN			○																	
21	RAVLIN			○												○		○			
22	FNX0531		●	○											○				○		
25	NetShelter			○	○										●					●	

○：DF セットしない場合は通信可

●：いずれの場合も通信可

試験結果(基本試験/運用性確認)

- IPフラグメンテーション発生時の通信試験
  - 試験結果
    - DF（Don’t Flagment）ビット＝OFF
      - 一様にパケットのフラグメント（分割）が行われた。
    - DF（Don’t Flagment）ビット＝ON
      - ハードウェア製品では、フラグメントする傾向が多かった。
      - ソフトウェア製品では、フラグメントせずに、パケット送信元ホストへICMP<dategram too big = fragmentation neeeded>/PMTUメッセージを返す傾向が多かった。
  - IPSec装置間の経路上にてフラグメントが発生する場合については未試験。

試験結果(基本試験/運用性確認)

- SA消失に関する試験
  - 一方が、不測の事態(電源断、機器障害など)によりSAの消失が発生。
    ⇒SAの不一致
  - SAが残っている側およびSAが残っていない側からの通信を発生させ、SAの再確立が行われ、IPSec通信が正常に復旧するか？

試験結果(基本試験/運用性確認)

- SA消失に関する試験

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ	○																			
3	VPN-1 (Solaris版)	○	○																		
4	VPN-1 (WinNT版)	○	○																		
5	VPN-1 (Linux版)																				
7	Nokia IPシリーズ																				
8	AR720		◎	○																	
9	Windows 2000																				
10	Fireboxll		○	○																	
11	Shiva VPN Gateway	○	◎	○	◎	◎		○		○											
14	VPN3005	○	○	○	○					○	○										
15	Cisco IOS	○	○	○						○	○	○									
16	INFONET-VP100	○	○	○	○			○		○	○	○	○								
17	VSUシリーズ							×		○	○			○							
18	IPSEC Express Toolkit		○	○	○					○		○		○	○						
19	CIPro	○	○	○						×	○	×		×							
20	PowerVPN	○	○	◎						◎							○				
21	RAVLIN	○	○	○						◎	○	○	○	○		○	×	○			
22	FNX0531	○	○	○				○		○	○	○	○	○	○			○	○		
25	NetShelter		○	×	○					○	○	○	○		○	○	×	○	○	○	

◎：いずれの場合も回復

○：消失した側より　ping送信で回復

×：回復手段なし

Shiva VPN Gateway　はSAの起動直後の動作特性によりレスポンダになることが困難であるためイニシエータのときのみを確認。

試験結果(基本試験/運用性確認)

- SA消失に関する試験
  - 結果
    - 「◎」自動復旧を行える機器はあまり無い。
    - 「○」SAが消失した側からの通信による復旧がほとんどであった。

試験結果(基本試験/運用性確認)

- End to End通信試験（ｱﾌﾟﾘｹｰｼｮﾝ動作試験)
  - 実際にアプリケーションを使用した安定動作の確認。
  - 通信中にRe-keyを発生(FTP試験のみ)
  - FTP/TCP、TFTP/UDPを使用。

試験結果(基本試験/運用性確認)

- End to End通信試験 （ｱﾌﾟﾘｹｰｼｮﾝ動作試験)

No	名称	1	2	3	4	5	7	8	9	10	11	14	15	16	17	18	19	20	21	22	25
1	Contivity Extranet Switch																				
2	PERMIT/Gateシリーズ	○																			
3	VPN-1 (Solaris版)	○	○																		
4	VPN-1 (WinNT版)	○	○																		
5	VPN-1 (Linux版)																				
7	Nokia IPシリーズ																				
8	AR720		○	○																	
9	Windows 2000																				
10	FireboxII			△																	
11	Shiva VPN Gateway	○	○	○	○			○		△											
14	VPN3005	○	○	○						△	○										
15	Cisco IOS	○	○	○																	
16	INFONET-VP100	○	○	○	○			○		△	－	○	○								
17	VSUシリーズ							○		△	×			○							
18	IPSEC Express Toolkit		○	○		○								○							
19	CIPro	○	○	○						×	○	○		○		○					
20	PowerVPN			○								○	×								
21	RAVLIN			○						△	○	○									
22	FNX0531	－	○	－				○		△	－	－	○	－	○		－	○	－		
25	NetShelter		×	○	○						○	×	×		×	○	○	○	○	×	

○：通信が正常に終了することを確認済み
×：通信で異常が認められたもの
△：FTP のみ確認。 TFTP は未試験
－：設定に誤りがあったため無効
Firebox はオペレータが UDP のフィルタを解除できていなかったため未試験相当

試験結果(基本試験/運用性確認)

- End to End通信試験（ｱﾌﾟﾘｹｰｼｮﾝ動作試験)
  - ほとんどの組み合わせで「○」
  - 「×」については、Re-key処理の遅延により、Timeout が発生したものと思われる。

総評

- 実運用で異機種間接続を行うには相応のスキルと労力が必要。
- 明確な技術的根拠に基づく「検証項目」と「判断基準」を確立していく必要がある。

機器選択のポイント

- 用途/規模に応じた機器の選択
  - トラフィックが集中するセンターで使用するのか？
    ⇒スループットや最大SA数の確認。
    ⇒リモートアクセス機能
    ⇒冗長化（フェイルオーバー）
    ⇒帯域制御（QoS）
  - SOHOで使用するのか？
    ⇒Router機能（簡易Firewall/NAT）なども兼用しているか？
    ⇒デフォルト状態でのセキュリティ設定。
    ⇒インターフェース（Ethernet、BRI、ADSL（pppoe））
    ⇒Aggressive-mode対応
  - セキュリティポリシーに合わせた機器の選択
    IPSec専用機、Firewall兼用機

今後の活動予定

- CA局
- IPv6
- ダイアルアップ、無線LAN、ｘDSL など