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

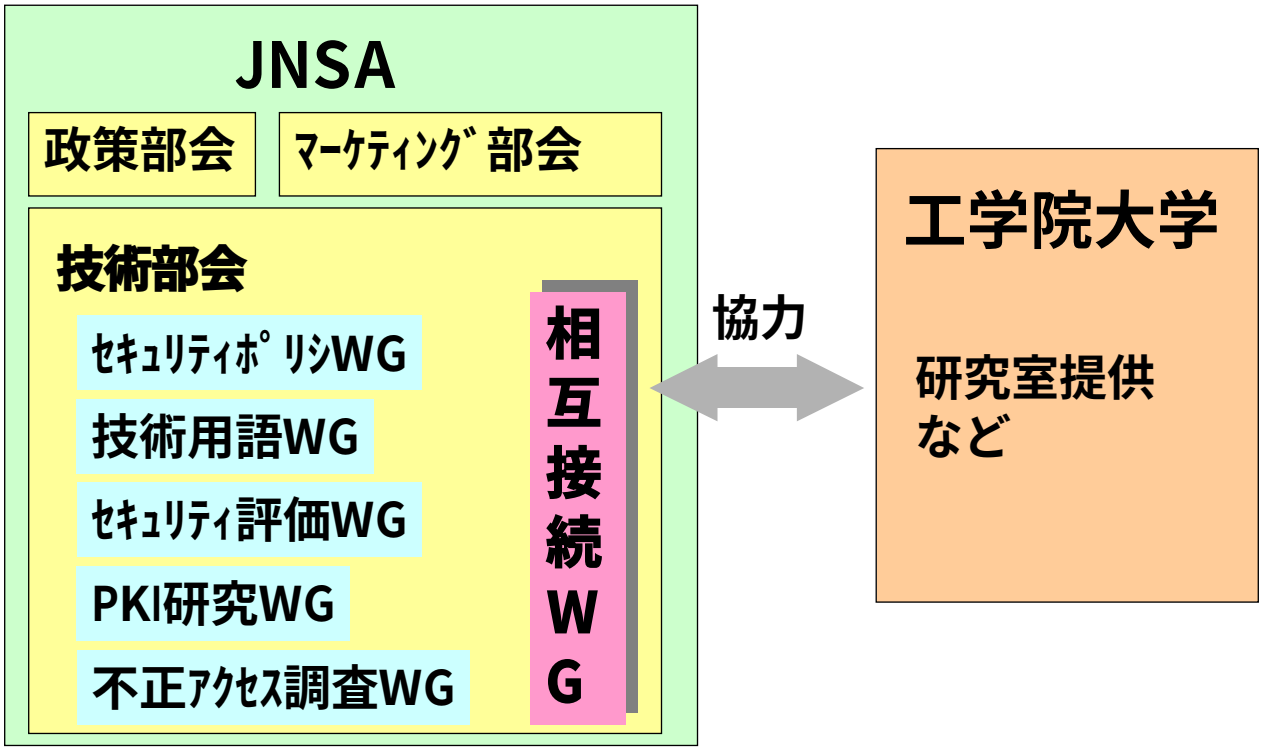
JNSA

相互接続ワーキンググループ

活動中間発表

2000 年 12 月 20 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

JNSA

- 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～
- **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**
  - 18社 34製品 (詳細は別紙参照)
    - IPSecGateway製品　23製品
    - IPSec Client製品　6製品
    - CA局　3製品
    - アナライザ　2製品

試験参加機器一覧

JNSA

IPSec相互接続試験 参加機器一覧

2000/11/2

1．Ｇａｔｅｗａｙ製品

1) LAN Gateway

	製造メーカ	製品名	Version	参加メンバー	IP Address
1	Nortel Networks	Contivity Extranet Switch	V2.62	ネットワンシステムズ(株)	192.168.1.1 / 10.0.1.254
2	Ａｌｃａｔｅｌ	PERMIT/Gateシリーズ	v.3.0 or 3.1	(株)ディアイティ	192.168.1.2 / 10.0.2.254
3	Ｃｈｅｃｋpoint	VPN-1 (Solaris版)	v4.1 sp2	(株)フォーバルクリエーティブ/ENICOM	192.168.1.3 / 10.0.3.254
4	Ｃｈｅｃｋpoint	VPN-1 (WinNT版)	v4.1 sp2	(株)フォーバルクリエーティブ/ENICOM	192.168.1.4 / 10.0.4.254
5	Checkpoint	VPN-1 (Linux版)	v4.1 sp2	(株)フォーバルクリエーティブ/ENICOM	192.168.1.5 / 10.0.5.254
6	Nokia	Nokia IPシリーズ	v4.1 sp2	(株)ネットマークス/ENICOM	192.168.1.7 / 10.0.7.254
7	AlliedTelesis	AR720	v2.0.2-01	アライドテレシス(株)	192.168.1.8 / 10.0.8.254
8	Microsoft	Windows 2000	sp1	マイクロソフト(株)	192.168.1.9 / 10.0.9.254
9	WatchGuard	FireboxII	v4.1 sp4	(株)ヒューコム	192.168.1.10 / 10.0.10.254
10	Intel	Shiva VPN Gateway	v6.70	(株)ヒューコム	192.168.1.11 / 10.011.254
11	Cisco systems	VPN3005	v2.5.2	シスコシステムズ(株)	192.168.1.14 / 10.0.14.254
12	Cisco systems	Cisco7100	v12.1	シスコシステムズ(株)	192.168.1.15 / 10.0.15.254
13	古河電工	INFONET-VP100	v02.01	古河電工(株)	192.168.1.16 / 10.0.16.254
14	VPNet	VSUシリーズ	v3.0.52	(株)ネットマークス	192.168.1.17 / 10.0.17.254
15	SSH	IPSEC Express Toolkit	v4.0	SSHｺﾐｭﾆｹｰｼｮﾝｽﾞ・ｾｷｭﾘﾃｨ(株)	192.168.1.18 / 10.0.18.254
16	RadGurad	clPro	v4.47	(株)東陽テクニカ	192.168.1.19 / 10.0.19.254
17	AXENT	PowerVPN	v6.5	日新電機(株)/ｱｸｾﾝﾄ・ﾃｸﾉﾛｼﾞｰｽﾞ(株)	192.168.1.20 / 10.0.20.254
18	RedCreek	RAVLIN	v3.3	日新電機(株)	192.168.1.21 / 10.0.21.254
19	フジクラ	FNX0531	v2.1.01	(株)フジクラ	192.168.1.22 / 10.0.22.254
20	Cisco systems	PIX		シスコシステムズ(株)	192.168.1.24 / 10.0.24.254

2) Dialup Gateway

	製造メーカ	製品名	Version	参加メンバー	IP Address
21	古河電工	MUCHO-EV	v30.0	古河電工(株)	172.16.1.26 / 10.0.26.254
22	古河電工	MUCHO-EV/PK	v40.0	古河電工(株)	172.16.1.27 / 10.0.27.254
23	フジクラ	FNX0510	v2.1.01	(株)フジクラ	172.16.1.28 / 10.0.28.254

2．Client製品

	製造メーカ	製品名	Version	参加メンバー	IP Address
1	Alcatel	PERMIT Client for Windows	v3.0 or v3.1	(株)ディアイティ	172.16.1.201
2	古河電工	INFONET-VPN Client	v5.0.1 Bu2	古河電工	172.16.1.202
3	SSH	Sentinel	v1.0	SSHｺﾐｭﾆｹｰｼｮﾝｽﾞ・ｾｷｭﾘﾃｨ(株)	172.16.1.203
4	RadGurad	clPro Client	v2.5	(株)東陽テクニカ	172.16.1.204
5	AXENT	Rapter Client	v6.5.1	日新電機(株)/ｱｸｾﾝﾄ・ﾃｸﾉﾛｼﾞｰｽﾞ(株)	172.16.1.205
6	RedCreek	RALIN Soft	v3.3	日新電機(株)	172.16.1.206

提供機器一覧

JNSA

IPSec相互接続試験 提供機器一覧

2000/11/1

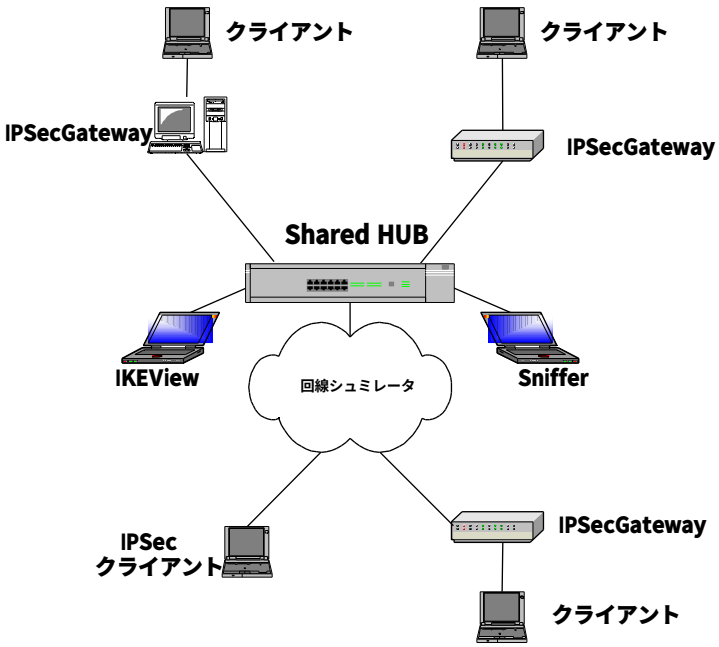
3．CA局

	製造メーカ	製品名	Version	協力ベンダー	IP Address
1	Baltimore	UniCERT	v3.0.1	日本ボルチモアテクノロジーズ(株)	192.168.1.241
2	SSH	Certifier	v1.0.2	SSHｺﾐｭﾆｹｰｼｮﾝｽﾞ・ｾｷｭﾘﾃｨ(株)	192.168.1.242
3	Entrust	Entrust	v5.0	セコムトラストネット(株)	192.168.1.240

4．アナライザ

	製造メーカ	製品名	Version	協力ベンダー	備考
1	松下電工	IKEVIEW	v1.5	松下電工(株)	
2	Network Associates	Sniffer		日本ネットワークアソシエーツ(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。

試験内容

- 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
  - 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
- 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
  - 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

試験項目

- **基本試験/相互接続性確認**
  - Pre-Shard相互認証方式の接続確認
    - 予め定めたパラメータを使用し、総当りで接続性を確認
  - Phase2 IDペイロードタイプ確認試験
    - 各機器がサポートしているPhase2 IDペイロードタイプを確認
    - Peerの設定内容が異なる場合の接続性の確認や、エラーの発生状況も併せて確認
  - 通信中のRe-key動作確認
    - 通信中にSAの更新が発生した際の通信状態を確認

試験項目

- **基本試験/運用性確認**
  - SA消失に関する試験
    - 機器の障害等により、SAを消失した際のSAリカバリ手順等を確認
  - End to End通信試験（ｱﾌﾟﾘｹｰｼｮﾝ動作試験)
    - ftp，http，HOST系のアプリケーションなどの通信をIPSecを使用して行った際の動作を確認
  - IPフラグメンテーション発生時の通信試験
    - IPSec機器でIPフラグメンテーションが発生した際の動作確認
  - SA Life Time動作確認
    - 無通信状態でSA Life Timeを迎えた際の動作を確認

試験項目

- **オプション試験/相互接続性確認**
  - **デジタル署名相互認証方式の接続性確認**
    - Phase1 **の相互認証で、デジタル署名方式を使用した際の接続性を確認**
  - Public-key**相互認証方式の接続性確認**
    - Phase1 **の相互認証で、**Public-key**方式を使用した際の接続性を確認**
  - NAT Traversal**接続試験**
    - NAT Traversal**を使用した際の接続性を確認**

試験項目

- **オプション試験/運用性確認**
  - NAT動作確認試験
    - NAT機能を実装した製品を使用し、NAT使用時のIPSec通信の動作を確認
  - CAに関する試験
    - 証明書の取得方法やCRLの参照方式、CAを使用する際に必要となる項目の動作を確認
  - 性能試験
    - IPSec機器が確立可能なSA数等、各IPSec機器の性能を計る試験
  - 回線障害試験
    - ネゴシエーション中に回線障害が発生した際の動作を確認

試験途中結果

- Pre-Shared接続試験結果 (12月11日集計)

Responder No.	製品名	Initiator 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Contivity Extranet		◎		◎		◎	◎	◎	△		◎	◎	◎	◎	◎	◎	◎	○	△
2	PERMIT Gate	◎		◎	◎	◎	◎	◎	◎	○	◎	◎	◎	◎	◎	◎	◎	◎	◎	△
3	VPN-1 Solaris		◎		◎	◎		◎	◎	◎	◎		◎	◎		◎		○		
4	VPN-1 WindowsNT	◎	◎	◎		◎	◎		◎	◎	◎		◎	◎		◎		◎	◎	△
5	VPN-1 Linux		◎	◎	◎				◎	◎	◎	◎	◎	◎	◎	◎	◎			
6	Nokia IP	◎	○		◎				◎					◎		◎				△
7	AR720	◎	◎	◎					○					○	◎	◎		◎		◎
8	Windows 200	◎	◎	◎	◎	◎	◎	○		◎	◎	○	◎	◎	◎	◎	◎	◎	◎	△
9	Fire Box II	△	◎	◎	◎	◎			◎				◎	◎	◎	◎		◎		◎
10	ShivaVPN GW		◎	◎	◎	◎			◎				◎	◎	◎	◎		◎		○
11	VPN3005	◎	◎			◎			○				◎	◎	◎	◎	◎			△
12	IOS(Cisco)	◎	◎	◎	◎	◎	○		◎	◎	◎	◎		◎	◎	◎		△	◎	◎
13	INFONET-VP100	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎		◎	◎	◎	◎	◎	◎
14	VSU Series	◎	◎			◎		◎	◎	◎	◎	◎	◎	◎		◎	◎	◎	◎	◎
15	IPSEC Express	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎		◎	◎	◎	◎
16	clPro	◎	◎			◎	○	◎	◎	○	○	◎	△	◎	◎	◎		◎	○	△
17	PowerVPN	◎	◎	◎	◎			◎	◎	◎	◎		△	◎	◎	◎	◎		◎	◎
18	RAVLIN	○	△		◎			◎	◎				◎	◎	◎	◎		◎		◎
19	FNX0531	△	◎		△		△	◎	△	◎	△	△	◎	◎	◎	△	△	◎	◎	

試験途中結果

JNSA

- 前頁表の見方
  - 接続確認試験は、以下の2つのﾊﾟﾗﾒｰﾀﾊﾟﾀｰﾝを使用

	パターン1	パターン2
暗号ｱﾙｺﾞﾘｽﾞﾑ	DES-CBC	DES-CBC
Hashｱﾙｺﾞﾘｽﾞﾑ	MD5	SHA-1
ペイロード	ESP	ESP
認証ｱﾙｺﾞﾘｽﾞﾑ	HMAC-MD5	HMAC-SHA1

  - ◎　：ﾊﾟﾗﾒｰﾀﾊﾟﾀｰﾝ1と2で接続性を確認
  - ○　：ﾊﾟﾗﾒｰﾀﾊﾟﾀｰﾝのどちらかで接続性を確認
  - △　：試験時間内での接続不可(原因判明し対応中)
  - 空欄　：12月11日時点で未試験

今後の予定

- IPv6
- **無線**LAN
- CA**局　など**…