\Orchestrating a brighter world NEC

UNIVERGE IXシリーズ
IX-YAMAHA(RTX)とのIPsec接続資料

日本電気株式会社
デジタルネットワーク事業部

目次

はじめに

本資料について

◆ 背景

昨今、SOHO/SMB向けルータ市場では部品調達難の影響をダイレクトに受け、納期通りの装置提供がどの競合企業においても難しくなっており、マルチベンダー構成を組むケースを視野に入れるお客様も増加傾向にある。そのようなお客様に対して、ご提案できる自社製品の情報を共有する。

◆ 目的

本資料は、UNIVERGE IXシリーズとYAMAHA社製RTXシリーズ(※)をVPN接続する際の注意点およびコンフィグ差分を説明することを目的とする。

(※)以降のページでは、RTX(シリーズ)と記載する。

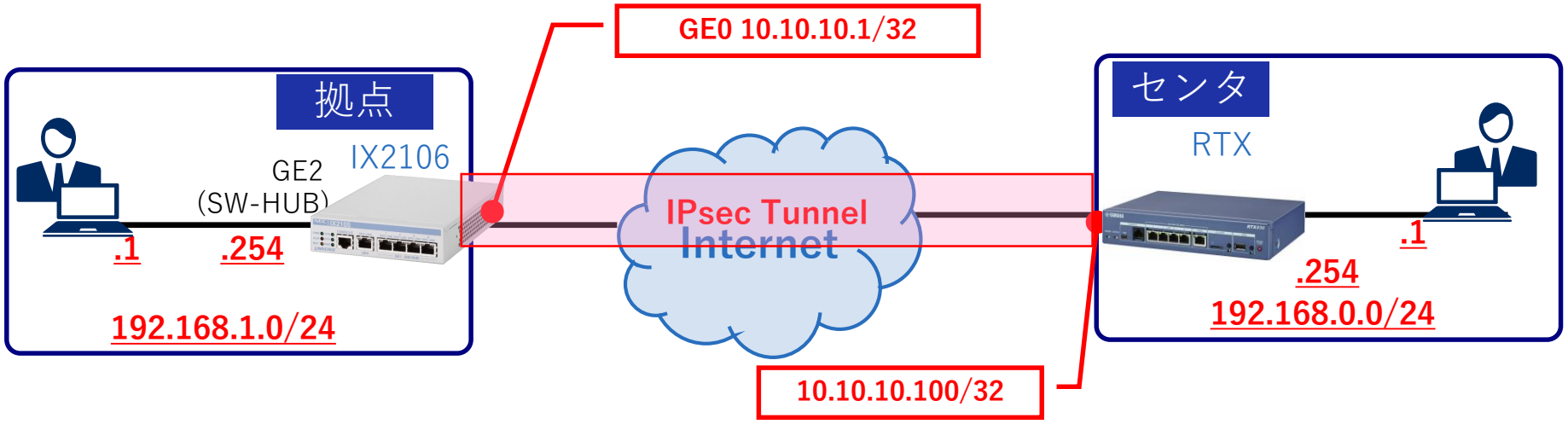
◆ 注意事項

・本資料を参考にして本番導入する際は、各パラメータを任意の値に変更すること。(セキュリティ向上のため。)

・本資料のコンフィグはあくまでもサンプルのため、動作を保証するものではない。必ず事前の確認を行うこと。

本資料の装置構成図

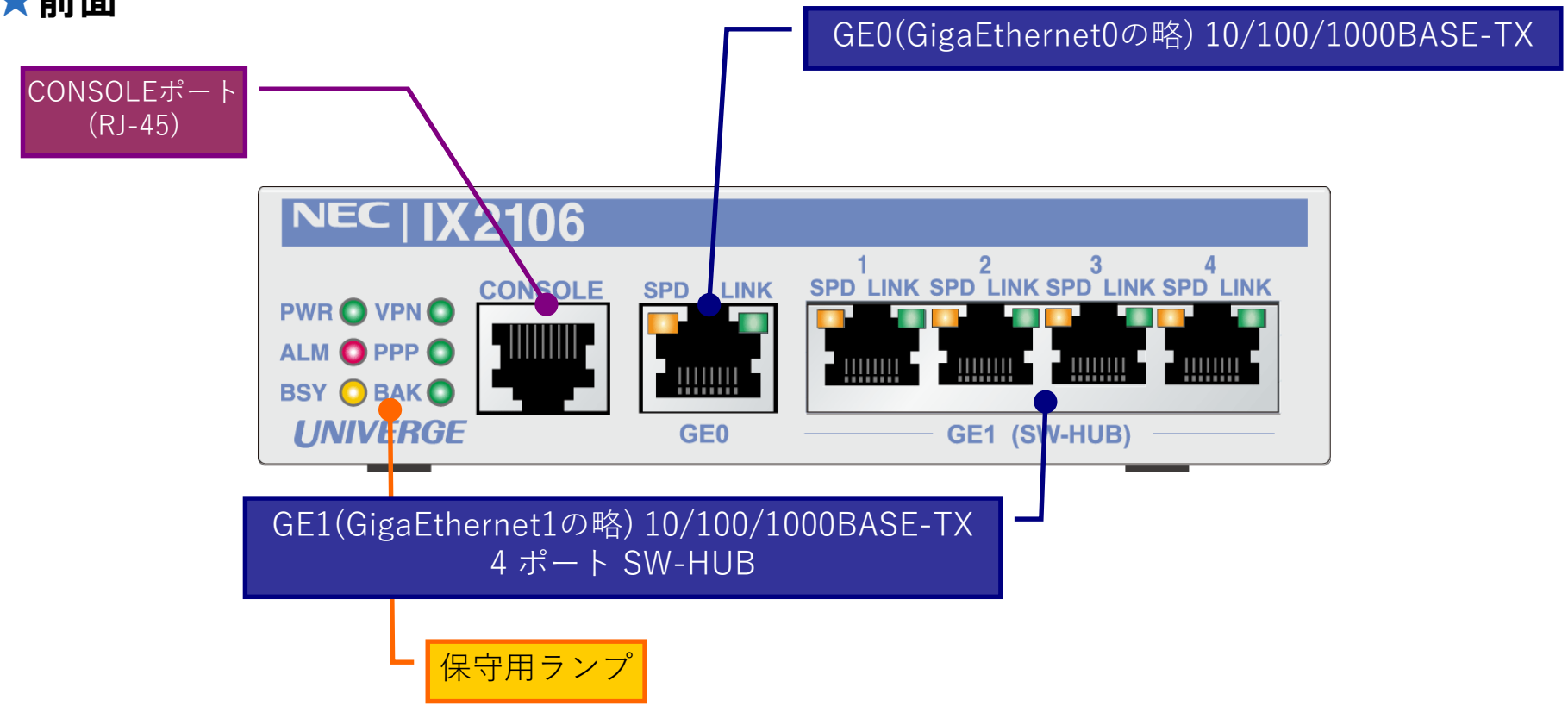
- 構成としては以下の通り、IP網を介してIXとRTXをVPN接続する。
- それぞれ以下の機種を使用する
  IXシリーズ：IX2106
  RTXシリーズ：RTX830



UNIVERGE　IXシリーズ設定準備

UNIVERGE IX2106外観図

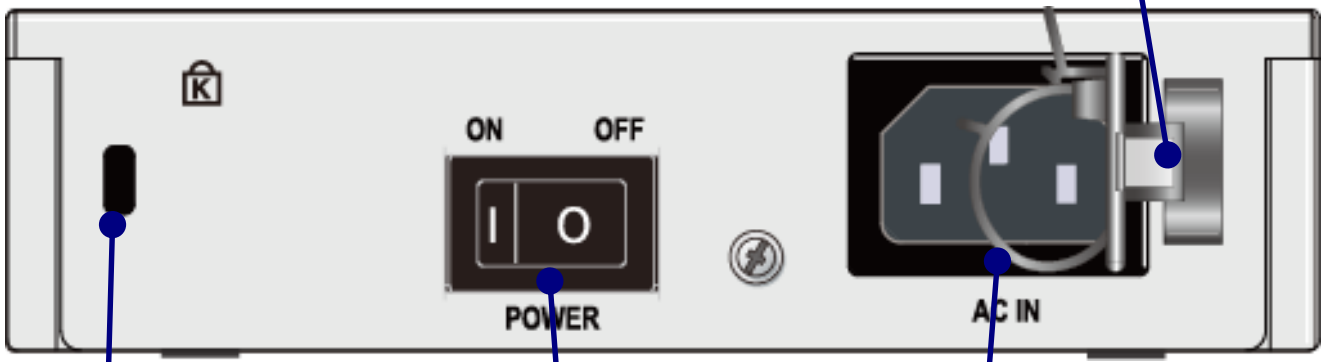
★前面



PWRランプ	電源on時に緑点灯	VPNランプ	IPsecSAが1つ以上確立している時に緑点灯
ALMランプ	ハード異常検出時、及び 温度・電圧異常検出時に赤点灯	PPPランプ	PPPセッションが1つ以上確立しているときに緑点灯 接続中は緑点滅します。
BUSYランプ	Flashメモリ書き込み時に橙点滅	BAKランプ	ネットワークモニタ機能により障害を検出すると緑点灯

UNIVERGE IX2106外観図

★背面



電源ケーブル固定ベルト

電源ケーブルが電源コネクタから
外れないように固定するベルトです。

電源スイッチ

電源コネクタ

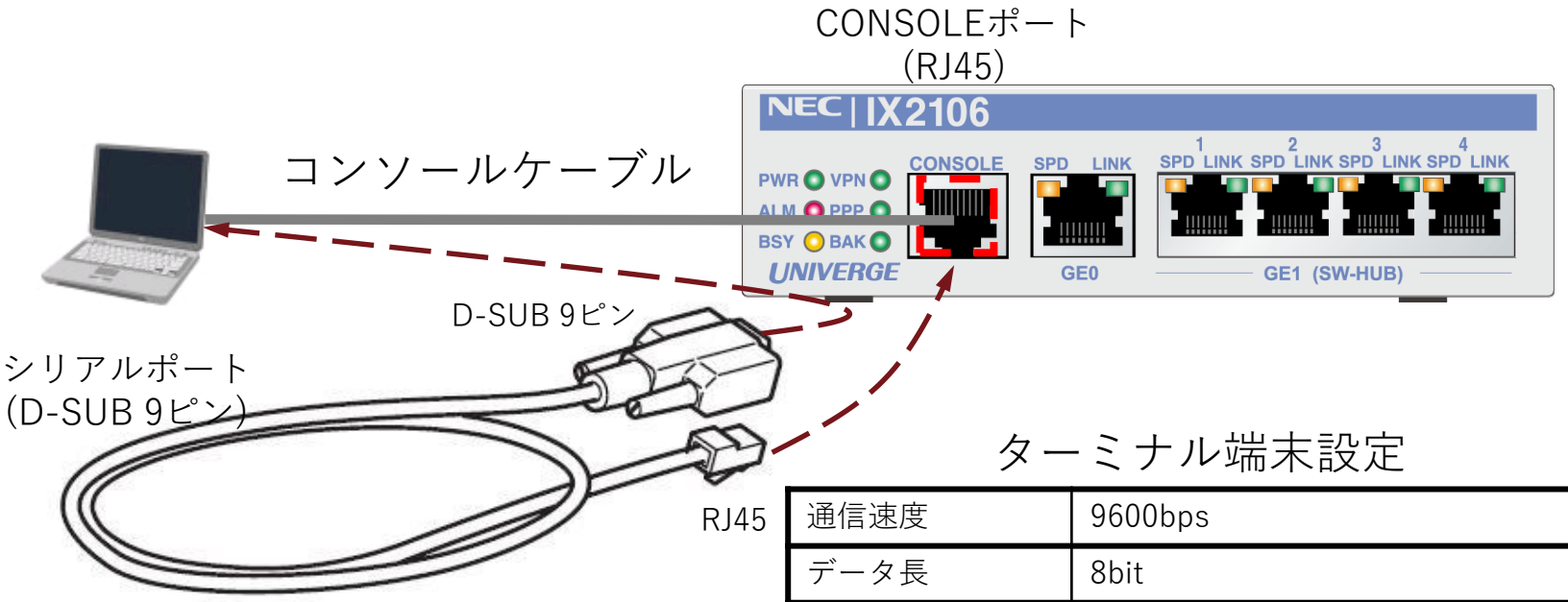
添付の電源ケーブルを接続

セキュリティスロット

盗難防止用鍵取付穴です。
別売のセキュリティワイヤを取り付けることで、
本装置の盗難を防ぐことができます。

コンソール端末の接続

- コンソール端末の接続方法は、RTXシリーズと大きな違いなし。
- Teratermを使う場合は、デフォルト値で接続可能。



ターミナル端末設定

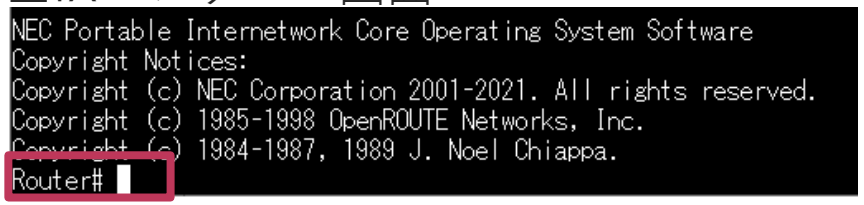
通信速度	9600bps
データ長	8bit
パリティ	なし
ストップビット	1bit
フロー制御	なし
ターミナル ソフトウェア	VT-100準拠通信ソフトウェア (Tera Term、Hyper Terminalなど)

コンソール操作の比較(RTXシリーズと比較)

- 起動時の差分
  Router#と表示されていれば、正常起動完了。

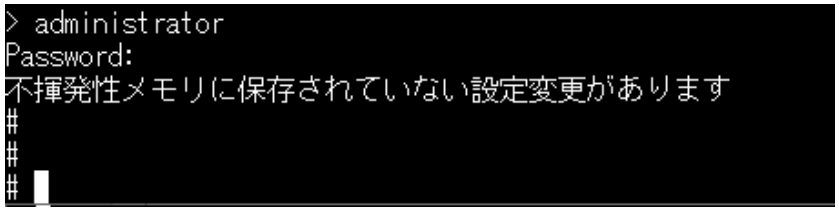
■RTXコンソール画面

■IXコンソール画面

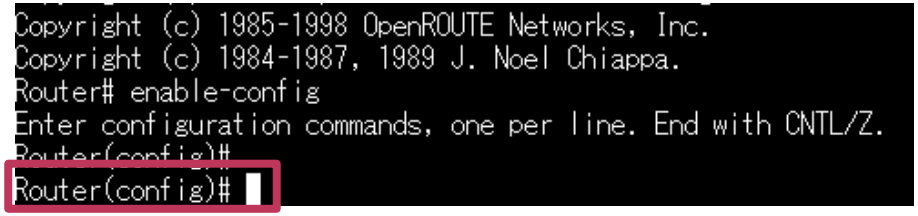


- 設定モードへの移行差分
  enable-config(enで省略可)コマンドを実行。
  Router(config)#と表示されれば、正常移行完了。

■RTXコンソール画面



■IXコンソール画面

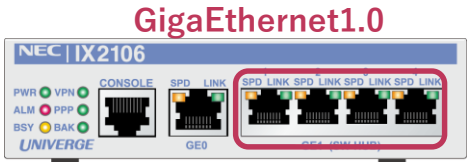


UNIVERGE　IXシリーズ設定準備

設定について

- RTXとIXシリーズの設定を比較する形で記載。
- コンフィグは、そのまま入力すれば動作します。
  ただし、実際の運用時に変更が必要になりそうな箇所は赤字で
  補足してありますので、必要に応じて変更ください。
- 設定の流れは以下。
  ①LANインタフェースの設定
  ②WANインタフェースの設定
  ③インターネット関連設定
  ④ルーティングの設定
  ⑤IPsecの設定
  ⑥フィルタ設定
  ⑦ログ収集の設定と設定保存

LANインタフェースの設定



LANインタフェースの設定 (IX)

```
Router(config)# interface GigaEthernet1.0
Router(config-GigaEthernet2.0)# ip address 192.168.1.254/24
Router(config-GigaEthernet2.0)# no shutdown
Router(config-GigaEthernet2.0)# exit
Router(config)#
```

- LANアドレスは、「192.168.1.254/24」で設定。
  TAGを利用する場合は、以下を参考(GigaEthernet1.1~32を使用)。
  例はTAG=10を使用。※設定後は、設定保存＋再起動が必要。

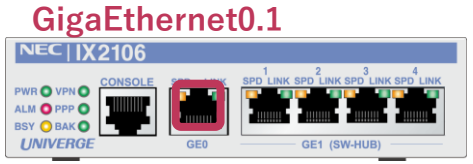
```
Router(config)# interface GigaEthernet1.1
Router(config-GigaEthernet1.1)# encapsulation dot1q 10 tpid 8100
Router(config-GigaEthernet1.1)# ip address 192.168.1.254/24
```

LANインタフェースの設定(RTX)

```
# ip lan1 address 192.168.0.254/24
```

- LANアドレスは、「192.168.0.254/24」で設定。IXとの違いとしては以下。
  - IXはポート(インタフェース設定モード)に遷移してから設定が必要
  - ポートはデフォルト無効(セキュリティ上)になっており、有効化のコマンドが必要(no shutdown)

WANインタフェースの設定①



PPPoEインタフェースの設定(IX)

```
Router(config)# ppp profile internet
Router(config-ppp-my-profile)# authentication myname test@test.com
Router(config-ppp-my-profile)# authentication password test@test.com test-password
Router(config-ppp-my-profile)# exit
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ppp binding internet
Router(config-GigaEthernet0.1)# ip address 10.10.10.1/32
Router(config-GigaEthernet0.1)# no shutdown
Router(config-GigaEthernet0.1)# exit
Router(config)#
```

- インターネット接続用のID/PWの設定(導入時はサービスにあわせて変更)
  ID：test@test.com
  PW：test-password
- WANアドレスは、「10.10.10.1/32」で設定。
  動的契約の場合は、IPCPを入力。
  ip address ipcp

WANインタフェースの設定②

PPPoEインタフェースの設定(RTX)

```
# pp select 1
pp1#  pp always-on on
pp1#  pppoe use lan2
pp1#  pp auth accept pap chap
pp1#  pp auth myname test@test.com test-password
pp1#  ppp lcp mru on 1454
pp1#  ip pp mtu 1454
pp1#  pp enable 1
pp1# ip lan2 address 10.10.10.100/32
```

- WANアドレスは、「10.10.10.100/32」で設定。
  IXとの違いとしては以下。
  - IXはインターネットの認証用の設定をプロファイルモードに移行して設定。
    プロファイル設定は、WANポート(インタフェース)への関連付けが必要。
  - IXシリーズでは、PPPの認証がデフォルトで被認証側[accept]で動作するため、
    pp auth acceptコマンド相当は設定不要。
  - IXシリーズでは、MTUやMRUをインタフェース種別から自動計算するため、
    ip pp mtu、 ppp lcp mruコマンド相当は設定不要(固定で設定することも可能)。

インターネット関連設定

インターネット関連の設定(IX)

```
■NAPT
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ip napt enable
Router(config-GigaEthernet0.1)# ip napt static GigaEthernet0.1 udp 500
Router(config-GigaEthernet0.1)# ip napt static GigaEthernet0.1 50
■DNS
Router(config)# proxy-dns ip enable
Router(config)# proxy-dns ip max-sessions 1024
Router(config)# proxy-dns server 8.8.8.8
```

- DNSアドレスは、プロバイダから指定されたアドレスを入力すること。
  - 「8.8.8.8」で設定。
  - アドレスをIPCPで取得する際には、DNSサーバのアドレスも自動取得

インターネット関連の設定(RTX)

```
■NAT
# ip lan2 nat descriptor 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 10.10.10.100
# nat descriptor masquerade static 1 1 10.10.10.100 udp 500
# nat descriptor masquerade static 1 2 10.10.10.100 esp
■DNS
# dns sever 8.8.8.8
# dns private address spoof on
```

ルーティング設定

スタティックルートの設定(IX)

```
Router(config)# ip ufs-cache enable
Router(config)# ip ufs-cache max-entries 40000
Router(config)# ip route 192.168.0.0/24 Tunnel0.0
Router(config)# ip route default GigaEthernet0.1
```

- UFSキャッシュの有効化(IXシリーズ独自の高速化キャッシュ)
- ルーティングの設定
  - トンネルの接続先はへ到達するためのスタティックルートを設定。
    ・GigaEthernet0.1：出力先インタフェース(デフォルトルート)
  - トンネル経由のLANに接続するためのスタテックルート設定
    ・Tunnnel0.0：出力インタフェース。本例では対向先NW192.168.0.0/24を設定

スタティックルートの設定(RTX)

```
# ip route default gateway pp 1
# ip route 192.168.1.0/24 gateway tunnel 1
```

- IXとの違いとしてはほとんどなし。
  - インタフェース名のみ違う。

IPsecの設定①

IPsecの設定(IX)

```
Router(config)# ike proposal ike-prop encryption aes-256 hash sha lifetime 3600
Router(config)# ike policy ike1 peer 10.10.10.100 key mykey ike-prop
Router(config)# no ike initial-contact payload
Router(config)# ip access-list sec-list permit ip src any dest any
Router(config)# ipsec autokey-proposal ipsec-prop esp-aes-256 esp-sha lifetime time 3600
Router(config)# ipsec autokey-map ipsec1 sec-list peer 10.10.10.100 ipsec-prop
Router(config)# ipsec local-id ipsec1 192.168.1.0/24
Router(config)# ipsec remote-id ipsec1 192.168.0.0/24
Router(config)# interface Tunnel0.0
Router(config-Tunnel0.0)# tunnel mode ipsec
Router(config-Tunnel0.0)# ip unnumbered GigaEthernet1.0
Router(config-Tunnel0.0)# ipsec policy tunnel ipsec1 out
Router(config-Tunnel0.0)# ip tcp adjust-mss auto
Router(config-Tunnel0.0)# no shutdown
```

- IPsecの設定
  以下については、セキュリティ上任意の値に変更すること。
  VPN対向先アドレス：10.10.10.100(案件時のアドレスに変更)
  事前共有鍵：mykey(変更する場合は、RTXと合わせること。)
- INITIAL-CONTACTメッセージ設定
  IXの送信メッセージをRTX側で認識できないため、送信方式を変更

IPsecの設定②

IPsecの設定(RTX)

```
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ipsec sa policy 101 1 esp aes256-cbc sha-hmac
tunnel1# ipsec ike duration ipsec-sa 1 3600
tunnel1# ipsec ike duration ike-sa 1 3600
tunnel1# ipsec ike encryption 1 aes256-cbc
tunnel1# ipsec ike group 1 modp768
tunnel1# ipsec ike hash 1 sha
tunnel1# ipsec ike local id 1 192.168.0.0/24
tunnel1# ipsec ike pre-shared-key 1 text mykey
tunnel1# ipsec ike remote address 1 10.10.10.1
tunnel1# ipsec ike remote id 1 192.168.1.0/24
tunnel1# tunnel enable 1
```

- IPsecの設定
  IXとの違いとしては以下。
  - RTXのIKEのDHグループはデフォルト「modp1024」(RTX830の場合)
    IXは、IKEのDHグループはデフォルト 「modp768」(全機種共通)

  ※ IX側で変更する場合は、以下のコマンドで変更可能。

  ike proposal ike-prop encryption aes-256 hash sha group 1024-bit

  - 事前共有鍵；mykey(※変更する場合は、IX側と合わせること)

フィルタ設定

フィルタの設定(IX)

```
Router(config)# ip access-list f-list permit ip src 10.10.10.100/32 dest 10.10.10.1/32
Router(config)# interface GigaEthernet0.1
Router(config-GigaEthernet0.1)# ip filter f-list 1 in
Router(config-GigaEthernet0.1)# exit
```

- インターネット側から受信するパケットを、送信元がトンネル接続先のパケットに限定する。案件ではグローバルアドレスを変更すること。
  送信元(RTX)：10.10.10.100、宛先(IX)：10.10.10.1
- ACLにマッチしなかったパケットは廃棄(暗黙のdeny)
- ip filterコマンドでインタフェースにin方向で適用

フィルタの設定(RTX)

```
# ip filter 1 pass 10.10.10.1/32 10.10.10.100/32
# pp select 1
pp1# ip pp secure filter in 1
```

- IXシリーズと基本的な考え方は変わりません。

ログ収集の設定と設定保存

ログ収集の設定/設定の保存(IX)

```
Router(config)# logging subsystem all warn
Router(config)# logging timestamp datetime
Router(config)# logging buffered
Router(config)# write memory
```

◆ログの情報を装置の内部バッファに蓄積
show buffersコマンドでログを取得。

ログ収集の設定／設定の保存(RTX)

```
# syslog info on
# save
```

◆IXシリーズは取得する内容をあらかじめ設定する。
IXシリーズでは、debug/info/notice/warn/errorの 5 段階を設定可能
IXシリーズは、機能単位でのログ収集も設定可能。

IPsec接続の確認方法

IPsec接続関連のログ確認(IX)

■SA(鍵情報)

```
Router(config)# show ipsec sa brief
IPsec SA - 1 configured, 2 created
Policy map                      Dir   Type   SPI          Life(secs/bytes)
auto-map                        IN    ESP    0xb65095c7      166/-
auto-map                        OUT   ESP    0x9b99b800      166/-
```

■端末間ping

```
 Router(config)# ping 192.168.0.1 source 192.168.1.1
 PING 192.168.1.1 > 192.168.0.1 56 data bytes
 64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=0.261 ms
 64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=0.203 ms
 64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=0.172 ms
 64 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=0.165 ms
```

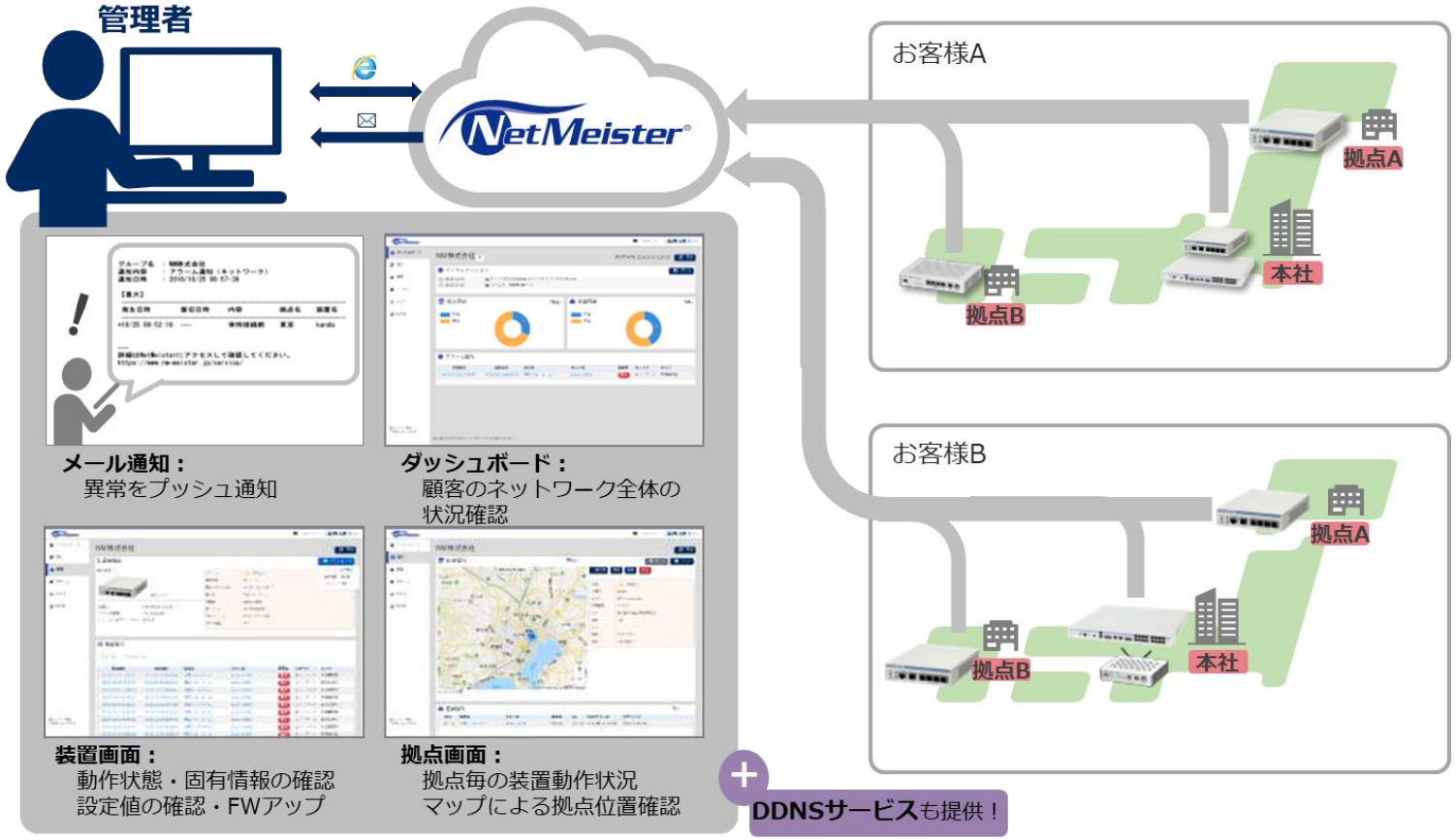
■通信状況(★)

```
Router(config)# sh interfaces Tunnel0.0 stats
Interface Tunnel0.0 is up
            ////中略///
  Encapsulation TUNNEL:
    Tunnel mode is ipsec (4-over-4)
    Tunnel is ready
    Statistics:
      10 packets input, 1320 bytes, 0 errors (★受信)
      10 packets output, 1520 bytes, 0 errors (★送信)
```

クラウド(NetMeister)の装置管理

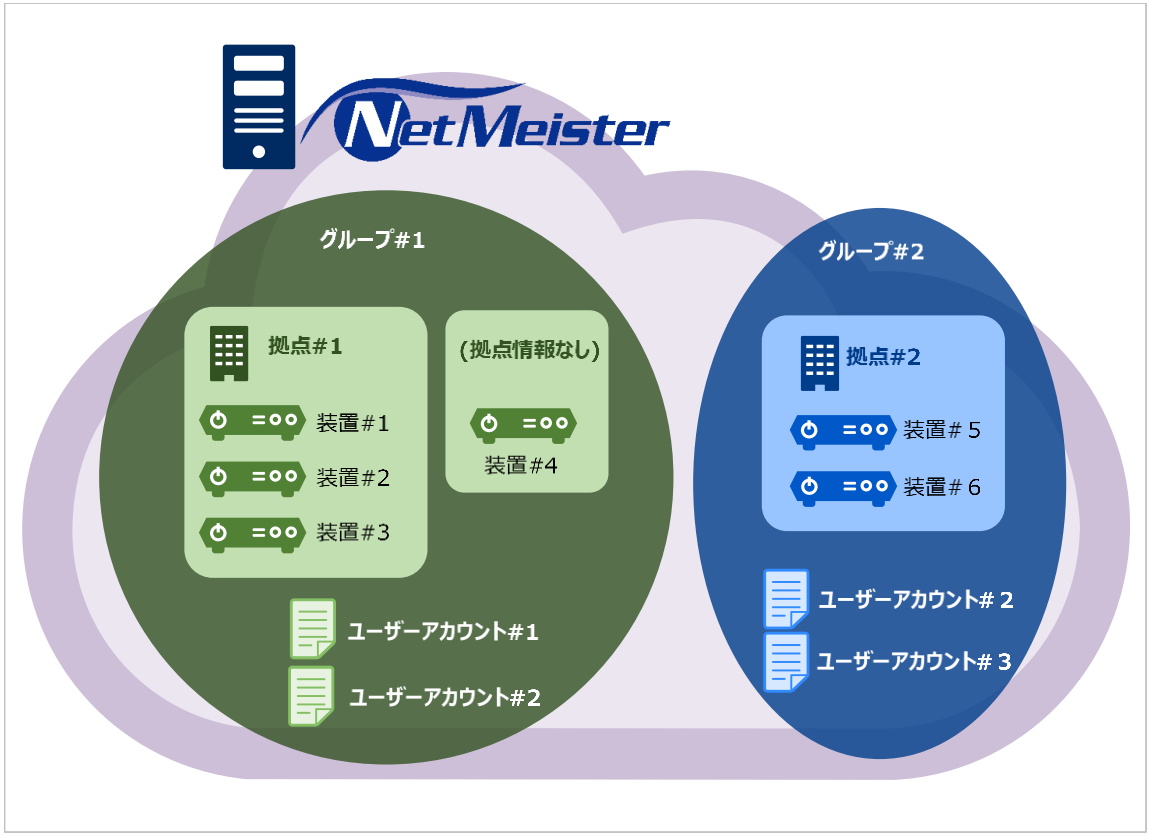
NetMeisterとは

- NetMeisterはクラウド上で顧客単位・拠点単位でのネットワーク機器管理が可能な**基本無料のサービス**です。運用管理者は各ユーザ毎の装置情報を一元管理出来ます。



NetMeisterの管理イメージ

- NetMeisterにおける装置の管理イメージ
  NetMeisterは、『グループ』に「ユーザーアカウント」「拠点」「装置」を関連付ける構成です。



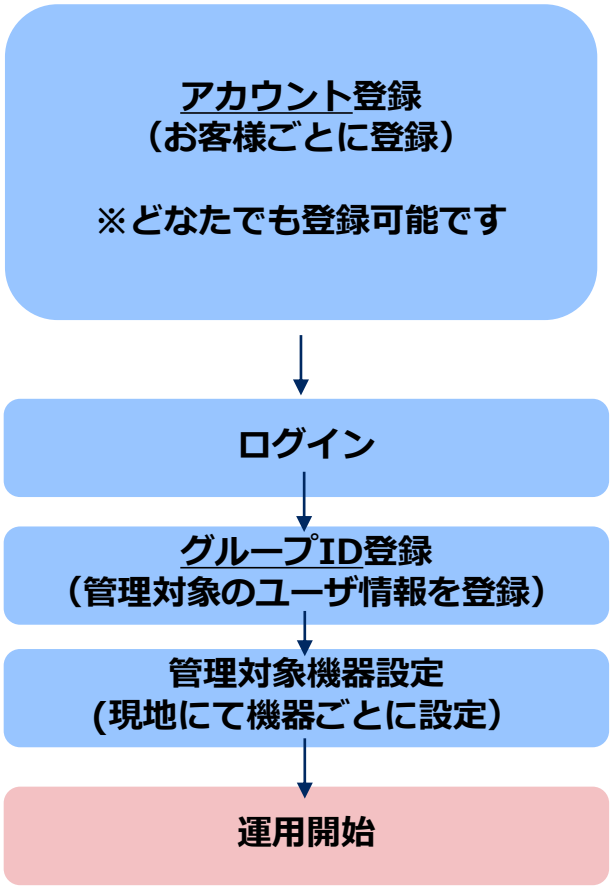
グループ
NetMeister上にグループID（任意のグループ名）を作成します。

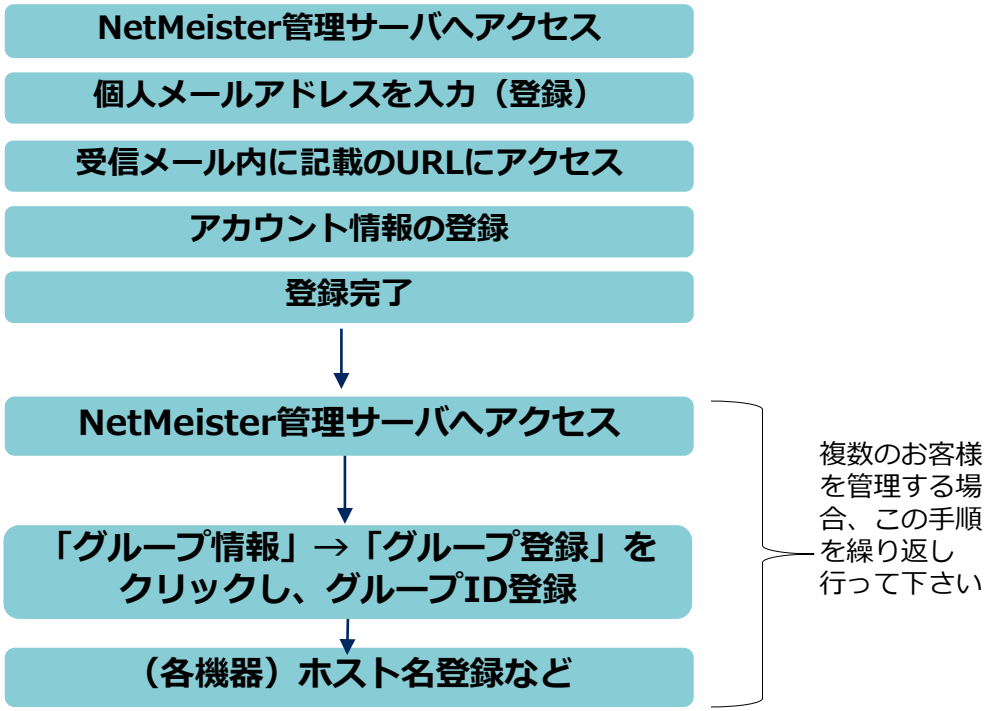
拠点
装置に拠点名を設定することで、NetMeister上に拠点ごとに表示します。
※装置に拠点名を設定していない場合は、拠点情報を表示しません（グループに装置情報を直接関連付けます）。

装置
装置にグループIDを設定することで、NetMeisterの該当グループ上で装置を管理します。

NetMeister 利用方法

◆ ご利用方法





■アカウントとグループIDについて
アカウント：管理者用のIDです。管理者のメールアドレスとパスワードを登録します。
グループID：組織ごと（企業、部署など）に取得する識別IDです。
アカウントと管理装置（ホスト情報）をひもづけて管理します。
１つのグループIDあたり10アカウントまで登録可能です。

管理機器への設定

NetMeisterへの登録設定(IX)

```
Router(config)# nm ip enable
Router(config)# nm account semi-nm password plain nec123
Router(config)# nm sitename site-name
Router(config)# nm ddns hostname host-name
```

◆ 各パラメータの開設

- nm ip enable : NetMeisterへの登録有効化
- nm account : NetMeister上で登録したグループID/グループパスワードの設定
  グループID/semi-nm
  パスワード/nec123
- nm sitename : NetMeiterで拠点情報の登録を行う際に必要な設定
  拠点ID/site-name
- nm ddns : NetMeister DDNSのドメイン名の登録に必要
  ドメインホスト名/host-name

※生成されるドメイン　[host-name].[semi-nm].nmddns.jp

NetMeisterDDNSを利用時のIPsec設定変更点

IPsecの設定(IX)

```
Router(config)# ike proposal ike-prop encryption aes-256 hash sha lifetime 3600
Router(config)# ike policy ike1 peer-fqdn-ipv4 host-name.semi-nm.nmddns.jp key  mykey ike-prop
Router(config)# no ike initial-contact payload
Router(config)# ip access-list sec-list permit ip src any dest any
Router(config)# ipsec autokey-proposal ipsec-prop esp-aes-256 esp-sha lifetime time 3600
Router(config)# ipsec autokey-map ipsec1 sec-list peer-fqdn-ipv4 host-name.semi-nm.nmddns.jp ipsec-prop
Router(config)# ipsec local-id ipsec1 192.168.1.0/24
Router(config)# ipsec remote-id ipsec1 192.168.0.0/24
Router(config)# interface Tunnel0.0
Router(config-Tunnel0.0)# tunnel mode ipsec
Router(config-Tunnel0.0)# ip unnumbered GigaEthernet1.0
Router(config-Tunnel0.0)# ipsec policy tunnel ipsec1 out
Router(config-Tunnel0.0)# ip tcp adjust-mss auto
Router(config-Tunnel0.0)# no shutdown
```

- 設定変更点は以下。
  接続先アドレス(10.10.10.100)→(host-name.semi-nm.nmddns.jp)
  コマンドも(peer)から(peer-fqdn-ipv4)に変更されているので注意すること。

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC