AX-Network-Manager クラウドサービス
VPN 接続ガイド

■ はじめに

本資料は，今回発行いたします AX-Network-Manager クラウドサービスに VPN 接続する際の設定例を説明するものです。本資料の設定例は当社で接続を確認しておりますが、必ずしも接続性を保証するものではありません。

■ 輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。なお，不明な場合は，ご購入先担当営業にお問い合わせください。

■ご注意

このガイドは，改良のため，予告なく変更する場合があります。

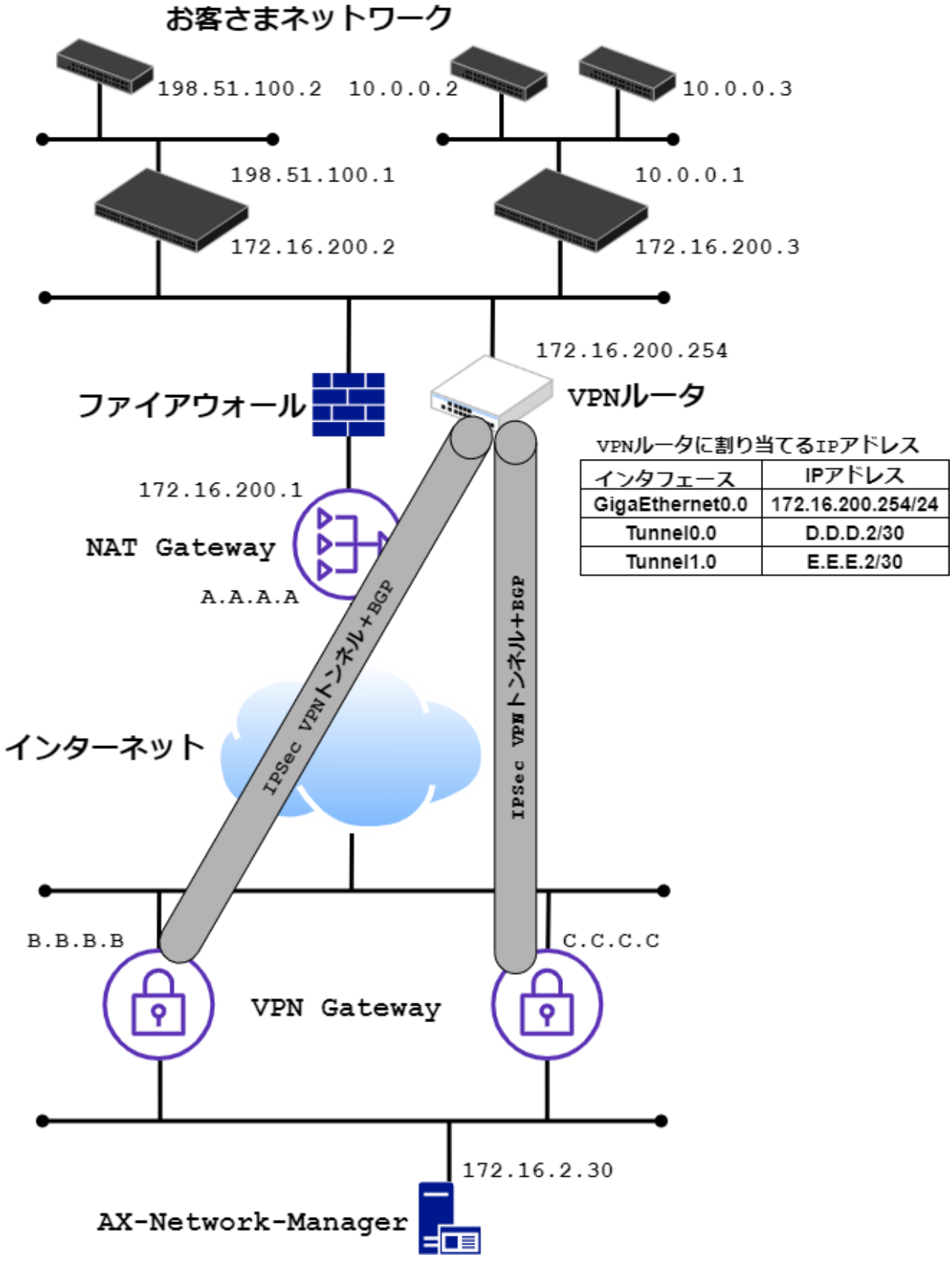
■発行

2021 年 5 月発行（初版）

目　次

１． 接続構成

AX-Network-Manager クラウドサービスは、AX-Network-Manager とお客さまネットワークを VPN 接続することでお客さまのネットワーク機器を管理します。本ガイドでは、VPN ルータとして AX620R シリーズを使用する場合について説明します。なお、インターネットと VPN ルータの WAN インタフェースの接続性はお客様側で用意・設定し、VPN ルータを経由してお客さまネットワークのネットワーク機器への SSH ログイン/SNMP アクセスができるように接続してあるものとしています。下図が構成のイメージ図です。



VPNルータに割り当てるIPアドレス

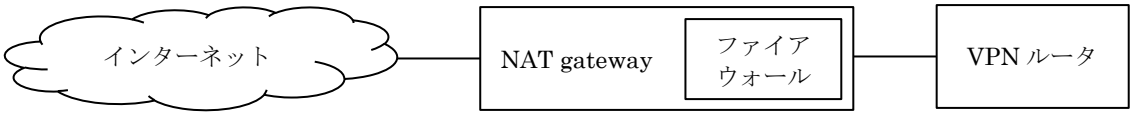
インタフェース	IPアドレス
GigaEthernet0.0	172.16.200.254/24
Tunnel0.0	D.D.D.2/30
Tunnel1.0	E.E.E.2/30

図中の記載している IP アドレスはパラメータシートのアラクサラ記入欄に記載している下記項目と対応しています。
A.A.A.A … VPN 対向エンドポイント IP アドレス
B.B.B.B … トンネル 1 の IPSec 接続先 IP アドレス
C.C.C.C … トンネル 2 の IPSec 接続先 IP アドレス
D.D.D.2/30 … トンネル 1 のトンネルインタフェースの IP アドレス
E.E.E.2/30 … トンネル 2 のトンネルインタフェースの IP アドレス

VPN ルータの IPsec VPN トンネルの対向となる VPN Gateway とは 2 本のトンネルを設定し、BGP も対向の VPN Gateway と 2 本のセッションを張ります。VPN Gateway の障害などにより VPN トンネルが一時的に切断されることがありますので、冗長化のために VPN トンネルを２つ設定することを強く推奨します。

アラクサラでサンプルコンフィグを提供できないルータをご利用の場合はパラメータシートに記載の VPN トンネルのパラメータを参照して設定する必要があります。

２．事前準備



VPN ルータを、NAT gateway の配下に設置している上図のような構成の場合、ファイアウォールに下表の通信を許可するルールを設定ください。また、NAT を利用してインターネットに接続する場合は VPN ルータで NAT トラバーサルを有効にした上で、500 番ポートを 4500 番ポートに読み替えてファイアウォールに設定ください。AX620R シリーズで NAT トラバーサルを有効にするコンフィグは「ike nat-traversal」です。

方向	送信元 IP	送信先 IP	プロトコル	送信元ポート	送信先ポート
ファイアウォールへの入力	IPSec VPN トンネル１の IPSec 接続先 IP アドレス	VPN ルータ GE0 インタフェースの IP アドレス	UDP	500	500
	IPSec VPN トンネル 2 の IPSec 接続先 IP アドレス	VPN ルータ GE0 インタフェースの IP アドレス	UDP	500	500
	IPSec VPN トンネル１の IPSec 接続先 IP アドレス	VPN ルータ GE0 インタフェースの IP アドレス	IP 50(ESP)	-	-
	IPSec VPN トンネル 2 の IPSec 接続先 IP アドレス	VPN ルータ GE0 インタフェースの IP アドレス	IP 50(ESP)	-	-
ファイアウォールからの出力	VPN ルータ GE0 インタフェースの IP アドレス	IPSec VPN トンネル１の IPSec 接続先 IP アドレス	UDP	500	500
	VPN ルータ GE0 インタフェースの IP アドレス	IPSec VPN トンネル 2 の IPSec 接続先 IP アドレス	UDP	500	500
	VPN ルータ GE0 インタフェースの IP アドレス	IPSec VPN トンネル１の IPSec 接続先 IP アドレス	IP 50(ESP)	-	-
	VPN ルータ GE0 インタフェースの IP アドレス	IPSec VPN トンネル 2 の IPSec 接続先 IP アドレス	IP 50(ESP)	-	-

３．サンプルコンフィグを用いた設定

アラクサラ提示のサンプルコンフィグがある場合の手順となります。もしサンプルコンフィグが無い場合は「７．[参考]パラメータシートを用いた設定」に進んでください。

パラメータシートのアラクサラ記入欄に記載してありますサンプルコンフィグをコマンドラインインタフェース(CLI)より VPN ルータに投入してください。サンプルコンフィグの一例を下表に示します。

```
ike proposal ike-prop encryption aes hash sha group 1024-bit
!
ike policy ike-policy1 peer B.B.B.B key M3V.Jy1iYP5lWUZ9CQEpFb._G6XrHL5l ike-prop
ike keepalive ike-policy1 10 3
!
ike policy ike-policy2 peer C.C.C.C key jIZ3qiKFlkkOfD5BjWNamWNrYOLuCl2c ike-prop
ike keepalive ike-policy2 10 3
!
ipsec autokey-proposal ipsec-prop esp-aes esp-sha lifetime time 3600
!
ipsec autokey-map ipsec-map1 sec-list peer B.B.B.B ipsec-prop pfs 1024-bit
!
ipsec autokey-map ipsec-map2 sec-list peer C.C.C.C ipsec-prop pfs 1024-bit
!
watch-group watch_tunnel_1 10
  event 10 ip unreach-host D.D.D.1 Tunnel0.0
  action 10 ipsec clear-sa Tunnel0.0
!
network-monitor watch_tunnel_1 enable
!
watch-group watch_tunnel_2 10
  event 10 ip unreach-host E.E.E.1 Tunnel1.0
  action 10 ipsec clear-sa Tunnel1.0
!
network-monitor watch_tunnel_2 enable
!
router bgp 65000
  neighbor D.D.D.1 remote-as FFFF
  neighbor D.D.D.1 timers 10 30
  neighbor E.E.E.1 remote-as GGGG
  neighbor E.E.E.1 timers 10 30
  address-family ipv4 unicast
    originate-default always
!
interface Tunnel0.0
  tunnel mode ipsec
  ip address D.D.D.2/30
  ip tcp adjust-mss auto
  ipsec policy tunnel ipsec-map1 df-bit ignore pre-fragment out
  no shutdown
!
interface Tunnel1.0
  tunnel mode ipsec
  ip address E.E.E.2/30
  ip tcp adjust-mss auto
  ipsec policy tunnel ipsec-map2 df-bit ignore pre-fragment out
  no shutdown
!
```

VPN ルータにコンフィグを投入できましたら「４．状態確認」に進んでください。

４．状態確認

VPN ルータのコマンドラインインタフェース(CLI)より AX-Network-Manager に ping コマンドで疎通確認をします。宛先はパラメータシートのアラクサラ記入欄に記載してあります AX-NetowrkManager の IP アドレス欄を参照してください。

AX-NetworkManager の IP アドレス	172.16.2.30/27

応答が無い場合、以下の状態確認コマンドを利用して問題箇所の特定を行ってください。

・show ipsec sa
　IPsec SA が正常に確立していることを確認するコマンドです。SA が確立していないときは、前の手順で設定した IPsec/IKE パラメータの設定に誤りは無いか確認してください。

・show ip bgp summary
　BGP ピアとの隣接関係が正常に確立していることを確認するコマンドです。IPsec SA が正常に確立しているにも関わらず、BGP ピアが確立しない場合は（ESTABLISH 以外)、前の手順で設定した BGP の設定に誤りは無いか確認してください。

＜AX620R シリーズでの show ipsec sa 実行例＞

```
IX2215(config)# show ipsec sa
IPsec SA - 2 configured, 6 created
Interface is Tunnel0.0
  Key policy map name is ipsec-map1
    Tunnel mode, 4-over-4, autokey-map
    Local address is A.A.A.A
    Remote address is B.B.B.B
    Outgoing interface is GigaEthernet0.0
    Interface MTU is 1438, path MTU is 1500
    Inbound:
      ESP, SPI is 0xb6eca893(3068962963)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 3584 seconds
      ESP, SPI is 0x4b8585cf(1267041743)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 456 seconds
      Replay detection support is on
    Outbound:
      ESP, SPI is 0xc4b83b01(3300408065)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 3584 seconds
      Replay detection support is on
    Perfect forward secrecy is 1024-bit
Interface is Tunnel1.0
  Key policy map name is ipsec-map2
    Tunnel mode, 4-over-4, autokey-map
    Local address is A.A.A.A
    Remote address is C.C.C.C
    Outgoing interface is GigaEthernet0.0
    Interface MTU is 1438, path MTU is 1500
    Inbound:
      ESP, SPI is 0x7d9c9d2b(2107415851)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 3398 seconds
      ESP, SPI is 0xd79a37c(226075516)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 298 seconds
      Replay detection support is on
    Outbound:
      ESP, SPI is 0xcd84d9d8(3448035800)
        Transform is ESP-AES-128-HMAC-SHA-96
        Remaining lifetime is 3398 seconds
      Replay detection support is on
```

```
    Perfect forward secrecy is 1024-bit
```

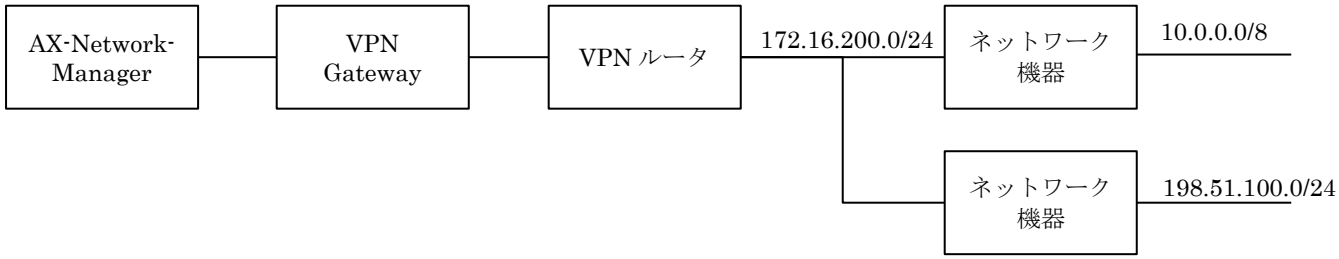
＜AX620R シリーズでの show ip bgp summary 実行例＞

```
IX2215(config)# show ip bgp summary
BGP router ID A.A.A.A, local AS number 65000
2 BGP AS-PATH entries

Neighbor        V    AS    MsgRcvd MsgSent Up/DownTime   State
 D.D.D.1        4    GGGG  22991   22991   2d15h51m28s   ESTABLISHED
 E.E.E.1        4    GGGG  22989   22991   2d15h51m27s   ESTABLISHED

Total number of neighbors 2
```

赤色太文字のようになっていれば問題がありません。問題がなければ「５．AX620R シリーズにお客さまネットワークへの経路を登録」に進んでください。

５．AX620R シリーズにお客さまネットワークへの経路を登録

VPN ルータのコマンドラインインタフェース(CLI)よりお客さまネットワークの経路を VPN ルータに登録してください。この設定が無い場合 AX-Network-Manager からネットワーク機器へ到達できません。ネットワーク構成例と投入するコンフィグについて下図、下表に示します。




```
ip route default 172.16.200.1 GigaEthernet0.0
ip route 10.0.0.0/8 172.16.200.3
ip route 198.51.0.0/16 172.16.200.2
```

VPN ルータにコンフィグを投入できましたら「６．ブラウザから AX-Network-Manager にアクセス」に進んでください。

６． ブラウザから AX-Network-Manager にアクセス

ブラウザから AX-Network-Manager にアクセスします。アクセスする IP アドレスはパラメータシートのアラクサラ記入欄に記載してあります AX-NetowrkManager の IP アドレス欄を参照してください。下図のような証明書のアラートがでることがありますが詳細設定ボタンを押下後に「XXX.XXX.XXX.XXX にアクセスする(安全ではありません)」のリンクをクリックください。

問題なければ下図のように AX-Network-Manager のログイン画面が表示されます。

7．[参考]パラメータシートを用いた設定

VPN ルータに AX620R シリーズを利用する場合の VPN トンネルおよび BGP の設定手順について説明します。

[VPN トンネルの設定手順]
パラメータシートのアラクサラ記入欄に記載してあります IPSec VPN トンネル 1 の情報をコマンドラインインタフェース(CLI)より VPN ルータに投入してください。投入するコンフィグとパラメータシートの値について下表に示します。なお、ご利用の VPN ルータによって必要なパラメータは異なりますが、本例では AX620R シリーズの設定に必要な項目のみ記載しております。

```
ike nat-traversal
!
ike proposal ike-prop encryption aes hash sha group 1024-bit
!
ike policy ike-policy1 peer ②B.B.B.B key ①BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB ike-prop
ike keepalive ike-policy1 10 3
!
ipsec autokey-proposal ipsec-prop esp-aes esp-sha lifetime time 3600
!
ipsec autokey-map ipsec-map1 sec-list peer ②B.B.B.B ipsec-prop pfs 1024-bit
!
watch-group watch_tunnel_1 10
  event 10 ip unreach-host ③D.D.D.1 Tunnel0.0
  action 10 ipsec clear-sa Tunnel0.0
!
network-monitor watch_tunnel_1 enable
!
interface Tunnel0.0
  tunnel mode ipsec
  ip address ④D.D.D.2/30
  ip tcp adjust-mss auto
  ipsec policy tunnel ipsec-map1 df-bit ignore pre-fragment out
  no shutdown
!
```

事前共有鍵(Pre-Shared Key)	BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB …①
IPSec 接続先 IP アドレス	B.B.B.B …②
接続先 BGP ピアの IP アドレス	D.D.D.1/30 …③
トンネルインタフェースの IP アドレス	D.D.D.2/30 …④

VPN ルータにコンフィグを投入できましたら IPSec VPN トンネル 1 と同様に IPSec VPN トンネル 2 の情報をコマンドラインインタフェース(CLI)より VPN ルータに投入してください。投入するコンフィグとパラメータシートの値について下表に示します。

```
ike policy ike-policy2 peer ②C.C.C.C key ①CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC ike-prop
ike keepalive ike-policy2 10 3
!
ipsec autokey-map ipsec-map2 sec-list peer ②C.C.C.C ipsec-prop pfs 1024-bit
!
watch-group watch_tunnel_2 10
  event 10 ip unreach-host ③E.E.E.1 Tunnel1.0
  action 10 ipsec clear-sa Tunnel1.0
!
network-monitor watch_tunnel_2 enable
!
interface Tunnel1.0
  tunnel mode ipsec
  ip address ④E.E.E.2/30
  ip tcp adjust-mss auto
  ipsec policy tunnel ipsec-map2 df-bit ignore pre-fragment out
```

```
  no shutdown
!
```

事前共有鍵(Pre-Shared Key)	CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC …①
IPSec 接続先 IP アドレス	C.C.C.C …②
接続先 BGP ピアの IP アドレス	E.E.E.1/30 …③
トンネルインタフェースの IP アドレス	E.E.E.2/30 …④

[BGP の設定手順]
パラメータシートのアラクサラ記入欄に記載してあります IPSec VPN トンネル 1 と IPSec VPN トンネル 2 の情報をコマンドラインインタフェース(CLI)より VPN ルータに投入してください。投入するコンフィグとパラメータシートの値について下表に示します。

```
router bgp 65000
  neighbor ①D.D.D.1 remote-as ②FFFF
  neighbor ①D.D.D.1 timers 10 30
  neighbor ③E.E.E.1 remote-as ④GGGG
  neighbor ③E.E.E.1 timers 10 30
  address-family ipv4 unicast
    originate-default always
!
```

IPSec VPN トンネル 1	接続先 BGP ピアの IP アドレス	D.D.D.1/30 …①
	接続先 BGP ピアの AS 番号	FFFF …②
IPSec VPN トンネル 2	接続先 BGP ピアの IP アドレス	E.E.E.1/30 …③
	接続先 BGP ピアの AS 番号	GGGG …④

VPN ルータにコンフィグを投入できましたら「４．状態確認」に進んでください。