



# ネットワーク関連の設定

---

この章は、次の内容で構成されています。

- [CIMC NIC の設定, 1 ページ](#)
- [共通プロパティの設定, 4 ページ](#)
- [IPv4 の設定, 4 ページ](#)
- [サーバ VLAN の設定, 6 ページ](#)
- [ネットワークセキュリティの設定, 7 ページ](#)

## CIMC NIC の設定

### CIMC NIC

CIMC への接続には、2 種類の NIC モードを使用できます。

#### NIC モード

CIMC ネットワークの設定により、CIMC に到達できるポートが決定します。プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- **Dedicated** : CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- **Shared LOM** : CIMC への接続は、オンボード LAN (LOM) イーサネット ホスト ポート上の LAN、およびルータの PCIe インターフェイスと MGF インターフェイスを介して利用できません。



---

(注) shared\_lom モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

---

## NIC 冗長化

CIMC ネットワーク冗長化の設定により、NIC 冗長化の処理方法が決定します。

- None : 冗長化は使用できません。
- Active-Standby : 1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。

## CIMC NIC の設定

NIC モードおよび NIC 冗長化を設定するには、次の手順を使用します。

### はじめる前に

NIC を設定するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope network</b>	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # <b>set mode {dedicated   shared_lom}</b>	NIC モードを次のいずれかに設定します。 <ul style="list-style-type: none"> <li>• Dedicated : CIMC へのアクセスに管理イーサネット ポートを使用します。</li> <li>• Shared LOM : CIMC へのアクセスに LAN On Motherboard (LOM; マザーボードのオンボード LAN) イーサネット ホスト ポートを使用します。 (注) SharedLOM を選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。</li> </ul>
ステップ 4	Server /cimc/network # <b>set redundancy {none   active-standby}</b>	NIC モードが Shared LOM である場合に、NIC 冗長モードを設定します。冗長モードは、次のいずれかになります。 <ul style="list-style-type: none"> <li>• none : LOM イーサネット ポートは単独で動作し、問題が生じた場合もフェールオーバーしません。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• active-standby : 1 つの LOM イーサネット ポートに障害が発生すると、トラフィックは別の LOM ポートにフェールオーバーします。</li> </ul>
ステップ 5	<pre>Server /cimc/network # set interface {console   ge1   ge2   ge3   ge1-ge2   ge1-ge3   ge2-ge3   ge1-ge2-ge3}</pre>	<p>NIC インターフェイスを次のいずれかに設定します。</p> <ul style="list-style-type: none"> <li>• console : ルータの PCIe インターフェイスを E シリーズサーバに接続するために使用される内部インターフェイス。</li> <li>• ge1 : 高速バックプレーンスイッチを介して CIMC にアクセスするために使用される内部インターフェイス。</li> <li>• ge2 : プライマリ インターフェイスまたはバックアップ インターフェイスとして使用できる外部インターフェイス。</li> <li>• ge3 : プライマリ インターフェイスまたはバックアップ インターフェイスとして使用できる外部インターフェイス。</li> <li>• ge1-ge2 : GE1 インターフェイスと GE2 インターフェイスの間のフェールオーバー (アクティブスタンバイのみ)。</li> <li>• ge1-ge3 : GE1 インターフェイスと GE3 インターフェイスの間のフェールオーバー (アクティブスタンバイのみ)。</li> <li>• ge2-ge3 : GE2 インターフェイスと GE3 インターフェイスの間のフェールオーバー (アクティブスタンバイのみ)。</li> <li>• ge1-ge2-ge3 : GE1、GE2、および GE3 の各インターフェイスの間のフェールオーバー (アクティブスタンバイのみ)。</li> </ul> <p>(注) GE3 インターフェイスを含むすべてのインターフェイス オプションは、倍幅 E シリーズサーバに対してのみ適用できます。</p>
ステップ 6	<pre>Server /cimc/network # commit</pre>	<p>トランザクションをシステムの設定にコミットします。</p> <p>(注) 使用可能な NIC モードおよび NIC 冗長モードのオプションは、お使いのプラットフォームによって異なります。サーバでサポートされていないモードを選択すると、変更を保存するときにエラーメッセージが表示されます。</p>

次に、CIMC ネットワーク インターフェイスを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
Server /cimc/network #
```

## 共通プロパティの設定

サーバを説明するには、共通プロパティを使用します。

### はじめる前に

共通プロパティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope network</b>	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # <b>set hostname</b> <i>host-name</i>	ホストの名前を指定します。
ステップ 4	Server /cimc/network # <b>commit</b>	トランザクションをシステムの設定にコミットします。

次に、コマンドのプロパティを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Server /cimc/network *# commit
Server /cimc/network #
```

## IPv4 の設定

### はじめる前に

IPv4 ネットワークの設定を実行するには、admin 権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope network</b>	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # <b>set dhcp-enabled {yes   no}</b>	CIMC で DHCP を使用するかどうかを選択します。 (注) DHCP がイネーブルである場合は、CIMC 用に 1 つの IP アドレスを予約するように DHCP サーバを設定することを推奨します。サーバの複数のポートを通じて CIMC に到達できる場合、それらのポートの全範囲の MAC アドレスに対して 1 つの IP アドレスを予約する必要があります。
ステップ 4	Server /cimc/network # <b>set v4-addr ipv4-address</b>	CIMC の IP アドレスを指定します。
ステップ 5	Server /cimc/network # <b>set v4-netmask ipv4-netmask</b>	IP アドレスのサブネット マスクを指定します。
ステップ 6	Server /cimc/network # <b>set v4-gateway gateway-ipv4-address</b>	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # <b>set dns-use-dhcp {yes   no}</b>	CIMC が DNS サーバアドレスを DHCP から取得するかどうかを選択します。
ステップ 8	Server /cimc/network # <b>set preferred-dns-server dns1-ipv4-address</b>	プライマリ DNS サーバの IP アドレスを指定します。
ステップ 9	Server /cimc/network # <b>set alternate-dns-server dns2-ipv4-address</b>	セカンダリ DNS サーバの IP アドレスを指定します。
ステップ 10	Server /cimc/network # <b>commit</b>	トランザクションをシステムの設定にコミットします。
ステップ 11	Server /cimc/network # <b>show [detail]</b>	(任意) IPv4 ネットワークの設定を表示します。

次に、IPv4 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
```

```

Server /cimc/network # set dhcp-enabled no
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: no
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated
  NIC Redundancy: none

Server /cimc/network #

```

## サーバ VLAN の設定

### はじめる前に

サーバ VLAN を設定するには、admin としてログインしている必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope network</b>	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # <b>set vlan-enabled {yes   no}</b>	CIMC を VLAN に接続するかどうかを選択します。
ステップ 4	Server /cimc/network # <b>set vlan-id id</b>	VLAN 番号を指定します。
ステップ 5	Server /cimc/network # <b>set vlan-priority priority</b>	VLAN でのこのシステムのプライオリティを指定します。
ステップ 6	Server /cimc/network # <b>commit</b>	トランザクションをシステムの設定にコミットします。
ステップ 7	Server /cimc/network # <b>show [detail]</b>	(任意) ネットワークの設定を表示します。

次に、サーバ VLAN を設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: yes
  VLAN ID: 10
  VLAN Priority: 32
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated
  NIC Redundancy: none

Server /cimc/network #
```

## ネットワークセキュリティの設定

### ネットワークセキュリティ

CIMCは、IPブロッキングをネットワークセキュリティとして使用します。IPブロッキングは、サーバまたはWebサイトと、特定のIPアドレスまたはアドレス範囲との間の接続を防ぎます。IPブロッキングは、これらのコンピュータからWebサイト、メールサーバ、またはその他のインターネットサーバへの不要な接続を効果的に禁止します。

禁止IPの設定は、一般的に、Denial of Service (DoS; サービス拒絶) 攻撃から保護するために使用されます。CIMCは、IPブロッキングの失敗回数を設定して、IPアドレスを禁止します。

### ネットワークセキュリティの設定

IPブロッキングの失敗回数を設定する場合は、ネットワークセキュリティを設定します。

#### はじめる前に

ネットワークセキュリティを設定するには、admin権限を持つユーザとしてログインする必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	Server# <b>scope cimc</b>	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # <b>scope network</b>	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # <b>scope ipblocking</b>	IP ブロッキング コマンド モードを開始します。
ステップ 4	Server /cimc/network/ipblocking # <b>set enabled {yes   no}</b>	IP ブロッキングをイネーブルまたはディセーブルにします。
ステップ 5	Server /cimc/network/ipblocking # <b>set fail-count fail-count</b>	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数を設定します。  この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。  3 ~ 10 の範囲の整数を入力します。
ステップ 6	Server /cimc/network/ipblocking # <b>set fail-window fail-seconds</b>	ユーザをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）を設定します。  60 ~ 120 の範囲の整数を入力します。
ステップ 7	Server /cimc/network/ipblocking # <b>set penalty-time penalty-seconds</b>	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数を設定します。  300 ~ 900 の範囲の整数を入力します。
ステップ 8	Server /cimc/network/ipblocking # <b>commit</b>	トランザクションをシステムの設定にコミットします。

次に、IP ブロッキングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```