

Express5800/R120i-1M, R120i-2M ご使用時の注意事項

このたびは弊社製品をお買い上げいただき、誠にありがとうございます。

本製品のご使用において、ご注意いただくことがあります。誠に您所入りますが、ご使用前に下記内容を必ずご一読ください。

なお、本書は必要なときにすぐに参照できるよう大切に保管してください。

- 1) はじめに
- 2) システム ROM の機能に関する注意事項
- 3) iLO5 の機能に関する注意事項
- 4) OS に関する注意事項
- 5) 全般の機能に関する注意事項
- A) ファームウェア変更に伴う変更点

1) はじめに

● 本製品のマニュアルについて

本製品に関する詳細は、以下の Web サイトに掲載しているマニュアルに記載しています。

<https://www.support.nec.co.jp/>

「NEC サポートポータル内検索」より、以下の ID で検索してください。

R120i-1M : 3170102645 R120i-2M : 3170102646

また、ESMPRO/ServerManager、ESMPRO/ServerAgentService、エクスプレス通報サービス/エクスプレス通報サービス(HTTPS)/エクスプレス通報サービス(MG)に関しては、

ESMPRO 日本語ポータルサイト<<https://jpn.nec.com/esmsm/>>

NEC サポートポータル <<https://www.support.nec.co.jp/View.aspx?id=9010102124>>

の最新の情報およびバージョンをご確認のうえ、ご利用ください。

● Starter Pack について

本製品で使用する Starter Pack は、以下の Web サイトに最新版が掲載されています。

Web サイトに掲載されている内容を確認し、バージョン S8.10-009.01 以降を適用してください。

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「S8.10-009」を検索)

● VMware ESXi/ESX のドライバ・サービスモジュールについて

本製品で使用する VMware ESXi/ESX のドライバ・サービスモジュールは、以下の Web サイトに最新版が掲載されています。Web サイトに掲載されている内容を確認し、適切なバージョンを適用してください。

(1) Agentless Management Service および iLO Channel Interface Driver

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「Agentless Management Service」を検索し、【最新版】と表示される「iLO FW X.XX 以上専用 Agentless Management Service および iLO Channel Interface Driver (VMware ESXi/ESX 8.0/9.0 版)」を適用してください。ESXi 7.0 をご利用の場合は、【旧版】と表示される該当の iLO FW X.XX 以上専用で、お使いの ESXi バージョンに対応したものを適用してください。(X.XX は数字))

(2) WBEM プロバイダおよび CLI ツール

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「WBEM プロバイダ」を検索し、【最新版】WBEM プロバイダおよび CLI ツール(VMware ESXi/ESX 7.0 版, 8.0 版, 9.0 版)」を適用してください)

(3) VMware ESXi/ESX デバイスドライバ

<https://www.support.nec.co.jp/View.aspx?id=3140105866>

(「PC サーバ/ブレードサーバ(Express5800 シリーズ)」から対象 OS の「デバイスドライバ一覧」を選択)

● 本製品の保守作業時間に関して

本製品は、障害発生時等に伴う保守作業に際し、保守部材と搭載ファームウェア、ドライバの組み合わせによっては、保守作業に時間を要することがあります。

2) システム ROM の機能に関する注意事項

● UEFI Boot Order Control の注意事項

システム ROM バージョン 2.24 の場合、UEFI Boot Order Control メニュー(*1)で新たなブートデバイスの有効化、または無効化の設定や保存ができません。

詳細は以下の Web サイトを確認してください。

<https://www.support.nec.co.jp/View.aspx?id=3140109992>

ブートデバイスの起動優先順位を変更する際は、UEFI Boot Order メニュー(*2)にて行ってください。

また、UEFI Boot Order メニューまたは UEFI Boot Order Control メニューに移動するたびに、画面下段にある "Changes Pending" 文字列の前に赤い◎が表示されます。

必要に応じて<F10>キーを押下し、設定の保存を行ってください。

(*1)BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control

(*2)BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order

● システムデフォルトオプション ご使用時の注意事項

システム設定をデフォルト値に戻す場合は、「Restore Default System Settings」を使用してください。

「Restore Default Manufacturing Settings」メニューを使用した場合、BIOS/Platform Configuration (RBSU)の設定がデフォルト値に戻るだけでなく、実装されている PCI カード(RAID コントローラのアレイ構成情報や、ネットワークカードの iSCSI 設定情報)もデフォルト値に戻ります。

そのため、RAID コントローラのアレイ構成に OS をインストールされていた場合、アレイの再構築後 OS の再インストールが必要となります。

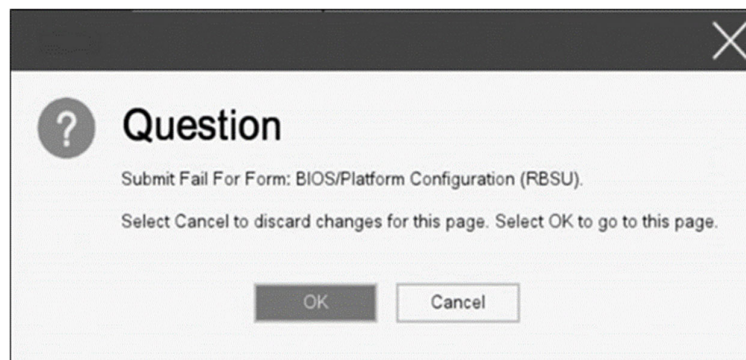
Restore Default System Settings (推奨)

Restore Default Manufacturing Settings (PCI カード含めてデフォルト値に戻す場合のみ)

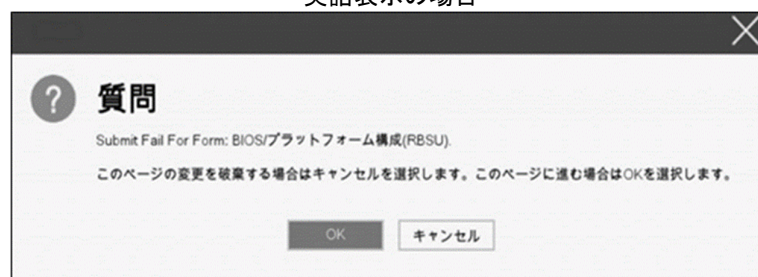
● Submit Fail For Form の Question(質問)ポップアップ表示についての注意事項

システムユーティリティにおいて設定の変更中に、次の Submit Fail For Form の Question(質問)ポップアップが表示された場合は、「キャンセル」を選択して変更を破棄してください。

さらに、サーバーの再起動を行ってシステムユーティリティに入り直してから設定の変更を再度行ってください。もし「OK」を押してそのまま設定変更を進めると、装置に記録されている Serial Number、Product ID などの設定情報が消失することがあります。



英語表示の場合

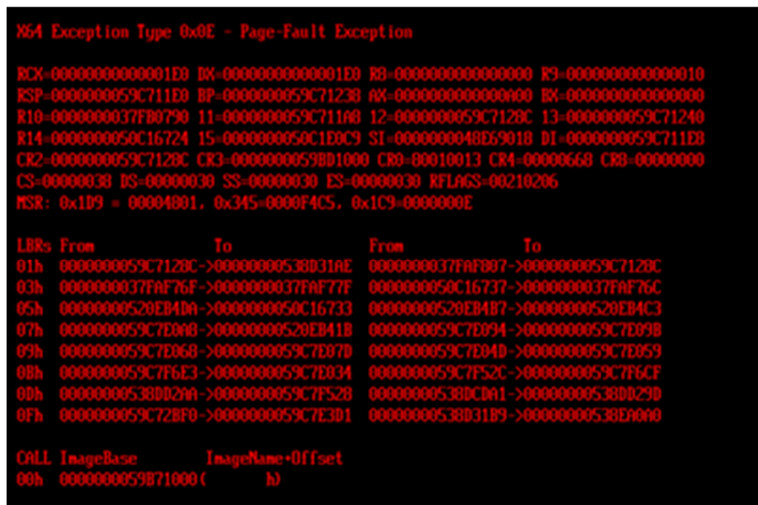


日本語表示の場合

- 赤文字画面(RSOD : Red Screen Of Death)が表示された場合の対処について

装置の構成変更や設定変更などシステムの状態を変更した場合や、接続デバイスへのアクセスタイミングにより、OS 起動前に稀に赤文字画面(RSOD)が表示され、本製品の操作ができなくなることがあります。構成変更や設定変更に伴う一過性の事象の場合があり電源をオフ、オンすることによって回復します。

赤文字画面(RSOD)が表示された場合、装置の電源のオフ、オンをお願いします。
問題が解決しないときは、ファーストコンタクトセンターにお問い合わせください。



赤文字画面の例

- セキュアブートに失敗した場合、赤文字画面(RSOD : Red Screen Of Death)が表示されることがある

RBSU の Attempt Secure Boot(*)を Enabled に設定している場合、セキュアブート時の署名検証に失敗すると、OS 起動前に赤文字画面(RSOD)が表示され、本製品の操作ができなくなることがあります。

(*) BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Attempt Secure Boot

赤文字画面(RSOD)が表示された場合、装置の電源をオフ、オンした後に、セキュアブートが失敗する原因(例:ブートローダ/OS のコンポーネントが古く、現在のセキュアブートポリシーで検証に失敗するなど)を解消してから、ブートデバイスから起動してください。

対処方法の一例として、Attempt Secure Boot を Disabled にした後に OS(またはブートローダ/回復環境)を最新の状態に更新し、再度 Attempt Secure Boot を Enabled に設定後、OS の起動を確認してください。

問題が解決しないときは、ファーストコンタクトセンターにお問い合わせください。

- 「Memory Initialization Start」のメッセージで POST 停止した場合の対処について

「Memory Initialization Start」のメッセージで POST 停止した場合、システムメンテナンススイッチの SW6 によりシステム設定をデフォルト値に戻すことで復旧することができます。

詳細な手順は、メンテナンスガイド「1章(7.4.3 システム設定をデフォルト値に戻す)」の項をご参照ください。

- Intel(R) Xeon(R) Silver 4309Y、または Gold 5315Y プロセッサをご使用のお客様への注意事項

システム ROM バージョン 2.00 (03/06/2024)未満が適用されている、かつ Intel(R) Xeon(R) Silver 4309Y、または Gold 5315Y プロセッサのいずれかを搭載しているサーバーをご使用の場合、ファンが高速回転することがあります。

システム ROM バージョン 2.00 (03/06/2024)では、この問題が修正されています。

● Boot Order Policy オプションについての注意事項

システム ROM U46 バージョン 1.64 (08/11/2022)以降を使用する場合、「Boot Order Policy」オプション(*)の設定は、「Reset After Failed Boot Attempt」に設定してください。本設定により、Boot Order のリストにあるすべてのブートデバイスでブートに失敗した(ブートデバイスが初期化に時間がかかるなど)場合、システムの再起動を行います。システムの再起動により、ブート処理を再実行することで OS ブートに成功することがあります。2022 年 12 月より、「Boot Order Policy」オプションの工場出荷時設定は[Retry Boot Order Indefinitely]から[Reset After Failed Boot Attempt]に変更されました。

(*)BIOS/Platform Configuration (RBSU) > Boot Options > Boot Order Policy

● Server Configuration Lock (SCL)についての注意事項

- (1) システム運用中は SCL 機能を無効にし、使用しないでください。
- (2) SCL 機能有効時に設定するパスワードは大切に保管してください。SCL のパスワードを紛失した状態で、SCL 機能によりロック(OS ブート前に停止)されると、ロック解除できず、二度とブートできなくなります。

ブート可能状態への復旧/回復は有償にて承ることになります。

なお、SCL のパスワードを紛失した場合、SCL のパスワードをクリアする方法はありません。

- (3) 保守を依頼する際は、SCL 機能を無効化していただく必要があります。
SCL 機能を無効にできない場合、**保守は有償にて承ることになります。**
- (4) RBSU の「Halt on Server Configuration Lock failure detection」機能は有効化しないでください。もし有効に設定した場合、SCL 機能が回復不能条件の該当を検出し、ロック(OS ブート前に停止)されてしま

と、

システムユーティリティも起動できず、二度とサーバー構成ロックを無効にすることができません。

ブート可能状態への復旧/回復は有償にて承ることになります。

SCL 機能の回復不能条件

- RBSU の設定変更によりロックされた場合
- ファームウェア更新によりロックされ、元のファームウェア バージョンに戻すことができない場合
- DIMM、または PCI オプションカードの故障によりロックされた場合

- (5) システム ROM バージョン 1.40 (04/28/2021)の場合、搭載 PCI オプションカードの取外し、または故障した際に、SCL 機能によりブートが抑止されますが、POST エラーメッセージが表示されず、インテグレートド マネジメントログ(IML)にもログは記録されません。システム ROM バージョン 1.52 (09/22/2021)では、ブート抑止の際、POST エラーメッセージが表示され、IML にもログが記録されます。

● iLO イベントログ(IEL)に IPMI Watchdog Timer Timeout のログが登録される。

システム ROM バージョン 1.58 (01/13/2022)が適用されている場合、かつ IPMI Watchdog Timer オプションを「Disabled(出荷時の設定)」に設定している場合、iLO イベントログに下記の IPMI Watchdog Timer Timeout が登録されることがあります。

以下の手順を実施することで本問題が解消します。

iLO IPMI Watchdog Timer Timeout: Action: None, TimerUse: 0x44, TimerActions: 0x00

イベントクラス: 0x23

イベントコード: 0xB3

復旧手順 :

以下の復旧手順 1、または 2 のどちらかを実施していただくことで、本問題が解消できます。

復旧手順 1

- (1) 装置の電源をオフにし、電源コードをコンセントから外す。
- (2) 30 秒以上経過したのち、電源コードをコンセントに接続する。

復旧手順 2

システムユーティリティより、IPMI Watchdog Timer オプションの設定を 2 回変更します。

- (1) POST 中に<F9>キーを押下し、システムユーティリティを起動する。
- (2) System Configuration > BIOS/Platform Configuration(RBSU) > System Options > Server Availability > IPMI Watchdog Timer オプションを「Enabled」に設定する。
- (3) <F12>キーを押下し、設定を保存してシステムを再起動する。
- (4) POST 中に<F9>キーを押下し、システムユーティリティを起動する。
- (5) System Configuration > BIOS/Platform Configuration(RBSU) > System Options > Server Availability > IPMI Watchdog Timer オプションを「Disabled」に設定する。
- (6) <F12>キーを押下し、設定を保存してシステムを再起動する。

● システムユーティリティおよびワнтаイムブートメニューの表示について

以下の発生条件を満たす場合、ワнтаイムブートメニューと RBSU の PCIe Device Configuration メニュー(*)に、RAID コントローラ名が正しく表示されないことがあります。RAID コントローラ名表示のみの問題であり、RAID コントローラに搭載されている HDD/SSD からのブートには影響しません。

(*)BIOS/Platform Configuration (RBSU) > PCIe Device Configuration

【発生条件】

- ・ N8103-189、N8103-190、N8103-191、N8103-192、N8103-193、N8103-194、N8103-195、N8103-196、N8103-197、N8103-201、N8103-237、N8103-238 の場合

以下 2 つの条件をすべて満たす場合、発生します。

1. RAID コントローラファームウェアが v4.11 以降、または v3.01.04.072 以降
2. システム ROM がバージョン 1.64 (08/11/2022)未満

● TPM Visibility のヘルプについての注意事項

「TPM Visibility」の設定を変更するには、「Platform Certificate Support」設定が【Disabled】に設定されている必要があります。

システムユーティリティの「TPM Visibility」に関するヘルプ表示(赤字部分)は“プラットフォーム証明書サポートは有効に設定されていません”と表示されますが、正しくは“プラットフォーム証明書サポートは無効に設定されていません”となります。

RBSU > Server Security > Trusted Platform Module Options > Advanced Trusted Platform Module Options
> TPM Visibility

RBSU > Server Security > Advanced Security Options > Platform Certificate Support

3) iLO5 の機能に関する注意事項

● iLO の再起動を行う場合の注意事項

サーバー起動から OS の起動完了までの間(POST 実行中も含みます)は、iLO の再起動を行わないでください。
また、システムユーティリティの操作途中も、iLO の再起動を行わないでください。

該当タイミングで iLO の再起動を行うと、期待しない動作となる場合があります。

たとえばシステムユーティリティの設定変更途中に iLO の再起動(※)を行うと、直後のシステム再起動処理(Reboot)が正常に動作しない場合や、装置に記録されている Serial Number、Product ID などの設定情報が消失することがあります。また、POST 実行中に iLO の再起動を行うと、iLO Web インターフェイス : [Information] > [Overview] ページにおける UUID、UUID(論理)が不正な表示になる場合があります。

不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

＜対象となる iLO の再起動の方法＞

- ・ iLO Web インターフェイスなどを利用したネットワーク経由での iLO の再起動。
- ・ UID スイッチを使用した iLO の再起動。

※ システムユーティリティの「BMC Configuration Utility」での設定変更後の iLO の再起動については、本書の「システムユーティリティの「BMC Configuration Utility」の操作についての注意事項」を参照して操作してください。

● iLO のダウングレードポリシー機能の注意事項

iLO の拡張ライセンスがインストールされている場合、[Security] > [Access Settings] > [Update Service] > [Downgrade Policy]の設定を『Permanently disallow downgrades』に変更しないでください。

『Permanently disallow downgrades』に設定した場合、ファームウェアのダウングレードを行うことができなくなります。また、iLO に対して永続的な変更が行われるため、『Permanently disallow downgrades』に設定後は、iLO の各種インターフェイスや各種ユーティリティから本設定の変更を行おうとしても変更することができません。

なお、本設定は Set to factory defaults オプションから iLO を出荷時のデフォルト設定にリセットを行った場合においても、リセットされず『Permanently disallow downgrades』を維持します。

● iLO のセキュリティ機能の注意事項

iLO Web インターフェイスの[Information] > [Security Dashboard]および iLO Web インターフェイス画面の右上部に  リスクが表示される場合があります。

RBSU の設定や iLO の設定の内容によって、iLO セキュリティの状態がリスク状態(赤色)で表示されますので、お客様のセキュリティポリシーに応じてセキュリティの対処を行ってください。

推奨値などの詳細については、iLO5 ユーザーズガイドを参照してください。

ただし、『Require Host Authentication』設定については、本書内の「iLO Web インターフェイスから[ホスト認証が必要]設定を有効(※)に設定した場合の注意事項」に記載がありますので、ご確認ください。

iLO の負荷の状態により[Information] > [Security Dashboard]の”全体セキュリティステータス”が『リスク』であっても、iLO Web インターフェイス画面の右上部の”iLO セキュリティ”アイコンが無色になる場合があります。
[Information] > [Security Dashboard]の”全体セキュリティステータス”が現在のセキュリティ状態を示します。

● ネットワークブリッジ構成時の iLO Web インターフェイスのネットワーク情報の表示について

ネットワークをブリッジ設定で構成してご使用の場合、iLO Web インターフェイスの[Information] > [Network] > [Physical Network Adapters]に表示される内容が OS 上の内容と一致しない場合があります。ブリッジ情報の詳細は、OS 上のネットワークアダプタのプロパティにてご確認ください。

● iLO Web インターフェイスから[ホスト認証が必要]設定を有効(※)に設定した場合の注意事項

(※) iLO5 ファームウェアバージョン : 1.40 以降を適用した環境の場合が対象となります。

[Security] > [Access Settings] > [iLO]にある[ホスト認証が必要/Require Host Authentication]を『有効』に設定しないでください。

設定を行った場合、次に示す状況が発生します。

- ・アラートビューアに、“Remote Insight/Integrated Lights-Out 認証されないログイン試行検出”のメッセージが多数表示されます。
- ・ Starter Pack (Standard Program Package)を適用するとエラーが発生します。

また、次のサービスや機能をご利用いただけません。

- ・ エクスプレス通報サービスにおいてハードウェア障害に関する通報
- ・ RAID 通報サービス
- ・ サーバ診断カルテのハードウェア診断機能
- ・ iLO が収集するハードウェアに関するデバイス情報や設定情報の参照、およびイベントログ採取機能

● iLO Web インターフェイスのストレージ情報に関する注意事項について

iLO5 ファームウェアバージョン 3.00 以降をご使用の場合:

サーバー再起動後に、iLO Web インターフェイスで[システム情報] > [ストレージ]タブをクリックすると、以下のメッセージが表示され、RAID コントローラや、ドライブ情報等のストレージ情報が表示されない場合があります。

"Failed to retrieve complete storage device information. Refresh the page in a few minutes. "

上記メッセージがストレージ情報ページに表示された場合、iLO リセットを行ってください。

● RESTful API ERROR が発生した場合の対処について

POST 実行中、稀に RESTful API Error が発生し、Integrated Management Log(IML)に記録されることがありますが、iLO リセットを行うことで復旧できます。

● EXPRESSBUILDER や Smart Storage Administrator(SSA)が起動できなくなった場合の対処について

iLO5 ファームウェアバージョン 2.60 未満をご使用の場合

POST 画面での<F10>キー押下、もしくは、System Utilities > Embedded Applications などから EXPRESSBUILDER を起動しようとしたとき、稀に起動できないことがあります。

また、System Utilities > System Configuration > RAID コントローラ から Launch Smart Storage Administrator(SSA)を選択し起動しようとしたとき、稀に起動できないことがあります。

その場合は、EXPRESSBUILDER を再インストールしてください。

本製品で使用する EXPRESSBUILDER は、以下の Web サイトに最新版が掲載されています。

Web サイトに掲載されている内容を確認し、バージョン E8.10-009.01 以降にアップデートしてください。

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」から、“E8.10-”を検索します)

※オンライン版の Smart Storage Administrator(SSA)の動作には影響ありません。

● 物理ドライブのステータス変更時の SNMP Trap 通報のロケーション情報欠損に関する対処について

物理ドライブのステータス変更時の SNMP Trap 通報において、ロケーション情報が欠損する場合があります。ロケーション情報に関しては、iLO Web インターフェイスの[情報] > [インテグレートドマネジメントログ]で同じイベントのロケーション情報をご確認ください。

例:Abnormal, physical drive status change detection, iLO SNMP Trap,mgr_WIN-U6HIHPNIH1Q,uru-rhel83,192.168.0.57,,2021/10/01
15:22:57, iLO, 0xc0000be6,"A physical drive status change has been detected. Current status is 3. (Location: Port 12 Controller: Slot 12)","If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

● iLO Web インターフェイスの Agentless Management Service (AMS)のステータスについて

iLO Web インターフェイスの[System Information] > [Summary] > [Subsystem and Devices]の Agentless Management Service (AMS)のステータスにおいて、不明(または利用不可能)※と表示された場合、iLO リセットを行ってください。また、その後、10 分程度経過した後、以下の Agentless Management Service (AMS)の再起動方法の対象 OS を参考に、Agentless Management Service (AMS)を再起動してください。

※ Agentless Management Service (AMS)のステータスが不明(または利用不可能)の状態の場合、iLO Web インターフェイスの[System Information] > [Storage]や[Network]の一部の情報が取得できず、正しく表示されません。

< Agentless Management Service (AMS)の再起動方法 >

・ Windows の場合

Windows の管理ツール → サービス → "Agentless Management Service"を右クリックし、再起動してください。

・ Red Hat Enterprise Linux 7.x/8.x の場合

以下のコマンドを実行します。

```
# systemctl restart smad  
# systemctl restart amsd
```

・ ESXi/ESX 7.0/8.0/9.0 の場合

以下のコマンドを実行します。

```
# /etc/init.d/amsd restart
```

● iLO5 ファームウェアバージョン 2.65 以降の注意点

iLO Web インターフェイスの「システム情報」>「デバイスインベントリ」で BackPlane (BP)の位置情報が不正になる場合がありますが表示だけの問題で動作に影響はありません。

正常時) Slot=#:Port=#:Box=#

※#は接続先により番号が変わります。

不正時) Slot=#:Port=?l:Box=?

数字の部分が?と表示されます。

または Box=#

Box のみ表示されます。

● Java IRC のセッションタイムアウト時の表示に関する注意事項について

Java 統合リモートコンソール(Java IRC)起動中にリモートコンソールのセッションが切れた場合に、セッションが切れたことを示すポップアップと一緒にセッション切れとは直接関係のない内容のポップアップも表示されます。

Java IRC のセッションが切れた場合には、IRC の下部に以下のメッセージが表示されます。本メッセージが表示されている場合には、表示されているポップアップの内容は無視してください。

■ “セッションはタイムアウトか認識されないアクセスによって閉じられました。”

● サーバー再起動時の FAN 高速化に関する注意事項について

iLO5 ファームウェアバージョン 2.90 以降をご使用の場合:

サーバーの再起動を行うと、稀に FAN の高速回転やうなり音が 7 分以上継続する場合があります。

この場合は、再度サーバーの再起動を実施してください。

- 通報に関する注意事項

iLO5 ファームウェアバージョン 3.00 以降をご使用の場合:

ESMPRO/ServerManager をご利用されている場合、物理ドライブの状態変化に伴い、アラートビューアにおいて「物理ドライブのステータス変化検出」のアラートが表示されます。

この際、物理ドライブのステータスに応じて、ロケーション情報が以下の二パターンのいずれかで表示されます。

① (Location: Slot=(A):Port=(B):Box=(C):Bay=(D) Controller: <NULL>)

② (Location: Port=(B):Box=(C):Bay=(D) Controller: Slot (A))

A:コントローラの位置(スロット番号)

B:物理ドライブのポート番号

C:物理ドライブのボックス番号

D:物理ドライブのベイ番号

- Intelligent Platform Management Interface (IPMI) の暗号化スイートを使用する場合の注意事項

iLO5 は、IPMI の暗号化スイート 17 をサポートしていません。

"ipmitool"ユーティリティバージョン 1.8.18 以降を使用して、インターフェイスを"lanplus"、暗号化スイートを"17"に指定し、IPMI コマンドを実行した場合、以下のエラーが発生し、IPMI コマンド実行が失敗します。

Error in open session response message : no matching cipher suite

Error: Unable to establish IPMI v2 / RMCP+ session.

4) OS に関する注意事項

● Windows Server OS ご使用時の注意事項

32 コア(物理コア)を超えるプロセッサを搭載している場合、Windows Server 2016、Windows Server 2019 でシステム情報(Msinfo32.exe)ツールとタスクマネージャーの[パフォーマンス]タブに、プロセッサのソケット数やコア数、L1 キャッシュと L2 キャッシュのサイズが正しく表示されません。
詳細は、下記のリンクを参照してください。

Windows Server 2016 サポート情報

<<https://www.support.nec.co.jp/View.aspx?id=3140105448>>

Windows Server 2019 サポート情報

<<https://www.support.nec.co.jp/View.aspx?id=3140106598>>

iLO Web インターフェイスまたは System Utilities を使用して正しい CPU 情報を確認してください。

● ESMPRO/ServerManager (Windows 版)およびエクスプレス通報サービス(MG)に関する注意事項

本製品の iLO5 ファームウェアバージョンと、ESMPRO/ServerManager (Windows 版)およびエクスプレス通報サービス(MG)のバージョンの組み合わせによっては ESMPRO/ServerManager (Windows 版)および iLO 管理機能向けの受信情報設定ファイルのアップデートが必要になる場合があります。

以下をご参照のうえ、アップデートが必要な場合は、最新バージョンにアップデートしてください。

各バージョンの確認方法については、本注意事項の末尾に記載します。

◆ESMPRO/ServerManager (Windows 版) に関する発生現象

iLO ファームウェア	ESMPRO/ ServerManager (Windows 版)	発生現象
Version 2.10 以降	Version 6.25 未満	・ 構成タブ > サーバー状態 "SNMP 通報設定"が"取得に失敗しました"と表示される ・ リモート制御タブ > iLO 情報 > IML の表示、IML の保存、IML 情報の取得に失敗し、表示および保存ができない ・ アラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに"不明タイプ"のアラートとして表示される
	Version 6.47 未満	・ アラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに表示されない、もしくは"不明タイプ"のアラートとして表示される

◆ESMPRO/ServerManager Ver.6 (Windows 版)のアップデート方法

(1) 以下の Web サイトより最新版の ESMPRO/ServerManager をダウンロードします。

<https://www.support.nec.co.jp/View.aspx?id=9010103524>

(2) 「ESMPRO/ServerManager Ver.6 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager をアップデートします。

◆ESMPRO/ServerManager Ver.7 (Windows 版)へのアップデート方法

(1) 以下の Web サイトより ESMPRO Platform Management Kit をダウンロードします。

<https://www.support.nec.co.jp/View.aspx?id=9010109532>

ESMPRO/ServerManager Ver.7 は ESMPRO Platform Management Kit に含まれています。

(2) ESMPRO Platform Management Kit の ESMPRO インストールツールを起動します。

(3) インストールツール画面の説明書をクリックし、Software Manuals から ESMPRO/ServerManager をクリックします。

(4) 「ESMPRO/ServerManager Ver.7 インストレーションガイド(Windows 編)」をクリックします。

(5) 「ESMPRO/ServerManager Ver.7 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager を Ver.6 から Ver.7 へアップデートします。

- ◆iLO 管理機能向けの受信情報設定ファイルに関する発生現象
※エクスプレス通報サービス(MG)をご利用されている方が対象です。

iLO ファームウェア	iLO 管理機能向けの 受信情報設定 ファイル	発生現象
Version 2.10 以降	ilo_jp.mtb Version 1.4.0 未満 iml_jp.mtb Version 1.5.0 未満 ※iLO 管理機能向けの受信 情報設定ファイルは 2 種類 あります。	ファームウェアアップデートにともない追加されたハード ウェアの障害を検知することができない。当該障害を通報 することができない。 ※受信情報設定ファイルをアップデートした場合で あっても、ESMPRO/ServerManager がアップデートされ ていないときは、上記と同様に追加されたハードウェア 障害の検知および通報ができない。

◆iLO 管理機能向けの受信情報設定ファイルのアップデート方法

- (1) 以下の Web サイトより最新版の受信情報設定ファイル(ilo_jp.mtb、iml_jp.mtb)をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010100096>
ilo_jp.mtb、iml_jp.mtb は MGMTB.zip に包含しています。
- (2) 「エクスプレス通報サービス(MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」
または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で登録済みの受信情報を削除します。
- (3) (1)でダウンロードした最新版の受信情報設定ファイルを登録します。
「エクスプレス通報サービス(MG) インストレーションガイド(Windows 編)」は以下の Web サイトからダウ
ンロードしてください。
<https://www.support.nec.co.jp/View.aspx?id=9010102124>

◆iLO5 ファームウェアのバージョン確認方法

- ・ Server Health Summary で確認する方法
サーバー本体の UID ボタンを押下して、サーバーに接続されたコンソールに表示される iLO5 ファームウェ
アのバージョンを確認します(Server Health Summary の詳細は iLO5 ユーザーズガイド参照)。
- ・ ネットワーク経由で確認する方法
iLO にネットワーク接続可能な場合、ブラウザから iLO にログインして、メニュー「ファームウェア & OS
ソフトウェア」から iLO のバージョンを確認します。

◆ESMPRO/ServerManager (Windows 版)のバージョン確認方法

- (1) ESMPRO/ServerManager にログインします。
- (2) 画面右上の「ESMPRO/ServerManager について」のリンクを選択します。
- (3) 表示される ESMPRO/ServerManager のバージョン情報を確認します。

◆iLO 管理機能向けの受信情報設定ファイルのバージョン確認方法

「エクスプレス通報サービス(MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」また
は「3.2.4 受信情報の設定」を参照して受信情報の設定画面で「詳細情報」の「iLO SNMP Trap」のバージョン
情報を確認します。

● N8104-208 を搭載した Windows Server 環境にて記録されるイベントについて

N8104-208 を搭載した Windows Server 環境にてシステムイベントログに以下のようなイベントが記録される場合
がありますが、システム運用上問題はございません。

ソース : icea
イベント ID : 89
レベル : エラー
説明 : Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
問題 : DDP パッケージの読み込み中に不明なエラーが発生しました。セーフモードに切り替え
ます。
対処 : アダプターを再起動してください。
問題が解決しない場合は、"<http://www.intel.com/support/go/network/adapter/home.htm>"から
最新のドライバーをダウンロードしてインストールしてください。
※x の値は環境により異なります。

ソース : icea
イベント ID : 91
レベル : エラー
説明 : Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
問題 : DDP パッケージの署名が無効なため、読み込めません。セーフモードに切り替えます。
対処 : "<http://www.intel.com/support/go/network/adapters/home.htm>"から最新のドライバーを
ダウンロードしてインストールしてください。
※x の値は環境により異なります。

ソース : icea
イベント ID : 1284
レベル : エラー
説明 : Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
問題 : DDP パッケージのエラー。
考えられる解決策 : 最新のベースドライバーと DDP パッケージにアップデートします。
※x の値は環境により異なります。

本事象は N8104-208 のファームウェア バージョン 3.20 以降で修正されています。
Starter Pack Version S8.10-010.5 以降を適用してください。

● VMware ESXi/ESX を使用する場合の注意事項

1. RBSU の「PCIe Hot-Plug Error Control」オプション(*)を「eDPC Firmware Control」に設定しないでください。
もし、本設定値で運用した場合、PSOD(Purple Screen Of Death)が発生することがあります。

(*) BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Hot-Plug Error Control

2. ESXi 起動時の VMware vSphere の監視 > ハードウェア > システムセンサー > センサーの表示について。

(1) 非冗長 FAN 構成において ESXi 起動完了後、下記のセンサーの健全性(vCenter : ステータス)の表示が『警告(黄色)』となる場合がありますが、ハードウェアの故障を示すものではなく運用に影響ありませんので、そのまま運用いただけます。
- Cooling Unit 1 Fans

(2) ESXi 起動完了後、下記のセンサーの健全性(vCenter : ステータス)の表示が『?』となる場合がありますが、ハードウェアの故障を示すものではなく運用に影響ありませんので、そのまま運用いただけます。
- System Chassis 1 UID

● VMware ESXi/ESX で TPM キットを使用する場合の注意事項

N8115-35 TPM キットが搭載されている場合 TPM Mode (*1)は「TPM 2.0」にて、VMware ESXi/ESX をご使用ください。

もし、TPM Mode が「TPM 1.2」に設定されている場合、稀に PSOD (Purple Screen Of Death)が発生することがあります。

(*1) 出荷時の初期設定は「TPM 2.0」です。

TPM Mode の確認および設定変更は下記メニューより確認してください。

- ・ System Utilities > System Configuration > RBSU > Server Security > Trusted Platform Module Options > Current TPM Type (設定確認)
> TPM Mode Switch Operation (設定変更)

● RAID 監視通報方式の変更について

VMware ESXi/ESX において、N8103-189/190/191/192/193/194/195/196/201/237/238 RAID コントローラと N8103-239 OS ブート専用 SSD ボードをご使用されている場合、RAID 監視通報は SNMP Trap による通報に変更になります。

詳細は、下記の Web サイトをご確認ください。

- ・ NEC サポートポータル
<https://www.support.nec.co.jp/View.aspx?id=3140108419>

● Linux OS を使用する場合の注意事項

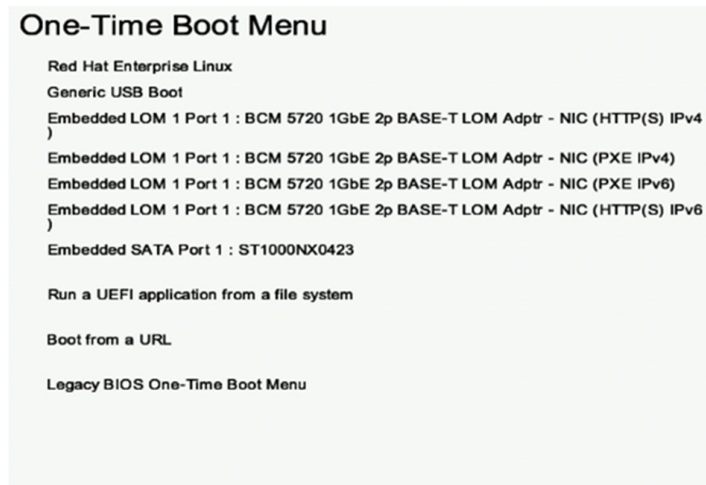
OS が自動的に認識する LOM やオプション NIC のデバイス名を使用してください。独自 udev ルールを追加する際、PCI アドレスを基準に NIC デバイス名を変更したり、固定したりする設定は行わないでください。また、PCI アドレスを含む/dev/disk/by-path/配下のストレージデバイス名は使用しないでください。

PCI アドレスを基準にしたデバイス名を使った運用が必要な場合は、PCI スロットへのカード増設/抜去、および、CPU 構成変更を行わないでください。PCI バスのアドレス情報が変化し、PCI 接続のデバイス名に影響がでることにより、ネットワークやストレージへのアクセスができなくなり、システムが正常に起動できなくなる場合があります。

● Red Hat Enterprise Linux 8.5 または、それ以前を使用する場合の注意事項

ワンタイムブートメニューから起動する場合、OS ブートマネージャー(例: Red Hat Enterprise Linux)を選択してください。

OS がインストールされた HDD や SSD などのブートデバイスを選択した場合、RSOD(Red Screen Of Death)が発生することがあります。



ワンタイムブートメニュー画面

● Red Hat Enterprise Linux 8 NVMe SSD を搭載環境での注意事項

grub2-efi-x64 パッケージをアップデートすると、OS が起動できなくなる場合があります。

NVMe SSD を搭載した対象機種において、RHEL8.3 をインストールした環境に、RHEL8.4 以降の grub2-efi-x64 パッケージを適用して再起動すると、OS が起動できなくなる問題を弊社評価で確認しているため、grub2-efi-x64 パッケージをアップデートしないでください。

- ◆ grub2-efi-x64 をアップデートして OS が起動しなくなった場合は、下記手順で grub2-efi-x64 パッケージを RHEL8.3 に戻してください。

(1) 復旧対象装置からネットワークアクセス可能な場所に、RHEL8.3 の下記パッケージを配置します。

```
grub2-efi-x64-2.02-90.el8.x86_64.rpm
grub2-common-2.02-90.el8.noarch.rpm
grub2-tools-2.02-90.el8.x86_64.rpm
grub2-tools-minimal-2.02-90.el8.x86_64.rpm
grub2-tools-efi-2.02-90.el8.x86_64.rpm
grub2-tools-extra-2.02-90.el8.x86_64.rpm
```

- (2) 弊社提供のインストレーションガイドを参照し、RHEL8.3 ブートメディアを作成して RHEL8.3 ブートメディアから起動します。
- (3) RHEL8.3 ブートメディアの起動メニューから"Troubleshooting"を選択後、"Rescue a Red Hat Enterprise Linux System"を選択してレスキューモードで起動します。

(4) レスキューモードの起動時メニューで"1) Continue"を選択後、リターンキーを押下してシェルプロンプトを表示します。

(5) "ip link" コマンドを実行し、ネットワーク接続に使用するネットワークデバイス名を確認します。

実行例:

```
sh-4.4# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
   group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

2: ens10f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode
   DEFAULT group default qlen 1000 ← 接続済みデバイス
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff

3: ens10f1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN mode
   DEFAULT group default qlen 1000
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff

4: ens10f2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN mode
   DEFAULT group default qlen 1000
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff

5: ens10f3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN mode
   DEFAULT group default qlen 1000
   link/ether xx:xx:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff
```

(6) "ifup"コマンドを実行し、ネットワークを有効化します。

実行例:

```
sh-4.4# ifup ens10f0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/
ActiveConnection/1)
```

(7) chroot コマンドを実行し、インストール済みの環境に root ディレクトリを変更します。

実行例: レスキューモードでは、インストール済みの環境が/mnt/sysrootにマウントされています。

```
sh-4.4# chroot /mnt/sysroot
bash-4.4#
```

(8) 手順(1)で準備したパッケージを scp や rsync 等のコマンドを実行して任意の場所にコピーします。

実行例: scp を使用し、装置名"server"の/workに配置したパッケージを取得

```
bash-4.4# scp server:/work/grub2-*.rpm /tmp/
```

(9) コピーしたパッケージを適用します。

実行例:

```
bash-4.4# rpm -Uvh --oldpackage /tmp/grub2-*.rpm
```

(10) chroot コマンドを終了後、レスキューモードを終了してシステムを再起動し、OS が起動できることを確認します。

実行例:

```
bash-4.4# exit → chroot 終了
sh-4.4# exit → レスキューモード 終了
```

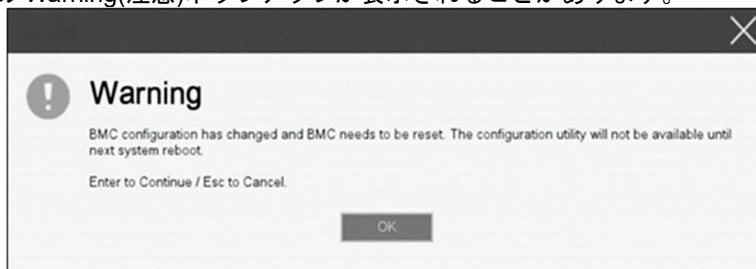
5) 全般の機能に関する注意事項

● システムユーティリティの「BMC Configuration Utility」の操作についての注意事項

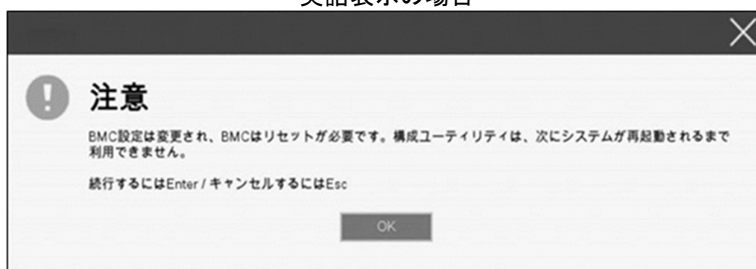
システムユーティリティの「BMC Configuration Utility」での操作において、以下の(1)のポップアップが表示された場合は(2)以降の手順を厳守してください。

注意事項に従った操作を実施されない場合、「Memory Initialization Start」のメッセージで POST 停止、あるいは装置に記録されている Serial Number、Product ID の消失が発生する場合があります。

- (1) システムユーティリティの「BMC Configuration Utility」において設定の変更を行うと、iLO の再起動を行うために、次の Warning(注意)ポップアップが表示されることがあります。



英語表示の場合

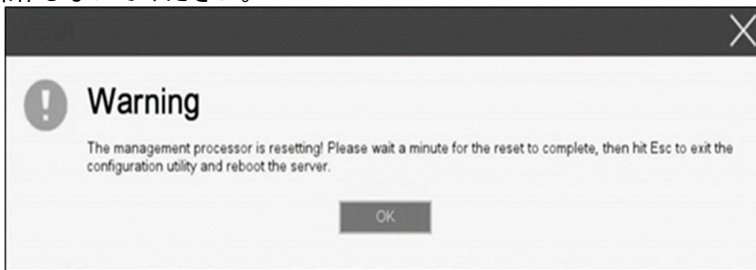


日本語表示の場合

- (2) 「OK」を押して進めます。

- (3) 次の Warning(注意)ポップアップが表示されます。

この Warning(注意)ポップアップが表示されている状態にて、必ず 1 分以上お待ちください。
その間、何も操作しないでください。



英語表示の場合



日本語表示の場合

- (4) 1 分以上経過後、装置前面のステータスランプが緑色で点灯していることを確認してください。

※ iLO が再起動中 : ステータスランプが緑色で点滅 (毎秒 1 回)

iLO の再起動が完了し正常動作 : ステータスランプが緑色で点灯

- (5) 再起動の完了が確認できたら、「OK」を押してください。

- (6) <ESC>キーを複数回押してシステムユーティリティの画面に戻ります。

- (7) システムユーティリティの「Reboot the System」を選択して再起動します。

● UPS 接続時の注意事項

UPS をシリアルポートに接続して使用する場合は、以下の設定を無効「Disabled」にしてください。

- (1) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port を「Disabled」に設定してください。
- (2) System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status を「Disabled」に設定してください。

● 冷却設定の変更について

以下のオプションを搭載する場合は、安定稼働のため本製品の冷却ファンの設定を「Increased Cooling」へ変更してください。

既に冷却ファンの設定を「Increased Cooling」または「Maximum Cooling」に設定されている場合は、本対策を行う必要はありません。

対象オプション

- ・ N8150-551 増設用 300GB HDD
- ・ N8150-552 増設用 600GB HDD
- ・ N8150-553 増設用 900GB HDD
- ・ N8150-602 増設用 900GB HDD
- ・ N8103-239 480GB OS ブート専用 SSD ボード (RAID 1)
- ・ N8154-151 2x2.5 型ドライブケージ(SAS/SATA, リア)
- ・ N8154-152 2x2.5 型ドライブケージ(U.3 NVMe x4/SAS/SATA)
- ・ N8154-153 2x2.5 型ドライブケージ(SAS/SATA)

◆設定手順

- (1) POST 中に<F9>キーを押下し、システムユーティリティを起動します。
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options を選択します。
- (3) Thermal Configuration メニューを「希望する設定」に変更します。
- (4) <F12>キーを押下し、設定を保存してシステムを再起動します。

※ 冷却ファン設定の変更に伴い、お客様の運用環境や負荷によっては冷却ファンの回転数が上がることがあります。

● N8154-147/148/152/155/156/157 増設ドライブケージ搭載時の注意事項

2022 年 12 月以降に本製品を単体で購入し、R120i-1M/2M に増設した場合は、ファームウェア・ドライバの更新が必要となる場合があります。詳細は下記をご参照ください。

ダウンロード先: <https://www.support.nec.co.jp/>

(「製品から探す: ハードウェア」 → 「型番・モデル名から探す」 → 「修正情報・ダウンロード」 → 以下のいずれかの型番で検索し、「増設ドライブケージ搭載時のファームウェア個別適用手順」を選択)

- ・ N8154-147
- ・ N8154-148
- ・ N8154-152
- ・ N8154-155
- ・ N8154-156
- ・ N8154-157

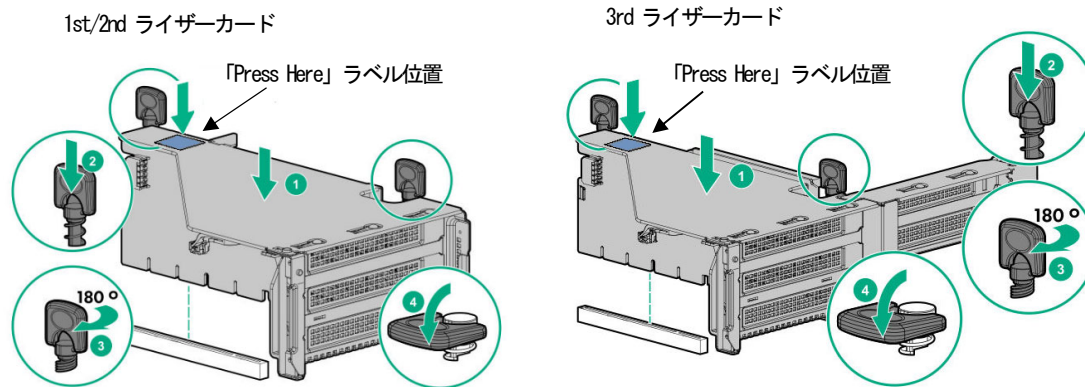
● ライザーカード取り付け時の注意事項

本装置に1st/2nd/3rdのライザーカードを取り付ける際は、コネクタ適合不良を回避するため、ライザーカードの端子部分とマザーボード上のスロット部分を合わせ、ライザーケース上面の「Press Here」ラベル部分を**必ず押して**、確実に差し込んでください。

このことによりコネクタ適合不良を回避することができます。

コネクタ適合不良が起こると、装置前面のStatus LEDが赤点滅します。

赤点滅した場合には本装置を電源OFFしてACケーブルを抜き、ライザーケース上面の「Press Here」ラベル部分を押ししてください。



● N8104-208 10/25GBASE 接続 LOM カード(SFP+ 2ch)ご使用時の注意事項

N8104-208 10/25GBASE 接続 LOM カード(SFP+ 2ch)にて Wake On LAN を使用しない場合は、必ず以下の手順に従って設定を変更してください。

本設定を行わない場合、Wake On LAN が機能する状態となります。

- (1) システムを起動します。
- (2) POST 中に<F9>キーを押下し、[システムユーティリティ (System Utilities)]に入ります。
- (3) [システム構成]に入り、Wake On LAN を設定する LAN コントローラを選択します。
本製品の場合、以下の名称となります。
 - ・ OCP Slot 10 Port 1: Intel(R) Ethernet Network Adapter E810-XXV-2 for OCP 3.0-xxxxxxxxxx
 - ・ OCP Slot 10 Port 2: Intel(R) Ethernet Network Adapter E810-XXV-2 for OCP 3.0-xxxxxxxxxx
- (4) [NIC 設定] > [Wake On LAN]の値を「無効」に設定します。
- (5) [F12:保存して終了]を選択後、[OK]または[はい - 変更の保存]を選択します。
[再起動]ボタンが表示されたら、<Enter>キーを押してシステムを再起動します。

N8104-208 10/25GBASE 接続 LOM カード(SFP+ 2ch)にて、Wake On LAN 機能を用いて本体装置の起動を行う場合、マジックパケットは本体装置をシャットダウンして、電源がオフの状態を受信するようにしてください。本体装置が稼働中にマジックパケットを受信した場合、その後本体装置がシャットダウンされ電源がオフに移行した後に、自動的に本体装置の電源がオンされてしまいます。

● N8103-184 SAS コントローラ ご使用時の注意事項

N8103-184 SAS コントローラを使用する場合、iLO Web インターフェイスの[System Information] > [Storage] > [Storage Controller]の Status が“不明(Unknown)”と表示される場合がありますが動作に影響はありません。

● EXPRESSBUILDER ヘルプについて

EXPRESSBUILDER のヘルプとメンテナンスガイドで記述が異なる場合は、メンテナンスガイドの記載を優先してください。

● サーバ診断カルテについて

サーバ診断カルテは、対象製品の稼働状況を記録し、月ごとに稼働状態の診断カルテを提供するサービスです。サーバ診断カルテの詳細は、Starter Pack 内の「サーバ診断カルテ セットアップガイド」を参照してください。

サーバ診断カルテの注意事項については下記の Web サイトをご確認ください。

■Windows 対応版

NEC サポートポータル (Windows 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010106809>

■VMware ESXi/ESX 対応版

NEC サポートポータル (VMware ESXi/ESX 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010107805>

● サーバ診断カルテの制限事項

- ・サーバ診断カルテを Windows Server 2022 環境で利用する場合以下の制限があります。

■Windows 対応版

サーバ診断カルテ(Windows 対応版)では、下記項目には対応していません。

- ① ソフトウェアログ情報
- ② ハードウェア構成情報の下記項目
 - ・ 製品情報
 - ・ 物理ディスク情報の累積稼働時間
 - ・ RAID 物理ディスク情報の累積稼働時間

※最新のサポート情報は下記の Web サイトをご確認ください。

NEC サポートポータル (Windows 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010106809>

■VMware ESXi/ESX 対応版

サーバ診断カルテ(VMware ESXi/ESX 上のゲスト OS 版対応版)では下記項目には対応していません。

- ① ソフトウェアログ情報
- ② 仮想マシン登録情報の下記項目
 - ・ 仮想マシン情報の累積稼働時間

※最新のサポート情報は下記の Web サイトをご確認ください。

NEC サポートポータル (VMware ESXi/ESX 対応版)

<https://www.support.nec.co.jp/View.aspx?&id=9010107805>

A) ファームウェア変更に伴う変更点

■ BIOS/Platform Configuration (RBSU)メニューの変更について

本製品の搭載ファームウェアの更新に伴い、メニューの一部に変更があります。
下記、変更点を記載します。

(1) Boot Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options」を選択すると、「Boot Options」メニューが表示されます。
追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Filter Non-bootable Drives (注 1)	[Auto] Enabled Disabled	「Enabled」に設定した場合、システムは起動できない固定ドライブの起動オプションを作成しません。「Auto」に設定した場合、ブートオプションの数が過剰になるとシステムは、予期しない副作用を避けるために、ブートできない固定ドライブのブートオプションを作成しません。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.00 以降にて利用できるパラメーターです。

(2) Power and Performance Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options」を選択すると、「Power and Performance Options」メニューが表示されます。
追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Minimum Processor Idle Power Core C-State	[C6 State] C3 State C6 Without C1E State (注 1) C1E State No C-states	このオプションは、「Workload Profile」が「Custom」に設定されている場合のみ設定できます。システムが使用するプロセッサの最小アイドル電力状態(C-ステート)を選択するには、このオプションを使用します。C-ステートが高いほど、そのアイドル状態の消費電力が低くなります。(プロセッサがサポートする最小電力アイドル状態はC6です)。
Energy Performance Preference (注 2)	[Disabled] Enabled	このオプションを使用して、エネルギーパフォーマンス優先を有効または無効にします。
Uncore Frequency Scaling	[Auto] Maximum Minimum Custom (注 3)	本オプションは、プロセッサの内部バス(アンコア)の周波数のスケーリングを制御します。本オプションを「Auto」に設定すると、プロセッサはワークロードに基づいて周波数を動的に変更できます。最大または最小の周波数に強制すると、レイテンシおよび消費電力の調整ができます。ユーザー入力によって最大周波数と最小周波数を変更するには、「Custom」を選択します。 (最小の設定が最大の設定を超えることはできません)
Uncore Frequency RAPL (注 5)	[Enabled] Disabled	実行平均電力制限(RAPL)バランサーを有効にするかどうかを制御します。このオプションを有効に設定すると、アンコア部分の電力配分が有効になります。
Maximum Uncore Frequency (注 4)	0-127 [24]	ユーザー入力の最大アンコア周波数(MHz) 本オプションは Uncore Frequency Scaling を「Custom」に設定したときのみ表示されます。
Minimum Uncore Frequency (注 4)	0-127 [8]	ユーザー入力の最小アンコア周波数(MHz) 本オプションは Uncore Frequency Scaling を「Custom」に設定したときのみ表示されます。
Disable Dynamic Loadline Switch (注 4)	Disable DLL Switch [Not Disable DLL Switch]	本オプションを有効または無効にすると、条件による電力やパフォーマンスに影響を与える可能性があります。DLLはP状態の動作に応じてEPBモードを切り替えます。
CPU C1 Auto Demotion (注 5)	Enabled [Disabled]	CPUが自動的にC1に降格できるようにします。
CPU C1 Auto Undemotion (注 5)	Enabled [Disabled]	CPUがC1から自動的に降格解除できるようにします。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.24 以降にて利用できるパラメーターです。

注 2: システム ROM バージョン 1.72 以降にて利用できるオプションです。

注 3: システム ROM バージョン 1.80 以降にて利用できるパラメータです。

注 4: システム ROM バージョン 1.80 以降にて利用できるオプションです。

注 5: システム ROM バージョン 2.54 以降にて利用できるオプションです。

(3) Advanced Performance Tuning Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options」を選択すると、「Advanced Performance Tuning Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Enhanced Processor Performance Profile	Conservative [Moderate] Aggressive	プロセッサパフォーマンス強化のプロファイルを選択します。
Snoop Response Hold Off	[0]-15	推奨されたデフォルト設定ではワークロードのパフォーマンスが低下する場合に、I/O サブシステムのスヌープ応答時間を調整するために設定します。 本オプションの設定値を増やした場合、スヌープ要求を保留できる時間が指数関数的に長くなります。

[]: 出荷時の設定

注 1: システム ROM バージョン 1.52 以降にて利用できるパラメーターです。

(4) Server Security メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security」を選択すると、「Server Security」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Microsoft(R) Secured-core Support	[Disabled] Enabled	Microsoft(R) Secured-core サポートの設定を行います。「Enabled」に設定すると、以下のオプションが自動的に変更され、「Enabled Cores per Processor」オプションがグレーアウトされ、設定できなくなります。 - Boot Mode: UEFI Mode - UEFI Optimized Boot: Enabled - TPM Mode Switch Operation: TPM 2.0 - TPM Visibility: Visible - Intel(R) TXT Support: Enabled - Intel(R) VT-d: Enabled

[]: 出荷時の設定

注 1: システム ROM バージョン 1.52 以降にて利用できるパラメーターです。

(a) Advanced Trusted Platform Module Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Trusted Platform Module Options > Advanced Trusted Platform Module Options」を選択すると、「Advanced Trusted Platform Module Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Omit Boot Device Event	[Disabled] Enabled	ブートデバイスイベント省略の記録を設定します。「Enabled」に設定すると、PCR ブート試行の測定が無効になり、PCR[4]での測定が記録されなくなります。

[]: 出荷時の設定

注 1: システム ROM バージョン 1.52 以降にて利用できるパラメーターです。

(5) Advanced Security Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options」を選択すると、「Advanced Security Options」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
UEFI Variable Access Firmware Control (注 1)	[Disabled] Enabled	オペレーティングシステムなど他のソフトウェアによる特定の UEFI 変数の書き込みを、システム BIOS で完全に制御できるように設定します。 「Disabled」が選択されている場合は、すべての UEFI 変数が書き込み可能です。「Enabled」が選択されている場合、システム BIOS 以外のソフトウェアによって重要な UEFI 変数に加えられる変更はすべてブロックされます。例えば、オペレーティングシステムが新しいブートオプションをブート順序の最上位に追加しようとする、実際にはブート順序の最下位に配置されます。注記: UEFI 変数アクセスのファームウェアコントロールが有効になっている場合、オペレーティングシステムの機能の一部が期待どおりに動作しないことがあります。新しいオペレーティングシステムのインストール中にエラーが発生する場合があります。

[]: 出荷時の設定

注 1: システム ROM バージョン 1.52 以降にて利用できるパラメーターです。

(6) Advanced PCIe Configuration メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration」を選択すると、「Advanced PCIe Configuration」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
PCIe Data Link Feature (注 1)	-	-
PCIe Hot-Plug Error Control (注 2)	[Hot-Plug Surprise] eDPC Firmware Control eDPC OS Control	本オプションは出荷時設定から変更しないでください。 プラットフォームの PCIe (NVMe) ホットプラグサポートを設定します。「Hot-Plug Surprise」を選択すると、プラットフォームはサプライズリムーバル時にエラーの発生を防止しようとします。拡張ダウンストリームポートコンテナメント(eDPC)をサポートしていない古いオペレーティングシステムの場合は、このオプションを選択する必要があります。「eDPC Firmware Control」を選択すると、プラットフォームファームウェアと OS が正しくネゴシエートし、すべてのホットプラグイベントをログに記録します。このオプションは現在、すべてのオペレーティングシステムでサポートされているわけではありません。「eDPC OS Control」を選択すると、ホットプラグイベントはオペレーティングシステムで処理され、プラットフォームは関与しません。このモードでは、イベントのログ記録はすべてオペレーティングシステムに限定されます。ホットプラグイベントとサプライズリムーバルイベントがプラットフォームで正しく処理されるようにするには、オペレーティングシステムに基づいて正しく設定することが重要です。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.24 以降にて利用できるオプションです。

注 2: システム ROM バージョン 1.52 以降にて利用できるオプションです。

(a) PCIe Data Link Feature メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Data Link Feature」を選択すると、「PCIe Data Link Feature」メニューが表示されます。

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
PCIe Slot XX Data Link Feature Exchange (注 1)	[Enabled] Disabled	Data Link Feature Capabilities (DLFCAP) レジスタでデータリンク機能ネゴシエーションを有効無効にします。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.24 以降にて利用できるオプションです。

■商標について

EXPRESSBUILDER、ESMPRO は日本電気株式会社の登録商標です。

Microsoft(R)、Windows(R)、Windows Server(R)、は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Intel(R)、Xeon(R) は米国 Intel Corporation の登録商標です。

Linux(R) は、Linus Torvalds 氏の米国およびその他の国における商標または登録商標です。

Red Hat(R)、Red Hat Enterprise Linux(R) は米国 Red Hat、Inc. の米国およびその他の国における商標または登録商標です。

VMware is a registered trademark or trademark of Broadcom in the United States and other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

その他、記載の会社名および商品名は各社の商標または登録商標です。

■本件に関するお問い合わせについて

本書の内容に不明点がありました場合は、下記ファーストコンタクトセンターまでお問い合わせください。

お問い合わせ先：ファーストコンタクトセンター TEL : 0120-5800-72 受付時間 : 9:00～12:00 13:00～17:00 月曜日～金曜日(祝日を除く) ※番号をお間違えにならないようお確かめのうえお問い合わせください。

Precautions for Using Express5800/R120i-1M, R120i-2M

Thank you for purchasing our products.

This document provides the precautions on the use of this product.

Please read through the instructions below and keep this document in a safe place for your future reference.

- 1) Introduction
- 2) Notice about the function of the System ROM
- 3) Notice about the function of the iLO5
- 4) Notice about the OS
- 5) Notice of the function in general
- A) The additional options by firmware update

1) Introduction

● About the manual of this product.

For Starter Pack, the user's guide and the other related documents of this product, please refer to Download on the following URL. Regarding Starter Pack, it is also provided as an optional product.

< <https://www.58support.nec.co.jp/global/download/> >

- > Document & Software
- > Rack
- > (Select your server model)

Please check latest information and versions on ESMPRO portal site before using NEC ESMPRO Manager, NEC ESMPRO ServerAgentService and Express Report Service / Express Report Service (HTTPS) / Express Report Service (MG).

< <https://www.58support.nec.co.jp/global/download/> >

- > ESMPRO

● About Starter Pack

Please see the following website to check the latest Starter Pack.

< <https://www.58support.nec.co.jp/global/download/> >

- > Document & Software
- > Rack
- > (Select your server model)

● About service and driver modules for VMware ESXi/ESX

Please see the following website to check the latest modules.

- (1) Agentless Management Service and iLO Channel Interface Driver

< <https://www.58support.nec.co.jp/global/download/> >

- > VMware

- (2) WBEM Provider and CLI tool

< <https://www.58support.nec.co.jp/global/download/> >

- > Utility

● Notice about service operation time of this product

The service operation hours of this product may require more hours than usual depending on the combination of the equipped firmware and driver.

2) Notice about the function of the System ROM

● Note for UEFI Boot Order Control

If the System ROM Version is 2.24, you cannot enable or disable new boot devices or save these settings in the UEFI Boot Order Control menu (*1). To change the priority of the device to boot from, please adjust the priority in the UEFI Boot Order menu (*2). Additionally, each time you navigate to the UEFI Boot Order menu or the UEFI Boot Order Control menu, a red circle (©) will appear in front of the "Changes Pending" string at the bottom of the screen. Press the F10 key as needed to save the settings.

(*1) BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control

(*2) BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order

● Precautions when using System default options

To restore the system settings to their default values, use the "Restore Default System Setting" menu.

When using the "Restore Default Manufacturing Settings" menu, not only will the BIOS/Platform Configuration (RBSU) settings be restored to their default values, but also the installed/mounted PCI cards (array configuration information for RAID controllers and iSCSI setting information for network cards) will be returned to their default values.

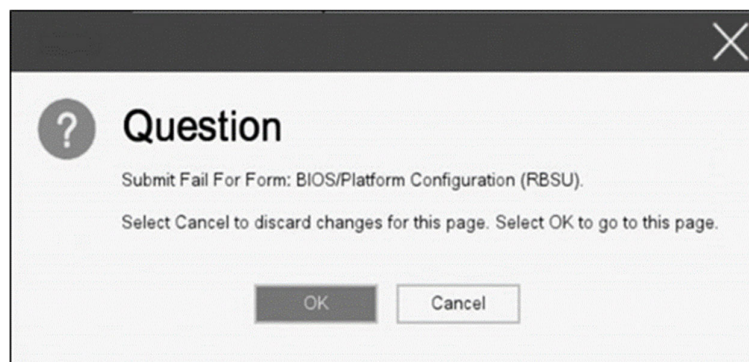
Therefore, if the OS is installed in the array configuration of the RAID controller, it will be necessary to reinstall the OS after the array is rebuilt.

Restore Default System Settings (Recommended)

Restore Default Manufacturing Settings (only for restoring the default values including PCI cards)

● Caution for the "Submit Fail For Form" Question pop-up

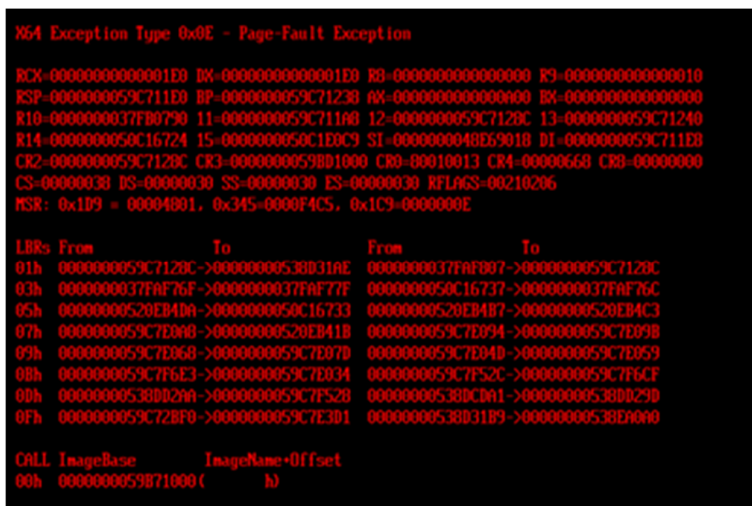
If you encounter the "Submit Fail For Form" Question pop-up while changing the configuration in the System Utilities, **discard the changes by pressing Cancel**. To apply the desired changes after that, reboot the server and re-enter the System Utilities. Selecting OK to continue the changes may cause some server settings such as Serial Number and Product ID to be lost.



● Caution for recovering from RSOD (Red Screen Of Death)

If you have changed the server configuration/settings or the system status, a Red Screen of Death (RSOD) screen appears in rare cases before starting up the OS. This may cause the server to become uncontrollable. However, the server may recover from the RSOD by turning off and then on the power again.

To recover from this condition, power off and then on the server again.
If the problem persists, contact your sales representative for maintenance.



● If Secure Boot fails, a red screen (RSOD: Red Screen Of Death) may be displayed

If Attempt Secure Boot (*) in RBSU is set to Enabled, and Secure Boot (signature verification) fails during boot, a red screen (RSOD) may be displayed before the OS starts, and you may no longer be able to operate this product.

(*) BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Attempt Secure Boot

If the RSOD is displayed, power the system OFF/ON, then resolve the cause of the Secure Boot failure (e.g., the boot loader/OS components are outdated and fail verification under the current Secure Boot policy), and then boot from the boot device.

As an example workaround, set Attempt Secure Boot to Disabled, update the OS (or the boot loader/recovery environment) to the latest version, then set Attempt Secure Boot back to Enabled and confirm that the OS starts successfully.

If the issue is not resolved, please contact the First Contact Center.

● How to recover stop POST by the message of "Memory Initialization Start"

If the server stops POST by a message of "Memory Initialization Start", recover them by setting to the default value by SW6 of the system maintenance switch.

Refer to "Chapter 1 - 7.4.3 Set the System Configuration Back to Default Values" of the maintenance guide.

● Note for Customers Using Intel(R) Xeon(R) Silver 4309Y or Gold 5315Y Processors

If the System ROM Version is earlier than 2.00 (03/06/2024) and equipped with either Intel(R) Xeon(R) Silver 4309Y or Gold 5315Y processor, the fans may operate at high speed.

This issue has been fixed in System ROM Version 2.00 (03/06/2024).

● Notes on Boot Order Policy options

If the version of your System ROM U46 is v1.64 (08/11/2022) or later, set the "Boot Order Policy" option (*) to "Reset After Failed Boot Attempt". This setting reboots the system if all boot devices in the "Boot Order" list fail to boot due to, for example, their time-consuming initialization. Rebooting the system may lead to a successful OS boot by rerunning the boot process.

The factory default setting for the "Boot Order Policy" option has been [Reset After Failed Boot Attempt] instead of [Retry Boot Order Indefinitely] since December 2022.

* Select BIOS/Platform Configuration (RBSU) > Boot Options > Boot Order Policy.

● Notes on the Server Configuration Lock (SCL)

- (1) Set SCL function to disabled and operate the system.
- (2) Set the password when the SCL function is enabled and keep the password in a safe place. If you lose your SCL password and it is locked by the SCL function (stopped before booting the OS), you will not be able to unlock it and you will not be able to boot the server OS again.

You will be charged for recovery / recovery to the bootable state.

If you lose your SCL password, there is no way to clear it.

- (3) When you will be requesting maintenance, it is necessary to disable the SCL function.
If you cannot be disabled the SCL function, **maintenance will be a charged one.**
- (4) Set "Halt on Server Configuration Lock failure detection." option to disabled and operate the system. If it was enabled, when the SCL function detects an unrecoverable condition and is locked (stopped before the OS boots), the system utility will not be able to start and the server configuration lock will never be disabled.

You will be charged for recovering to the bootable state.

Unrecoverable conditions of SCL function:

- When the server boot is locked by the SCL function due to change in the RBSU settings.
 - When the server boot is locked by the SCL function due to the update of firmware, and the original firmware version cannot be restored.
 - When the server boot is locked by the SCL function due to a failure of the DIMM or PCI option card
- (5) When System ROM v1.40 (04/28/2021), if the installed PCI option card is removed or fails, the SCL function suppresses booting, but the POST error message is not displayed and integrated management. No logs are recorded in the log (IML) either. When System ROM v1.52 (09/22/2021), POST error message is displayed and IML is recorded when suppressing boot.

● "IPMI Watchdog Timer Timeout" may be logged in the iLO event log (IEL)

When System ROM is v1.58 (01/13/2022) and the **IPMI Watchdog Timer** option is set to **Disabled** (factory setting), the following "IPMI Watchdog Timer Timeout" may be logged in the IEL:

iLO IPMI Watchdog Timer Timeout: Action: None, TimerUse: 0x44, TimerActions: 0x00.

Event Class: 0x23

Event Code : 0xB3

Recovery procedure:

This problem will be solved by exercising either of the recovery options (A or B) described below.

Recovery option A

1. Power off the server. Then disconnect the plug from the outlet.
2. Wait for 30 seconds. Then plug the server into the outlet again.

Recovery option B

In System Utilities, change the setting of the **IPMI Watchdog Timer** option two times as follows:

1. Power on the server.
2. During the POST, press the F9 key to start System Utilities.
3. In **System Configuration**, select **RBSU > System Options > Server Availability**. Then set the **IPMI Watchdog Timer** option to **Enabled**.
4. Press the F12 key, save the change, and then restart the system.
5. During the POST, press the F9 key to start System Utilities again.
6. In **System Configuration**, select **RBSU > System Options > Server Availability**. Then set the **IPMI Watchdog Timer** option to **Disabled**.
7. Press the F12 key, save the change, and then restart the system.

● About the System Utilities and One-Time Boot Menu display

- (4) In the PCIe Device Configuration menu of BIOS/Platform Configuration (RBSU) (*) and in One-Time Boot Menu, the name of a RAID controller may not be correctly displayed on the following conditions:

- For N8103-189, N8103-190, N8103-191, N8103-192, N8103-193, N8103-194, N8103-195, N8103-196, N8103-197, N8103-201, N8103-237, or N8103-238

The above problem occurs if both of the following conditions are met:

1. The version of the RAID controller firmware is v4.11 or higher, or v3.01.04.072 or higher.
2. The version of System ROM is lower than v1.64 (08/11/2022)

However, the problem does not affect a boot from the HDD/SSD managed by the RAID controller.

* Select BIOS/Platform Configuration (RBSU) > PCIe Device Configuration.

● Notes on TPM Visibility Help

"Platform Certificate Support" must be set to [Disabled] in order to change the "TPM Visibility" setting.

Although "Platform Certificate Support is not set to Enabled" is displayed in the help display (red) of "TPM Visibility" in the system utility, the correct message is "Platform Certificate Support is not set to Disabled".

RBSU > Server Security > Trusted Platform Module Options > Advanced Trusted Platform Module Options > TPM Visibility

RBSU > Server Security > Advanced Security Options > Platform Certificate Support

3) Notice about the function of the iLO5

● Caution about Reset iLO

Do NOT Reset iLO during the period from server boot start to the completion of OS boot. This period includes the execution of POST (Power On Self Test)

Do NOT Reset iLO while users are using the System Utilities.

Under such circumstances, restarting the iLO may cause unexpected result.

For example, while changing options of the System Utilities, Reset iLO may lead to loss of server settings such as Serial number and Product ID. If the iLO is reset during POST execution, the screen display of UUID and UUID logic in iLO Web Interface : [Information] > [Overview], may be corrupted. Please turn off and turn on the power this product.

iLO Resets which is subject to this caution

- Reset iLO via network such as iLO Web Interface
- Reset iLO via UID switch

* Refer to Caution for operating "BMC Configuration Utility" in the System Utilities below, for the cases where iLO is reset after changing the settings in "BMC Configuration Utility" in the System Utilities.

● Caution about iLO Downgrade Policy

In case that iLO License for Remote Management is installed, Do NOT set "Permanently disallow downgrades" in [Security] > [Access Settings] > [Update Service] > [Downgrade Policy] setting.

If the setting "Permanently disallow downgrades" is set, downgrade of any firmware cannot be done afterward. The setting of this "Permanently disallow downgrades" is permanent and irreversible, and users cannot change this setting from any iLO interfaces or any utilities.

This setting cannot be removed by setting "Set to factory defaults" and the setting "Permanently disallow downgrades" is kept unchanged.

● Caution about iLO security function



is always displayed in [Information] > [Security Dashboard] and in iLO Web Interface screen.

Depending on the setting of RBSU or iLO, the status of security may be displayed in red showing security is at Risk. Please set security settings appropriately in order to follow customer's security policy.

For the recommended settings, please review the iLO5 User's Guide.

For the settings of "Require Host Authentication", please refer to the other descriptions of **Caution for the case where the setting "Require Host Authentication" is enabled from iLO Web Interface**

The iLO security icon on the right upper portion of iLO Web Interface may be transparent even if "Overall Security Status" of [Security Dashboard] is "Risk".

"Overall Security Status" of [Security Dashboard] indicates the current security status.

● Caution for the case where the setting "Require Host Authentication" is enabled from iLO Web Interface (*).

(*) Set "Require Host Authentication" Enabled in "Security > Access setting > iLO"

When the setting described above is executed, the following symptoms are expected

- Many messages "Remote Insight/Integrated Lights-Out Unauthorized Login Attempts" are displayed in alert viewer.
- Error occurs, when Starter Pack (Standard Program package) is applied.

The following services and functions are not supported

- Report services for hardware faults in Express Report Service
- RAID Report Service
- Function to display Device information and configuration collected by iLO
- Function to collect event logs collected by iLO

● About iLO time setting

It is recommended that SNTP is set enabled at iLO Web Interface.
For the details of iLO SNTP setting, please refer to iLO5 User's Guide.

● About the corrupted screen display of UUID in iLO Web Interface

If the iLO is reset during POST execution, the display of UUID and UUID logic in iLO Web Interface : [Information] > [Overview] page may be corrupted.

When any corrupted texts are displayed, please turn off and on the system.

● Display of Network information on iLO Web Interface

The network bridge is configured, the information displayed (for each adapter) in [Physical Network Adapters] in [Network] of [Information] on iLO Web Interface may differ from the actual status on OS.

For the detail of the bridge information, please check the Property of each network adapter on OS.

● About Storage Information of iLO Web Interface

If you are using the iLO5 Firmware Version 3.00 or later

iLO5 may not retrieve Storage Information after server reboot.

In this case in the iLO Web Interface, under "System Information," clicking on the "Storage" tab displays the following:

"Failed to retrieve complete storage device information. Refresh the page in a few minutes."

If above the message is displayed on "storage" page in iLO Web Interface, please run the iLO reset.

● What to do when a RESTful API ERROR occurs

In the case that the RESTful API Error may occur during POST execution, the error will be recorded in the Integrated Management Log (IML), however, it can be fix by perform an iLO reset.

If the problem persists, please contact the First Contact Center.

● What to do when EXPRESSBUILDER or Smart Storage Administrator (SSA) cannot be started?

If you are using the iLO5 firmware lower than 2.60:

You may fail to start EXPRESSBUILDER on rare occasions, for example, by pressing the F10 key on the POST screen or by selecting **System Utilities > Embedded Applications**.

You may also fail to start Smart Storage Administrator (SSA) on rare occasions by selecting **System Utilities > System Configuration > RAID Controller > Launch Smart Storage Administrator (SSA)**.

In the above cases, reinstall the EXPRESSBUILDER.

The latest version of EXPRESSBUILDER for this product is available on the following website:

<https://www.support.nec.co.jp/>

(Search for "E8.10-" from "Search in NEC Support Portal")

Checking the content on the website, update EXPRESSBUILDER to version E8.10-009.01 or higher.

* The above measure does not affect the operation of the online version of SSA.

● What to do if you receive a corrupted alert about physical drive status changes

When you received the corrupted SNMP alert about physical drive status changed, confirm the location information of the same event at "Information" - "Integrated Management log" of iLO Web Interface.

e.g.:

Abnormal, physical drive status change detection, iLO SNMP Trap, mgr_ WIN-U6HHPNIIH1Q, uru-rhel83, 192.168.0.57, 2021/10/01

15:22:57, iLO, 0xc0000be6, "A physical drive status change has been detected. Current status is 3.

(Location: of 12 Controller: Slot 12)", "If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

● About status of Agentless Management Service(AMS) on iLO Web Interface.

When you received the corrupted SNMP alert about physical drive status changed, confirm the location information of the same event at "Information" - "Integrated Management log" of iLO Web Interface.

When status of Agentless Management Service(AMS) is "Unknown" or "Not available"(*) on iLO Web Interface, please reset iLO.

After about 10 minutes, please restart Agentless Management Service(AMS) by following procedures.

* Verifying AMS status

Please confirm the status from iLO Web Interface : [System Information] > [Summary] > [Subsystems and Devices] > "Agentless Management Service".

If the status of Agentless Management Service(AMS) is "Unknown" or "Not available", iLO can't collect some part of information of storage, network and iLO can't display those information correctly.

< Restarting AMS >

Procedure

· Windows

Navigate to the Windows Services page and restart AMS.

· Red Hat Enterprise Linux 7.x and 8.x

Enter the following command:

```
# systemctl restart smad
```

```
# systemctl restart amsd
```

· ESXi/ESX 7.0/8.0/9.0

Enter the following command:

```
# /etc/init.d/amsd restart
```

● About Java IRC session timeout message.

While Integrated Remote Console (Java IRC) is launching, the pop-up messages indicate the IRC session expired appear after that session has expired. At the same time, irrelevant popup appears too together.

When the following message in bottom layer of Java IRC window, ignore description in displayed pop-up message.

- "Sessions Closed due to Timeout or Unauthorized Access."

● Possible high-speed fan rotation and abnormal sound

If you are using the iLO5 firmware 2.90 or later

Restarting the server can on rare occasions rotate the fan at high speed and emit an abnormal sound.

If this state continues for more than seven minutes, restart the server again.

● SNMP Alert

If you are using the iLO5 firmware 3.00 or later

For NEC ESMPRO Manager, the Alert Viewer notifies you of a change in a physical-drive status when it is detected.

Depending on the status, the location information is displayed in either of the following two patterns:

1. (Location: Slot=(A);Port=(B);Box=(C);Bay=(D) Controller: <NULL>)

2. (Location: Port=(B);Box=(C);Bay=(D) Controller: Slot (A))

A: Controller location (slot number)

B: The port number of the physical drive

C: box number of the physical drive

D: The bay number of the physical drive

- **Caution about Using Cipher Suite for Intelligent Platform Management Interface (IPMI)**

iLO5 does not support IPMI Cipher suite 17. If you run the "ipmitool" utility version 1.8.18 with the interface specified as "lanplus" and cipher suite as "17" for an iLO5, the following error will be displayed.

Error in open session response message: no matching cipher suite
Error: Unable to establish IPMI v2 / RMCP+ session.

4) Notice about the OS

● Notice of Windows Server

If you have a processor with more than 32 cores (physical cores), the Performance tab of the System Information (Msinfo32.exe) tool and Task Manager in Windows Server 2016 and Windows Server 2019 will not display the correct number of processor sockets, cores, L1 and L2 cache sizes. Cache and L2 Cache sizes are not displayed correctly.

For more information, please refer to the following links

Windows Server 2016 Support Information

<<https://www.support.nec.co.jp/View.aspx?id=3140105448>>

Windows Server 2019 Support Information

<<https://www.support.nec.co.jp/View.aspx?id=3140106598>>

Use the iLO Web Interface or System Utilities to verify the correct CPU information.

● Note on using NEC ESMPRO Manager (Windows) and Express Report Service (MG)

Depending on the combination of iLO5 Firmware Version of this product with NEC ESMPRO Manager (Windows) and Express Report Service (MG) (Windows), it may be necessary to update NEC ESMPRO Manager (Windows) and iLO Receiving Information (ilo_en.mtb). Please refer to the end of this chapter to confirm/update to the latest version, if needed.

◆Phenomena regarding NEC ESMPRO Manager (Windows)

iLO5 Firmware Version	NEC ESMPRO Manager (Windows) Version	Phenomena
2.10 or higher	Lower than 6.25	- Configuration Tab - Server Status screen "SNMP Alert setting" will show error message "Failed to get SNMP Alert setting". - Remote Control Tab - iLO Information - Show IML or Save IML NEC ESMPRO Manager will fail to get IML information and Show IML or Save IML feature will not work. - AlertViewer New Alerts of hardware failure added with firmware update will be displayed as "Unknown" alert on AlertViewer.
	Lower than 6.47	AlertViewer New Alerts of hardware failure added with firmware update will be displayed as "Unknown" alert on AlertViewer, or they will not be displayed on AlertViewer.

◆Updating NEC ESMPRO Manager Ver 6 (Windows)

(1) Download the latest version of NEC ESMPRO Manager from the following website.

<https://www.58support.nec.co.jp/global/download/index.html>

- ESMPRO tab

- NEC ESMPRO Manager

(2) Update NEC ESMPRO Manager. For details, refer to Chapter 2 Installation in "NEC ESMPRO Manager Ver. 6 Installation Guide (Windows) [PDF]".

◆Phenomena regarding iLO Receiving Information (ilo_en.mtb)

* Intend for users of NEC Express Report Service (MG)

iLO5 Firmware Version	iLO Receiving Information Version	Phenomena
2.10 or higher	ilo_en.mtb Lower than 1.4.0	It is impossible to detect a failure of the hardware added along with the update of hardware and to issue an alert of this failure. * If iLO Receiving Information has been updated and NEC ESMPRO Manager has not been updated, it is impossible to detect the failure of the added hardware and issue the alert of the failure, as with the above.
	iml_en.mtb Lower than 1.5.0	
	* There are 2 kinds of iLO Receiving Information.	

◆Updating iLO Receiving Information

- (1) Download the latest version of iLO Receiving Information (ilo_en.mtb, iml_en.mtb) from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows) Receiving Information
 - iLO.zip
 - (2) Delete current Receiving Information from Express Report Service (MG) (Windows).
For details refer to "3.1.5 Setting for Receiving Information" or "3.2.4 Setting for Receiving Information" in "Express Report Service (MG) Installation Guide (Windows)".
 - (3) Set the latest version of Receiving Information downloaded in step (1) to Express Report Service (MG)
- * Download "Express Report Service (MG) Installation Guide (Windows)" from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows)

◆The steps of confirmation for iLO FW version

- Server Health Summary
Push the UID button on the server and check the version of the iLO Firmware on the console connected to the server.
(For the detail, refer to Server Health Summary in iLO5 user guide.)
- Remote
Check the version of the iLO Firmware on "Firmware & OS Software - Installed Firmware" by iLO Web Interface.

◆The steps of confirming version for NEC ESMPRO Manager (Windows)

- (1) Log in NEC ESMPRO Manager.
- (2) Click the "About NEC ESMPRO Manager" link at the top right of the screen.
- (3) Confirm the version information of NEC ESMPRO Manager.

◆The steps of confirming version for iLO Receiving Information (ilo_en.mtb, iml_en.mtb)

- Confirm the version of "iLO SNMP Trap" in "Setting for receiving information" screen.
- Regarding "Setting for receiving information" screen, refer to 3.1.5 Setting for Receiving Information or 3.2.4 Setting for Receiving Information in "Express Report Service (MG) Installation Guide (Windows)".

● Note on using VMware ESXi/ESX

1. In "BIOS/Platform Configuration (RBSU)", avoid setting the "PCIe Hot-Plug Error Control" option (*) to "eDPC Firmware Control", otherwise a PSOD (Purple Screen Of Death) may occur.

* Select BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Hot-Plug Error Control.
2. This caution is about the screen display of VMware vSphere : Monitor > Hardware > System Sensor > Sensor when the ESXi is booted.

(1) In case of non-redundant FAN Configuration, there are cases where the screen display of following sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, This "Warning (Yellow)" does not indicate hardware malfunction and there is no impact to the system operation.

- Cooling Unit 1 Fans
- (2) There are some cases where the screen display of following sensor Health (vCenter : Status) shows "?" after ESXi completes boot, this does not indicate hardware malfunction and there is no impact to the system operation.

- System Chassis 1 UID

●Events recorded in Windows Server environments with N8104-208

Using N8104-208 with Windows Server may cause the system event log to record events as described below. However, ignore the messages since the events do not cause any problem for the system operation.

Event ID: 89
Source: icea
Level: Error
Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
PROBLEM: An unknown error occurred when loading the DDP package. Entering Safe Mode.
ACTION: Restart the Adapter. If the problem persists, install the latest driver from "<http://www.intel.com/support/go/network/adapter/home.htm>".
* "x" depends on the system environment.

Event ID: 91
Source: icea
Level: Error
Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
PROBLEM: The DDP package signature is not valid and cannot be loaded. Entering Safe Mode.
ACTION: Install the latest driver from "<http://www.intel.com/support/go/network/adapter/home.htm>".
* "x" depends on the system environment.

Event ID: 1284
Source: icea
Level: Error
Intel(R) Ethernet Network Adapter E810-XXV-2 xxx
PROBLEM: DDP package failed.
Possible Solution: Update to latest base driver and DDP package.
* "x" depends on the system environment.

This issue has been fixed in firmware version 3.20 or later of the N8104-208.
Please apply Starter Pack Version S8.10-010.5 or later.

● Notes for using TPM in VMware ESXi/ESX

If your system has TPM kit (N8115-35) and is running VMware ESXi with System ROM Version 2.00 (02/02/2019) or later, TPM mode should be set to "TPM 2.0" (*1).

PSOD (Purple Screen Of Death) occasionally occurs when TPM Mode is set to "TPM 1.2".

(*1) The factory default setting is "TPM 2.0".

Check TPM Mode and change setting from the following menu.

Menu Location : System Utilities > System Configuration > RBSU > Server Security > Trusted Platform Module Options
Indicating : Current TPM Type
Settings : TPM Mode Switch Operation

● Change of RAID monitoring and reporting method

If VMware ESXi/ESX uses N8103-189/190/191/192/193/194/195/196/201/237/238 RAID controller and N8103-239 SSD Adapter for OS Boot, the RAID monitoring report will be changed to snmp trap reporting.

For details, please check the following website.

NEC Support Portal
http://www.58support.nec.co.jp/global/download/N8103-239/WBEM_uninstall_en.pdf

● Cautions on using Linux OS

Use the device name of LOM or optional NIC which the OS automatically recognizes. When adding a unique udev rule, do not change or fix the NIC device name based on the PCI address.

In addition, do not use the storage device name under /dev/disk/by-path/ that includes the PCI address.

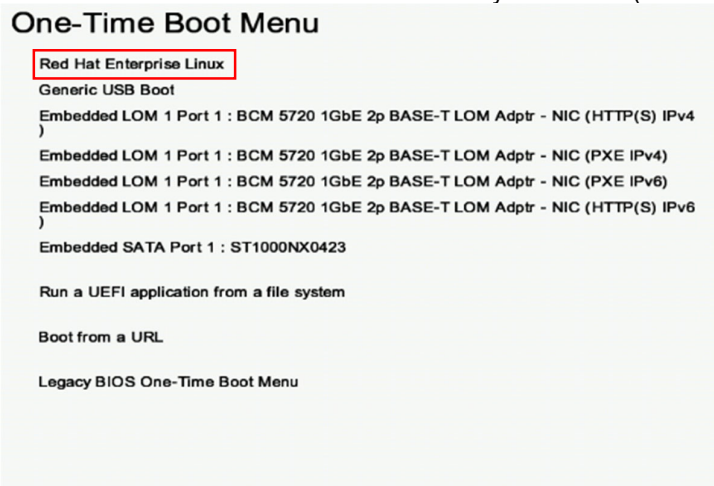
If operation using a device name based on the PCI address is required, do not add/remove the card to/from the PCI slot, or change the CPU configuration. If the PCI bus address information changes and the name of the PCI-connected device is affected, you may not be able to access the network or storage, and the system may not boot normally.

- **Cautions on using Red Hat Enterprise Linux 8.4 or later**

Select "OS Boot Manager" when booting OS from "One-Time Boot Menu".

Selecting an OS boot device such as HDD/SSD on the "One-Time Boot Menu" may cause RSOD (Red Screen Of Death).

One-Time Boot Menu



Red Hat Enterprise Linux

Generic USB Boot

Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (HTTP(S) IPv4)

Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (PXE IPv4)

Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (PXE IPv6)

Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (HTTP(S) IPv6)

Embedded SATA Port 1 : ST1000NX0423

Run a UEFI application from a file system

Boot from a URL

Legacy BIOS One-Time Boot Menu

One-Time Boot Screen

5) Notice of the function in general

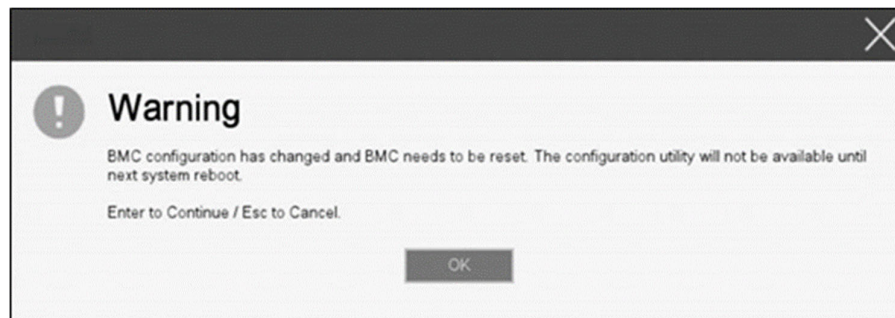
● Caution for operating BMC Configuration Utility in the System Utilities

If you execute POST or change the BMC configuration while rebooting the iLO, some server settings such as Serial Number and Product ID may be lost.

In addition, there is a possibility that it does not operate normally in the restart process immediately after.

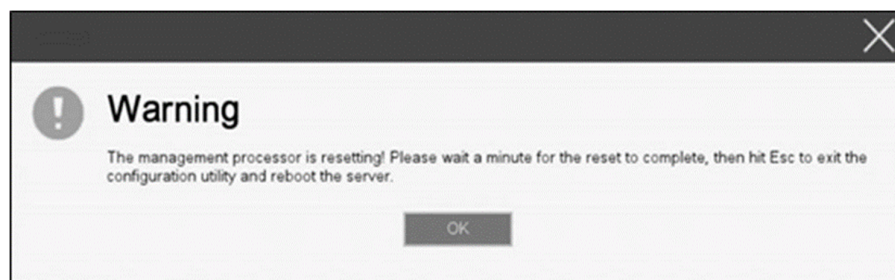
To avoid this trouble in rebooting the iLO, follow these steps:

- (1) In the System Utilities, changing the settings of BMC Configuration Utility may display the following pop-up before rebooting the iLO:



- (2) Press OK to proceed.

- (3) The iLO will start to reboot and then the following pop-up appears:



- (4) Leave this pop-up at least for one minute.

- (5) Confirm if the iLO reboot is completed.

The iLO is restarting : the Status LED flashes in green (once per second)

The iLO is operating normally through the restart completion : the Status LED lights in green.

- (6) If the confirmation succeeds, press OK to proceed.

- (7) Press the ESC key several times to return to the top screen of the System Utilities.

- (8) From the top screen, select Reboot the System to reboot the server.

● Note on using UPS

When connecting UPS to a serial port, set the items to "Disabled" in the following settings as below:

- (1) **System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port → [Disabled]**

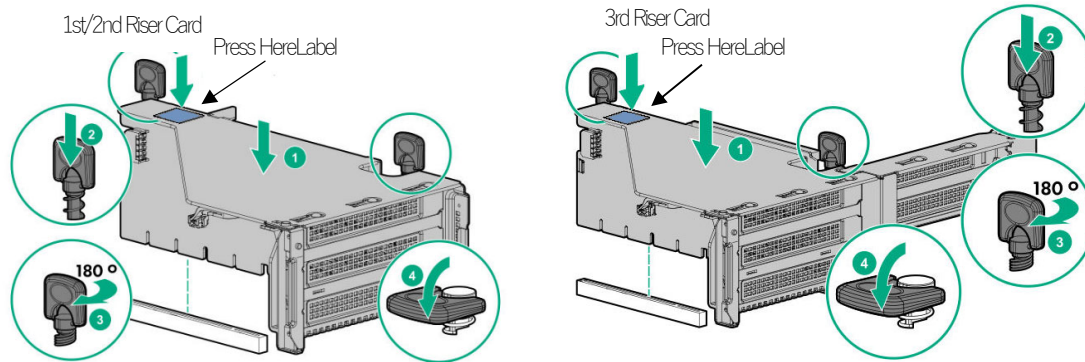
- (2) **System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status → [Disabled]**

●Precautions when installing the riser card

When installing the 1st, 2nd, or 3rd riser card in the server, be sure to align the riser card terminals with the slots on the motherboard and press the "Press Here" label on the top of the riser cage to insert the card securely in order to avoid connector mismatch.

If the connector mismatch occurs, the Status LED on the front of the unit will blink red.

If the Status LED is blinking red, turn off the server, unplug the AC cable, and press the "Press Here" label on the top of the riser cage.



●Changing the cooling setting

This topic pertains to the following Options:

N8150-551 300GB 15K Hot Plug 2.5-inch SAS HDD
N8150-552 600GB 15K Hot Plug 2.5-inch SAS HDD
N8150-553 900GB 15K Hot Plug 2.5-inch SAS HDD
N8150-602 900GB 15K Hot Plug 2.5-inch SAS HDD
N8154-151 2x2.5-inch Hot Plug Drive Cage Kit(SAS/SATA, Rear)
N8154-152 2x2.5-inch Hot Plug Drive Cage Kit(SAS/SATA, Rear)
N8154-153 2x2.5-inch Hot Plug Drive Cage Kit(SAS/SATA)

If your HDD is any of the above, but its current cooling fan setting is **Increased Cooling** or **Maximum Cooling**, leave it as it is (i.e., no need to change the setting). With neither of the two specified, for the HDD's stable operation, please change the setting to **Increased Cooling** as follows:

◆Procedure for changing the setting

- (1) Power on the server. During the POST, press the F9 key to start **System Utilities**.
- (2) Select **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Configuration**.
- (3) Change the setting to **Increased Cooling**.
- (4) Press the F12 key, save the change, and then restart the system.

Note:

Changing the cooling fan setting may increase the cooling fan speed, which depends on the operating environment for and the load on the system.

● N8104-208 Dual Port 10/25GBASE SFP+ LOM Card, notes on using

If the "Wake On LAN" feature is not required on the N8104-208 Dual Port 10/25GBASE SFP+ LOM Card, follow the below procedure to disable the feature.

- (1) Start the system.
- (2) Press the F9 key when the POST screen is display it to access "System Utility".
- (3) From the "System Configuration", select the LAN controller which the Wake On LAN setting is going to be configured.
For the R120i-1M server, the name of the NIC devices are as follows.
 - OCP Slot 10 Port 1 : Intel(R) Ethernet Network Adapter E810-XXV-2 for OCP 3.0 - xxxxxxxxxxxx
 - OCP Slot 10 Port 2 : Intel(R) Ethernet Network Adapter E810-XXV-2 for OCP 3.0 - xxxxxxxxxxxx
- (4) Select "NIC Configuration", set the "Wake On LAN" to "Disabled".
- (5) Press "F12: Save and Exit", and then select "OK" or "Yes - Save Changes".
When the "Reboot" button is display it, press enter key to restart the system.

When the system is powered on by "Wake On LAN" feature of the N8104-208 Dual Port 10/25GBASE SFP+ LOM Card, Magic packets should be received while the system is power off.

If the system receives a magic packet while the system is power on, the system will automatically power on after next power off.

● Notes of using SAS controller (N8103-184)

When using N8103-184, "Status" of iLO Web Interface [System Information] > [Storage] > [Storage Controller] might be displayed as "Unknown", but it does not affect server operation and SAS Controller operation.

● Note on using N8103-239 480GB SSD Adapter for OS Boot (RAID 1)

If you use N8103-239 480GB SSD Adapter for OS Boot (RAID 1), please change following setting as below.

- (1) Power on the server. During the POST, press the F9 key to start System Utilities.
- (2) Please set the following settings to "Increased Cooling".

System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Configuration

- (3) Press the F10 key to save the configuration.
- (4) Restart the server.

A) The additional options by firmware update

■ About changing the BIOS/Platform Configuration (RBSU) menu

Some options are added or changed by firmware update of this product.
The additional options are listed below.

(1) Boot Optionsメニュー

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options** from the System Utilities, the **Boot Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Filter Non-bootable Drives *1	[Auto] Enabled Disabled	When "Enabled", the system will not create boot options for fixed drives that are not bootable. When "Auto", the number of boot options becomes excessive, the system will not create boot options for fixed drives that are not bootable to avoid unintended side effects.

[]: Default setting

*1: an option usable with System ROM Version 2.00 or later.

(2) Power and Performance Options Menu

In **System Utilities**, selecting **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options** displays the **Power and Performance Options** menu.

Its additional options are described in the following table:

Option	Parameter	Description
Energy Performance Preference *1	[Disabled] Enabled	Use this option to enable/disable Energy Performance Preference.
Uncore Frequency Scaling	[Auto] Maximum Minimum Custom(*2)	This option controls the frequency scaling of the processor's internal busses (the uncore.) Setting this option to "Auto" enables the processor to dynamically change frequencies based on workload. Forcing to the maximum or minimum frequency enables tuning for latency or power consumption. Select "custom" to change the maximum and minimum frequency by the user input (the minimum can't be more than the maximum).
Uncore Frequency RAPL *4	[Enabled] Disabled	This option controls the Running Average Power Limit (RAPL) balancer is enabled or not. Setting this option to Enabled, it activates the uncore power budgeting.
Maximum Uncore Frequency *3	0-127 [24]	User input uncore frequency maximum(MHz). This option is displayed only when Uncore Frequency Scaling is set to Custom .
Minimum Uncore Frequency *3	0-127 [8]	User input uncore frequency minimum(MHz). This option is displayed only when Uncore Frequency Scaling is set to Custom .
Disable Dynamic Loadline Switch *3	Disable DLL Switch [Not Disable DLL Switch]	Enabling/Disabling the switch could affect the power and performance by condition. DLL (Dynamic Loadline) will switch EPB(Energy/Performance Bias) mode depending on the P-state behavior.
CPU C1 Auto Demotion *4	Enabled [Disabled]	Allows CPU to automatically demote to C1. Takes effect after reboot.
CPU C1 Auto Undemotion *4	Enabled [Disabled]	Allows CPU to automatically undemotion from C1. Takes effect after reboot.

[]: Default setting

*1: an option usable with System ROM Version 1.72 or later.

*2: a parameter usable with System ROM Version 1.80 or later.

*3: an option usable with System ROM Version 1.80 or later.

*4: an option usable with System ROM Version 2.54 or later.

(3) Advanced Performance Tuning Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options** from the System Utilities, the **Advanced Performance Tuning Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Enhanced Processor Performance Profile *1	Conservative [Moderate] Aggressive	Use this option to select the profile of Enhanced Processor Performance.
Snoop Response Hold Off *1	[0]-15	Allows the ability to tune the snoop response time of the I/O subsystem in the rare case that a workload's performance is hindered by the recommended default setting. Increasing the value of this setting exponentially increases the amount of time that snoop request can be held off.

[]: Default setting

*1: an option usable with System ROM Version 1.52 or later.

(4) Server Security Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Server Security** from the System Utilities, the **Server Security** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Microsoft(R) Secured-core Support *1	[Disabled] Enabled	Use this option to configure the server for Microsoft(R) Secured-core Support. When set to "Enabled", the following settings will be enabled and "Enabled Cores per Processor" option will be grayed out and cannot be set. - Boot Mode: UEFI Mode - UEFI Optimized Boot: Enabled - TPM Mode Switch Operation: TPM 2.0 - TPM Visibility: Visible - Intel(R) TXT Support: Enabled - Intel(R) VT-d: Enabled

[]: Default setting

*1: an option usable with System ROM Version 1.52 or later.

(a) Advanced Trusted Platform Module Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server security > Trusted Platform Module Options > Advanced Trusted Platform Module Options** from the System Utilities, the **Advanced Trusted Platform Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
Omit Boot Device Event *1	[Disabled] Enabled	Use this option to record Omit Boot Device Event. If enabled, PCR Boot Attempt Measurements will be disabled and measurement in PCR[4] will not be recorded.

[]: Default setting

*1: an option usable with System ROM Version 1.52 or later.

(5) Advanced Security Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options** from the System Utilities, the **Advanced Security Options** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
UEFI Variable Access Firmware Control *1	[Disabled] Enabled	Use this option to allow the system BIOS to completely control certain UEFI variables from being written to by other software such as an OS. When Disabled is selected, all UEFI variables are writable. When Enabled is selected, all changes made by software other than the system BIOS to critical UEFI variables will be blocked. For instance, new boot options the OS attempt to add to the top of BootOrder will actually be placed at the bottom of the Boot Order. Note: When UEFI Variable Access Firmware Control is Enabled, some OS functionality may not work as expected. Errors may occur while installing a new OS.

[]: Default setting

*1: an option usable with System ROM Version 1.52 or later.

(6) Advanced PCIe Configuration Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration** from the System Utilities, the **Advanced PCIe Configuration** menu appears.

For details about the additional options, see the table below.

Option	Parameter	Description
PCIe Hot-Plug Error Control *1	[Hot-Plug Surprise] eDPC Firmware Control eDPC OS Control	For this option, do not change the setting from the factory shipped setting unless otherwise specified. Use this option to select PCIe (NVMe) Hot-Plug support for the platform. When Hot-Plug Surprise is selected, the platform will attempt to protect the platform from experiencing an error on a surprise removal event. This option should be selected for older OS that do not support Enhanced Downstream Port Containment (eDPC). When eDPC Firmware Control is selected, the platform firmware and OS will properly negotiate and log all hot-plug events. This option is currently not supported by all OS. When eDPC OS Control is selected hot-plug events are handled by the OS with no involvement by the platform. All logging of events in this mode will be limited to the OS only. It is important that this option be set properly based on the OS to ensure hot-plug events and surprise removal events are handled properly by the platform. Please consult OS documentation for additional details.

[]: Default setting

*1: an option usable with System ROM Version 1.52 or later.

■ For Inquiries Regarding this Matter

If you have any questions on the contents of this document, please contact the dealer where you purchased the product or our sales representative.