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。誠におそれ入りますが、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

● 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 以上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「Agentless Management Service および iLO Channel Interface Driver(VMware ESXi 7.0版)」を適用してください)
(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 7.0版)」を適用してください)
(3) VMware ESXi 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「デバイスドライバー覧」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

● 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なお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などの設定情報を消失することがあります。

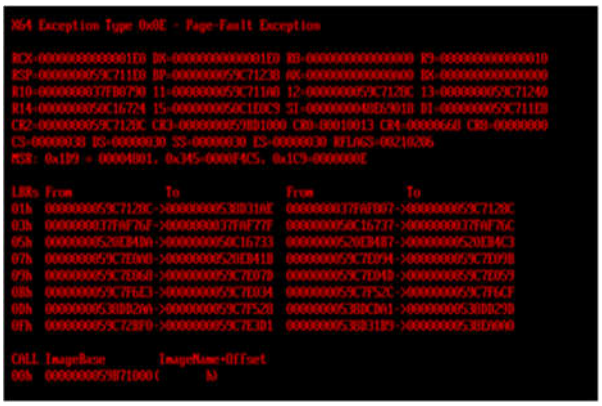
英語表示の場合

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、本製品の操作が出来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OFF/ON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OFF/ON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

● 「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。

● 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)されてしまうと、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 v1.40 (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、インテグレーテッ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 v1.52 (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 v1.58 (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) 装置の電源を切り、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再起動する。

● **システムユーティリティおよびワンタイムブートメニューの表示について**

RAIDコントローラ(N8103-189、N8103-190、N8103-191、N8103-192、N8103-193、N8103-194、N8103-195、N8103-196、N8103-197、N8103-201、N8103-237、N8103-238)のファームウェアバージョンがv4.11、またはv3.01.04.072の場合、ワンタ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。

(*)RBSU > PCIe Device Configuration

● **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) iLO 5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 (Power On Self Test)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などの設定情報を消失することがあります。また、POST (Power On Self Test)実行中にiLOの再起動を行うと、iLO Webインターフェース：[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インターフェー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ー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インターフェースの[Information] - [Security Dashboard]およびiLO Webインターフェース画面の右上部に 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、iLO 5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インターフェースから、[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”全体セキュリティーステータス”が『リスク』であっても、iLO Webインターフェース画面の右上部の”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”全体セキュリティーステータス”が現在のセキュリティ状態を示します。

● **iLOの時刻設定について**

iLOの時刻設定は、iLO WebインターフェースにてSNTPの設定を行い、ご使用いただくことを推奨します。
iLOのSNTPの設定方法については、iLO 5ユーザーズガイドを参照してください。

● **iLO Webインターフェースから、[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**

(※) [Security] – [Access Setting] – [iLO]にある[ホスト認証が必要/Require Host Authentication]を『有効』に設定する。

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頂けません。
- 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インターフェースのUUID不正値表示について**

POST (Power On Self Test)実行中にiLOの再起動を行うと、iLO Webインターフェースの[Information] – [Overview]ページのUUID、UUID(論理)の値が稀に不正な表示となることがあります。
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。

● **ネットワークブリッジ構成時のiLO Webインターフェー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インターフェースの[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上のネッワークアダプタのプロパティにてご確認ください。

● **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。
問題が解決しない場合は、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。

● **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以上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トラップ通知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トラップ通知において、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、iLO5 webインターフェースの[情報]-[インテグレーテッ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: ot 12 Controller: Slot 12)","If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

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

iLO Webインターフェースの[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インターフェースの[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
```

○ ESXi6.5/6.7の場合
以下のコマンドを実行します。

```
# /etc/init.d/amsd.sh restart
```
もしくは
```
# /etc/init.d/ams.sh restart
```

※ お使いのAMSバージョンによりコマンドが異なります。

○ ESXi7.0の場合
以下のコマンドを実行します。

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

● iLO5 Ver2.65以降の注意点

iLOwebインターフェースの「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=#I:Box=# ※#は接続先により番号が変わります。

不正時) Slot=#:Port=?I: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。

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

● **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/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 : 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。

● **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 iLO 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 以上	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 以上	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.mtd)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.mtd 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

◆iLO 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 iLO Firmware のバージョンを確認します(Server Health Summary の詳細は iLO 5 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、ブラウザーから 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」が「iLO SNMP Trap」のバージョンを確認します。

● VMware ESXi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 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 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 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" 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

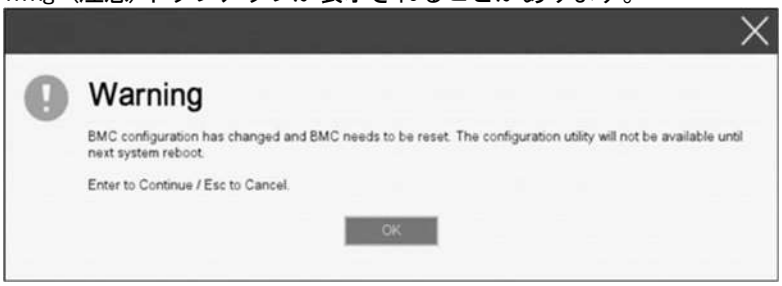
(10) "chroot"コマンドを終了後、レスキューモードを終了してシステムを再起動し、OSが起動できることを確認します。
実行例: bash-4.4# exit → chroot終了
sh-4.4# exit → レスキューモード終了

5) 全般の機能に関わる注意事項

● **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。

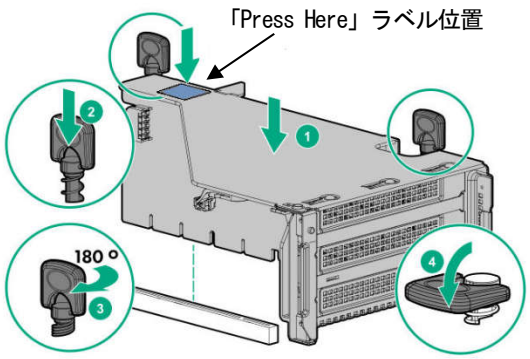
(1) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port を「Disabled」に設定してください。
(2) System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status を「Disabled」に設定してください。

● **ライザーカード取り付け時の注意事項**

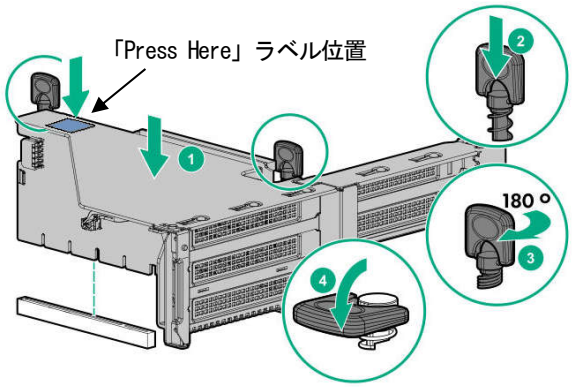
本装置に1st/2nd/3rdのライザーカードを取り付ける際は、コネクタ勘合不良を回避するため、ライザーカードの端子部分とマザーボード上のスロット部分を合わせ、ライザーケージ上面の「Press Here」ラベル部分を**必ず押して、**確実に差し込んでください。
このことによりコネクタ勘合不良を回避することができます。

コネクタ勘合不良が起こると、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、ライザーケージ上面の「Press Here」ラベル部分を押してください。

1st/2nd ライザーカード



3rd ライザーカード



● **増設ドライブケージ(N8154-151/152/153) ご使用時の注意事項**

増設ドライブケージ(N8154-151/152/153)をリアドライブケージとして使用する場合は、安定動作に必要な冷却を行うため、以下の設定を「Increased Cooling」にしてください。

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

● **N8154-149 2x2.5型ドライブケージ(U.2 NVMe x4) ご使用時の注意事項(2021年12月末出荷開始予定)**

(1) N8154-149(2x2.5 型ドライブケージ(U.2 NVMe x4))を増設する際は、StarterPack(S8.10-010.01)以降を適用した環境でご使用ください。

(2) VMware ESXi7.0 U2 または、ESXi7.0 U3 の OS 環境において、NVMe SSD を Hot-Add にて追加(増設)する際、操作が正常に完了しない事象が発生することがあります。
また、まれに PSOD(Purple Screen of Death)が発生することがあります。
この事象を回避するため、NVMe SSD を増設する際は装置の電源をオフしてから作業を実施してください。
※Hot-Swap(交換)については、問題ございません。

● **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 - xx:xx:xx:xx:xx:xx
・OCP Slot 10 Port 2 : Intel(R) Ethernet Network Adapter E810-XXV-2 for OCP 3.0 - xx:xx:xx:xx:xx:xx
(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、電源がオフの状態で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インターフェースの[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おりません。
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 対応版
サーバ診断カルテ(VMWare ESXi 上のゲスト OS 版対応版)では、下記項目には対応しておりません。
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 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。

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。

(1) 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。

項目	パラメーター	説明
Enhanced Processor Performance Profile	Conservative [Moderate] Aggressive	プロセッサー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 Version 1.52以降にて利用できるオプションです。

(2) 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。

項目	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 Version 1.52 以降にて利用できるオプションです。

(3) 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。

項目	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 Version 1.52 以降にて利用できるオプションです。

(4) 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。

項目	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と、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 Version 2.54以降にて利用できるオプションです。

(5) 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 Devices Configuration > Advanced PCIe Configuration」を選択すると、「Advanced PCIe Configuration」メニューが表示されます。
追加のメニューについて、次の表を参照してください。

項目	パラメーター	説明
PCIe Hot-Plug Error Control	[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インメント(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 Version 1.52以降にて利用できるオプションです。

■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。

NEC

2022年 6月　第5版

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

● 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

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 hour 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

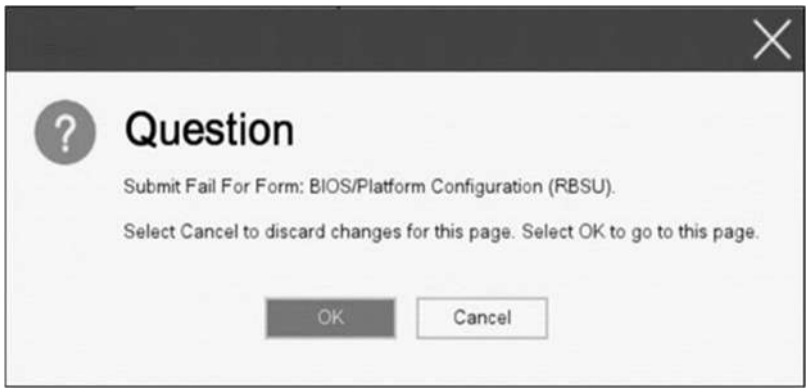
● Precautions when using System default options

To restore the system settings to their default values, use the "**Restore Default System Settings**" menu.
When using the "Restore Default Manufacturing Settings" menu, not only will the BIOS/Platform Configuration (RBSU) settings be restore 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

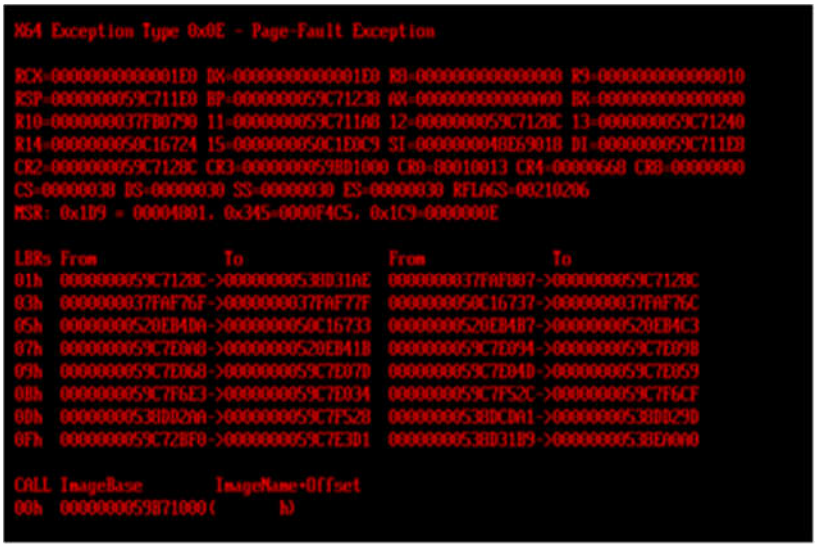
If you encounter the "Submit Fail For Form" Question pop-up while changing the configuration in the System Utilities, **discard the changes by pressing Cancel**. To apply the desired changes after that, reboot the server and re-enter the System Utilities. Selecting OK to continue the changes may cause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



● Caution for recovering from a Red Screen of Death (RSOD) screen

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.



● 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 - 7.43 Set the System Configuration Back to Default Values” of the maintenance guide.

● 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.

● **Notes on TPM Visibility Help**

"Platform Certificate Support" must be set to [Disabled] in order to change the "TPM Visibility" setting.
Although the "Platform Certificate Support is not been set as Enabled" message is displayed (in red) in the help display of "TPM Visibility" in the system utility, the correct message is "Platform Certificate Support is not been set as Disabled".

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

● **One-Time Boot Menu display**

RAID controller (N8103-190, N8103-191, N8103-193, N8103-194, N8103-238) firmware version 4.11 or 3.01.04.072, the RAID controller name may not be displayed correctly in One-Time Boot Menu. This problem only displays the RAID controller name, and does not impact the boot.

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 Setting] - [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 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.

● 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 performe 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 todo when corruption of SNMP alert about the physical drive status changed is recived?

When you recived the corrupted SNMP alert about physical drive status changed, confirm the location information of the same event at "Information" - "Integarated Management log" of iLO5 Web interface.

e.g.:
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: ot 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 recived the corrupted SNMP alert about physical drive status changed,confirm the location information of the same event at “Information” - “Integarated Management log” of iLO5 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
```

・ESXi6.5/6.7
Enter the following command:

```
# /etc/init.d/amsd.sh restart
or
# /etc/init.d/ams.sh restart
```

* Command depends on the version of AMS you are using

・ESXi7.0
Enter the following command:

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

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 iLO 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)

iLO 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)

iLO firmware version	iLO Receiving Information Version	Phenomena
2.10 or higher	ilo_en.mtb Lower than 1.4.0 iml_en.mtb Lower than 1.5.0 * There are 2 kinds of iLO Receiving Information.	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.

◆Updating iLO Receiving Information

(1) Download the latest version of iLO Receiving Information (ilo_en.mtb, iml_en.mtd) 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.mtd)
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)".

● Caution about VMware ESXi

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.

● Notes for using TPM in VMware ESXi

If your system has TPM kit (N8115-35) and OS is VMware ESXi with the, should be used "TPM 2.0" in TPM Mode.(*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

● 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.

● Change of RAID monitoring and reporting method

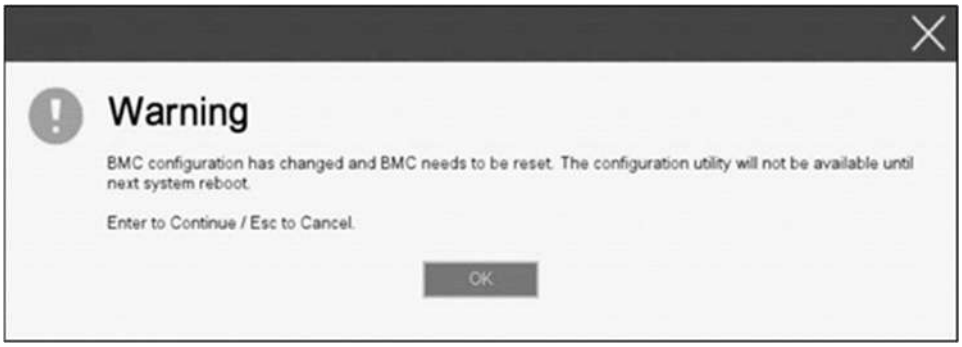
If VMware ESXi uses N8103-189/190/191/192/193/194/195/196/201/237/238 RAID controller and N8103-239 SSD Adapter for OS Boot, the RAID monitoring report will be changed to snmp trap reporting.
For details, please check the following website.
NEC Support Portal
http://www.58support.nec.co.jp/global/download/N8103-239/WBEM_uninstall_en.pdf

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

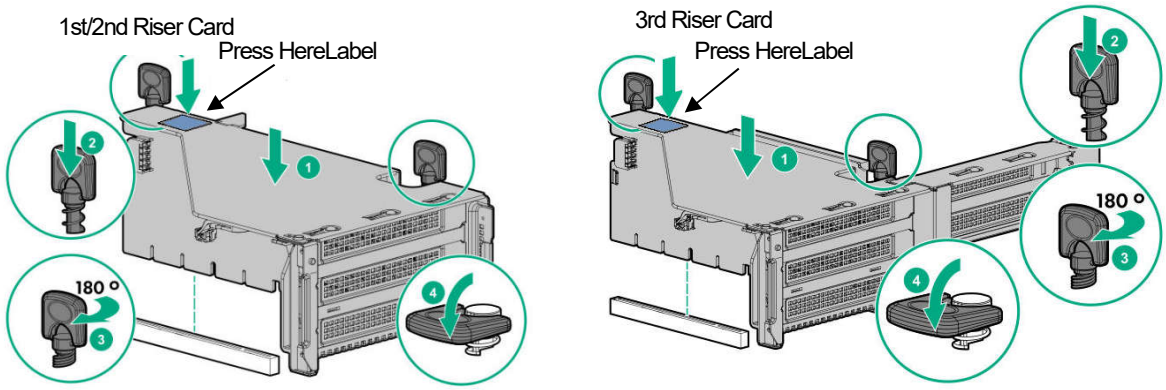
・When connecting UPS to a serial port, set the items to “Disabled” in the following settings as below:
(1) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port → [Disabled]

(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.



● Precautions for using the expansion drive cage (N8154-151/152/153)

When using the expansion drive cage (N8154-151/152/153) as a rear drive cage, please set the following settings to "Increased Cooling" in order to provide the necessary cooling for stable operation.

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

● Notes for N8154-149 2x2.5-inch Hot Plug Drive Cage Kit(U.2 NVMe x4) (Scheduled to start shipping at the end of December 2021)

(1) When installing N8154-149 (2x2.5-inch Hot Plug Drive Cage Kit(U.2 NVMe x4)), Please use in an environment that Starter Pack (S8.10-010.01) or later is applied.

(2) In the OS environment of VMware ESXi7.0 U2 or ESXi7.0 U3, when adding (expanding) NVMe SSD with Hot-Add, the operation may not be completed normally.
In rare cases, PSOD (Purple Screen of Death) may occur.
To avoid this event, turn off the power of the device before adding NVMe SSD.
There is no problem with Hot-Swap (replacement).

● 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 during the startup process to access "System Utility".
(3) Enter the "System Configuration", select the LAN controller to set Wake On LAN.
In the case of this product, it is the following name.
- OCP Slot 10 Port 1 : Intel(R) Ethernet Network Adapter E810-XXV-2 for COP 3.0 - xx:xx:xx:xx:xx:xx
- OCP Slot 10 Port 2 : Intel(R) Ethernet Network Adapter E810-XXV-2 for COP 3.0 - xx:xx:xx:xx:xx:xx

(4) Select "NIC Configuration", set the "Wake On LAN" to "Disabled".
(5) Select "F12:Save and Exit", and select "OK" or "Yes - Save Changes".
When the "Reboot" button appears, press enter 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] is might display to “Unknown”, but it does not affect server operation and SAS Controller operation.

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) 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	Conservative [Moderate] Aggressive	Use this option to select the profile of Enhanced Processor Performance.
Snoop Response Hold Off	[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.

(2) 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	[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.

(3) 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	[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.

(4) 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	[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.

(5) 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	[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.

NEC
Jun 2022 5th Edition

* CBZ-049000-001-04 *