

Express5800/R120h-1M (3rd-Gen), R120h-2M (3rd-Gen)

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
- 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。

R120h-1M (3rd-Gen) : 3170102353

R120h-2M (3rd-Gen) : 3170102354

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。

本製品に搭載する CPU の型番が、N8101-1519A など末尾が A または B であればバージョン S8.10-006.06 以降、N8101-1723C など末尾が C または D であればバージョン S8.10-007.01 以降を適用してください。

また、[2022 年販売モデル] は S8.10-010.04 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、「S8.10-006」あるいは「S8.10-007」「S8.10-010」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 6.x または 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 6.x 版 (x=5 または 7), 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「デバイスドライバー一覧」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。

● **Linux のサポートについて**

RHEL のサポート状況については、以下の Web サイトをご確認いただくか、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。

NEC Linux サービスセット対応モデル

<https://jpn.nec.com/linux/linux-os/ss/model.html>

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 3.34 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。

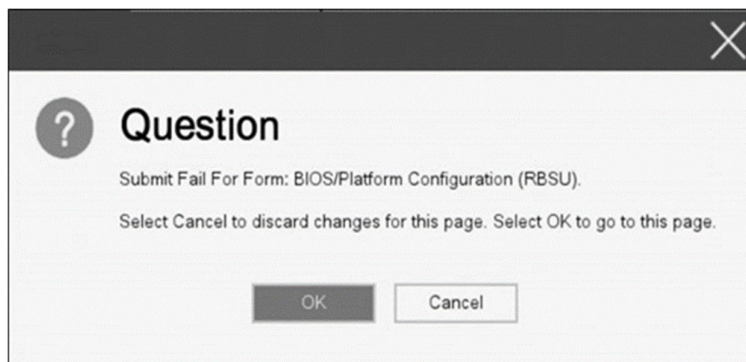
(*1) BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control

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

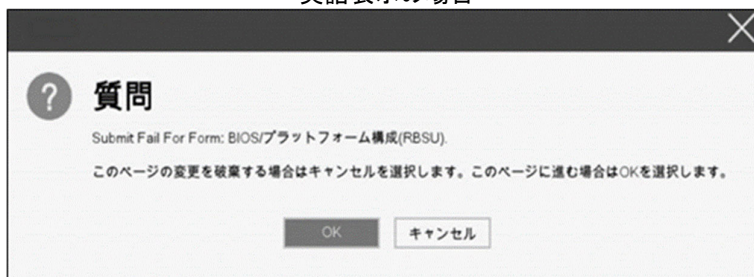
● Submit Fail For Form の Question(質問) ポップアップ表示についての注意事項

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

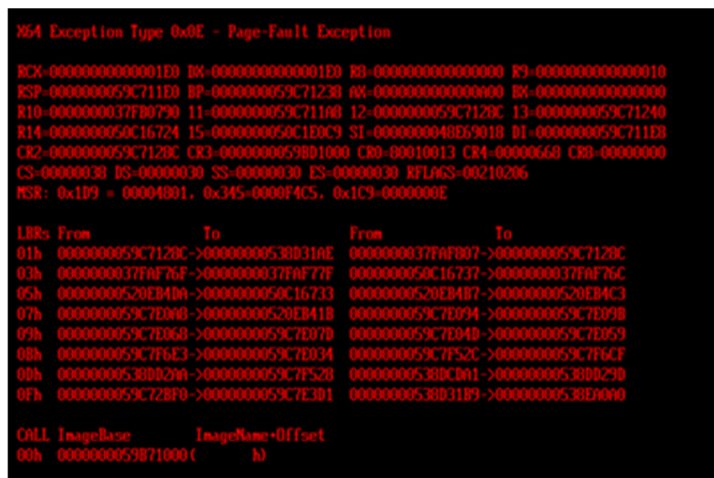


日本語表示の場合

● 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 起動前にまれに赤文字画面 (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。

● ネットワーク PXE ブートでサーバーの操作ができなくなることがある

システム ROM バージョン 3.10 (02/22/2024) 未満の場合、ネットワーク PXE ブートによる OS 起動中に、まれに本製品が応答なくなることがあります。

この問題が発生した場合、以下 a)、b)、いずれかの手順を実施し、本製品を再起動してください。

- POWER スイッチを長押しして本製品の電源をオフにし、その後、POWER スイッチの押下により本製品の電源をオンにしてください。
- iLO Web インターフェイスから「電源」>「押し続ける」を選択して本製品の電源をオフにし、その後、「電源」>「瞬間的に押す」を選択して本製品の電源をオンにしてください。

システム ROM バージョン 3.10 (02/22/2024) では、この問題が修正されています。

● 「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。

● シリアルコンソールに POST デバッグ情報が出力される件について

システム ROM バージョン 2.32 (03/09/2020)において、POST 実行時、まれに POST デバッグ情報がシリアルポートに出力され、POST 実行時間がおおよそ 2 分長くなることがあります。
システム ROM バージョン 2.34 (04/09/2020)では、この問題が修正されています。

● 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 機能が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

● RESTful インターフェースツールによる RBSU 設定のバックアップ(保存)とリストア(復元)の注意事項

iLO5 ファームウェアバージョン 2.40 以降の場合、RESTful インターフェースツールを使用した RBSU 設定の保存と復元は使用できません。

RBSU 設定の保存と復元は、システムユーティリティの Backup and Restore Settings メニューから行ってください (メンテナンスガイド(共通編)の「システムユーティリティの RBSU 設定の保存と復元」を参照)。

● SW RAID 有効時、内蔵 DVD ドライブ (N8151-137/138)が 2 個表示される件について

システム ROM バージョン 2.32 (03/09/2020)未満の場合、Embedded SATA Configuration 設定(*1)を [Smart Array SW RAID Support]設定時、運用環境により Disk Utilities メニュー(*2)に内蔵 DVD ドライブ情報が 2 個表示されます。

どちらのドライブを選択した場合でも同じ内蔵 DVD ドライブの情報が参照できます。

(*1) 「System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration」

(*2) 「System Configuration > HPE Smart Array S100i SR Gen10 > Disk Utilities」

● 工場出荷時の設定について

以下の項目については、工場出荷時に以下のように設定しています。

- (1) System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile を「Custom」に設定。
- (2) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Core C-State を「No C-states」に設定。
- (3) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Package C-State を「No Package States」に設定。

● 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 2.62 (03/08/2022) 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

- (1) BMC Configuration Utility 配下のメニューの変更権限については、BMC Configuration Utility > Setting Option > Require user login and configuration privilege for BMC Configuration を有効にすることで保護してください。
BIOS/Platform Configuration (RBSU) > Server Security > Set Admin Password の設定では保護されません。
- (2) System Information > Processor Information で表示される L2 Cache、L3 Cache の Maximum Size、Installed Size は 1MB を 1048576 バイトに換算した数値で表示されます。
- (3) 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 2.68 (07/14/2022) 未満

- ・ N8103-240 の場合

以下の条件を満たす場合、発生します。

- RAID コントローラファームウェアが v52.16.3-4455

● PCIe Slot X MCTP Broadcast Support メニューについて (X は PCIe Slot 番号)

システム ROM バージョン 2.10 (05/21/2019) 以降の装置において、初めて PCIe MCTP Options メニュー(*1) を選択した場合、装置のデフォルト設定を強制的に設定する旨のポップアップ(*2)が、設定可能な PCIe Slot 数分表示されます。

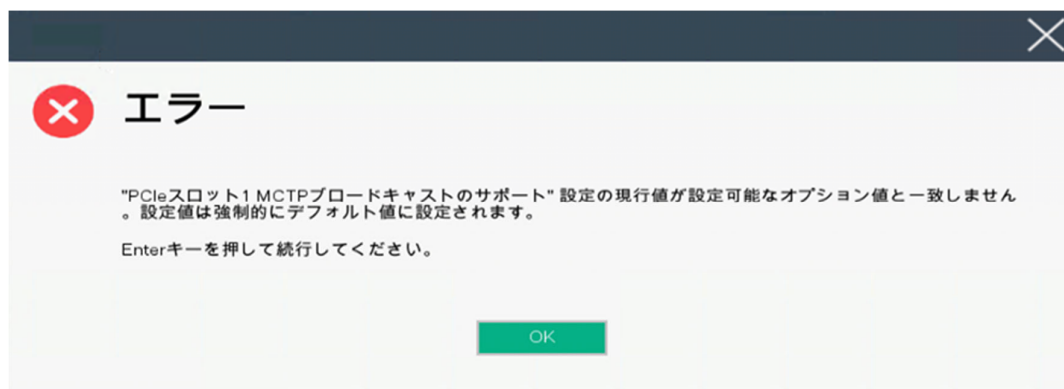
設定を一度保存すると、次回以降ポップアップ表示はされません。

なお、下記システム ROM バージョンの場合、設定保存時にポップアップ(*3)が表示され設定は保存されません。保存されないことにより、本メニューを表示させるたびに PCIe Slot 数分のポップアップ(*2)が表示されることになります。この場合、MCTP Broadcast は常に有効で動作します。

- ・ 2.22 (11/13/2019)
- ・ 2.30 (02/11/2020)
- ・ 2.32 (03/09/2020)

*1 : System Configuration > BIOS/Platform Configuration(RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options

*2 :



*3 :



● Extended Memory Test オプションの設定値について

システム ROM バージョン 2.36 (07/16/2020) の場合、Extended Memory Test オプションは、自動的に Disabled となります。

System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Extended Memory Test

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ません。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。

● 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 Virtual NIC 設定の注意事項

[Security] > [iLO]の“Virtual NIC”のデフォルト値は、iLO5 ファームウェアのバージョンにより異なります。BMC 構成ユーティリティにて“工場出荷時のデフォルトにセット”を実施した場合は、以下をご確認ください。

- (1) iLO5 ファームウェアバージョン 2.10 以降、2.18 未満でご使用の場合、デフォルト値は『有効(Enabled)』です。
仮想 NIC をサポートしていない Windows Server 2012 R2 や USB CDC-EEM ドライバがインストールされていない Windows Server 2016/2019/2022 上のデバイスマネージャーで「Virtual NIC」が警告表示される場合があります。
[Security] > [iLO]の” Virtual NIC” の設定を『無効(Disabled)』に変更してください。
- (2) iLO5 ファームウェアバージョン 1.40 以降、1.47 未満、または 2.31 以降でご使用の場合、デフォルト値は『無効(Disabled)』です。

● Windows 上での vEthernet (Hyper-V Virtual Ethernet Adapter) 構成時の iLO Web インターフェイスのネットワークアダプタの IPv6 アドレス表示に関する注意事項

iLO5 ファームウェアバージョン 2.10 以降、2.18 未満でご使用の場合、Windows OS 上で vEthernet (Hyper-V Virtual Ethernet Adapter) が構成されている場合、iLO Web インターフェイスの [Information] > [Network] > [Physical Network Adapters] において、構成されている各 [Adapter] の [Network Ports] の” IPv6 Address” において正しい IPv6 アドレスが表示されない場合があります。vEthernet 構成時の IPv6 アドレスに関しては、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。

● 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、iLO5 ファームウェアバージョン 2.31 以降でご使用の場合、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 インターフェイスの Device Inventory 情報の表示について

＜SAS エキスパンダカード (N8116-51) 構成時＞

iLO5 ファームウェアバージョン 2.31 以降でご使用の場合、iLO Web インターフェイスの [System Information] > [Device Inventory] において、SAS エキスパンダカードの表示情報が以下のように表示される場合がありますが、サーバーの運用および SAS エキスパンダカードの動作に影響はありません。

- Firmware Version : N/A
- Status : Disabled

● 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。

● iLO Web インターフェイスのセキュリティダッシュボードの注意事項

iLO5 ファームウェアバージョン 1.47 以降、2.10 未満をご使用の場合、[Information] > [Security Dashboard]に [Last Firmware Scan Result]が表示されますが、本ハイパーリンクをクリックしないでください。
誤ってクリックした場合、Web サイト内のメニュー間移動ができなくなります。その場合、ブラウザのリロードボタンをクリックするか、もしくはいったん iLO Web インターフェイスのログアウトを実行して再度ログインしてください。

情報 - セキュリティダッシュボード

概要 セキュリティダッシュボード セッションリスト iLOイベントログ インテグレートドマネジメントログ

Active Health Systemログ 診断

全体セキュリティステータス: OK

セキュリティ状態 本番環境
サーバー構成ロック: Disabled

セキュリティパラメーター	↓ステータス	状態	無視
セキュリティオーバーライドスイッチ	♥ OK	Off	☐
IPMI/DCMI over LAN	♥ OK	無効	☐
最小パスワード長	♥ OK	OK	☐
iLO RBSELへのログイン要求	♥ OK	有効	☐
認証失敗ログ	♥ OK	有効	☐
セキュアブート	♥ OK	有効	☐
パスワードの複雑さ	♥ OK	有効	☐
ホスト認証が必要	♥ OK	無効	☐
最新のファームウェアスキャン結果	♥ OK	OK	☐

日本語表示の場合

Information - Security Dashboard

Overview Security Dashboard Session List iLO Event Log Integrated Management Log

Active Health System Log Diagnostics

Overall Security Status : OK

Security State Production
Server Configuration Lock: Disabled

Security Parameter	↓Status	State	Ignore
Security Override Switch	♥ OK	Off	☐
IPMI/DCMI Over LAN	♥ OK	Disabled	☐
Minimum Password Length	♥ OK	OK	☐
Require Login for iLO RBSEL	♥ OK	Enabled	☐
Authentication Failure Logging	♥ OK	Enabled	☐
Secure Boot	♥ OK	Enabled	☐
Password Complexity	♥ OK	Enabled	☐
Require Host Authentication	♥ OK	Disabled	☐
Last Firmware Scan Result	♥ OK	OK	☐

英語表示の場合

● 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 6.5/6.7 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。

・ 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=#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。

● 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。”

● Rapid Setup 実行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 2.71 または 2.72 をご使用の場合:

Smart アレイ SW RAID 構成時に、POST 時に<F10>キー押下 > Provisioning > EXPRESSBUILDER から Rapid Setup を実行する際は、事前に iLO Web インターフェイスの[System Information] > [Device Inventory]で、Smart Array S100i SR の Status が” Enabled” になっていることを確認してください。
Status が” Unknown” と表示されている状態で、Rapid Setup を実行すると “推奨される RAID 構成を準備中…” の表示の後に以下のメッセージが表示される場合があります。

- “Rapid Setup は、このシステムに設置されているサポート対象ディスクを見つけられませんでした。
ディスクが設置されていないか、ケーブル接続などの別の問題があります。
Rapid Setup を終了し、ハードウェア構成を確認してください。”

● 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、まれに 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

● EXPRESSBUILDER での Windows 「手動」 インストールについて

EXPRESSBUILDER から Windows をインストールするとき、「手動」オプションを選択した場合であっても、インストール先ディスクのパーティションがすべてクリアされます。再インストール時、ユーザーデータが存在する場合は注意してください。

● Windows Server OS ご使用時の注意事項

サポート対象の Windows Server OS で USB デバイスをお使いの場合、以下のシステムイベントログが採取されることがあります。
これについては、システム動作上問題ありません。

<イベントログ>

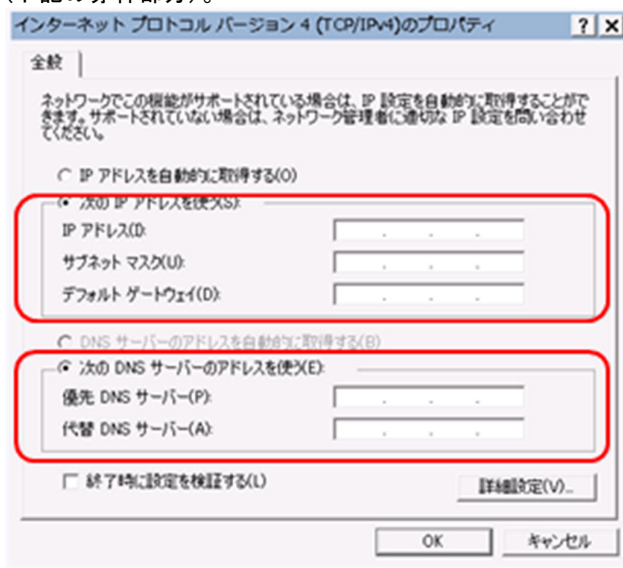
ID : 1
ソース : VDS Basic Provider
レベル : エラー
説明 : 予期しないエラーが発生しました。エラーコード:32@01000004

● Windows Server 2019/2016/2012 R2 環境構築後、CPU ボードの構成変更を行う場合の注意事項

次の Option に固定 IP アドレス/固定 DNS を設定している場合、以下の手順で増設 CPU ボードを増設してください (CPU 増設後も固定 IP アドレス設定を引き継ぐために本手順が必要です)。

N8104-182 10GBASE-T 接続ボード (2ch)
N8104-183 10GBASE-T 接続ボード (2ch)
N8104-185 10GBASE 接続基本ボード (SFP+/2ch)
N8104-187 25GBASE 接続基本ボード (SFP28/2ch)
PCI-to-PCI ブリッジを持つ増設 PCI カード

- (1) 該当のオプションを参照するサービスが自動起動しないように設定を変更し、サービスを停止する。
また、該当のオプションにストレージを接続している場合、以下の作業前に該当のオプションから LAN ケーブルを外す等ストレージを認識しないようにする。
- (2) 該当のオプションで LAN のチーミング設定をしている場合、チーミングを解除する。
- (3) 該当のオプションの IP アドレス/サブネットマスク/デフォルトゲートウェイ/優先 DNS サーバー/代替 DNS サーバーを記録する (下記の赤枠部分)。



- (4) 該当のオプションの IP アドレスを「IP アドレスを自動的に取得する」、DNS アドレスを「DNS サーバーのアドレスを自動的に取得する」に設定変更する。
- (5) 増設 CPU ボードをユーザーズガイドに従って増設する。
- (6) 該当のオプションに手順 (3) で記録した IP アドレス/サブネットマスク/デフォルトゲートウェイ/優先 DNS サーバー/代替 DNS サーバーを設定する。
- (7) LAN のチーミングを再設定する。
- (8) 手順 (1) で設定変更したサービスを自動起動するように再設定する。また、該当のオプションにストレージを接続していた場合、LAN ケーブルを再接続しストレージを認識できるようにする。



上記手順で行わなかった場合、固定 IP アドレスがほかのデバイスで使用されている等のメッセージが表示されて固定 IP アドレスが設定できないことがあります。

その場合、以下のコマンドをコマンドプロンプトで実行して、デバイスマネージャーを起動してください。

その後、[表示] > [非表示デバイスの表示] をクリックし、ネットワークアダプターツリーを展開し、グレー表示になっている未使用のデバイスを削除してください。

```
>set devmgr_show_nonpresent_devices=1
```

```
>Start DEVMGMT. MSC
```

ESMPRO/ServerManager でネットワークを参照した場合、増設 CPU ボードの構成変更後にネットワークカードが重複して表示されます。OS 上で見えないネットワークデバイスの詳細は「Unknown」と表示されますので、無視してください。

● 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 インストールガイド(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 インストールガイド(Windows 編)」をクリックします。
- (5) 「ESMPRO/ServerManager Ver. 7 インストールガイド(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。

● VMware ESXi/ESX を使用する際の注意事項

ESXi/ESX 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/ESX 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/ESX 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。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

システム ROM バージョン 2.00 (02/02/2019) 以降、かつ 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、まれに 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。

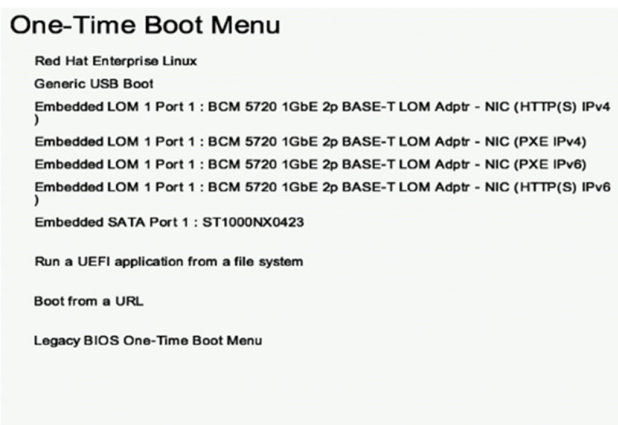
また、PCI アドレスを含む/dev/disk/by-path/配下のストレージデバイス名は使用しないでください。

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нта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нтаイムブートメニュー画面

● Nutanix on Express5800 / Nutanix Core on Express5800 について

N8100-2834S1Y/2834S2Y/2835S1Y/2835S2Y/2837S1Y/2837S2Y/2839S1Y/S2839S2Y をご使用される場合は、以下の Web サイトに掲載している情報を必ずご確認ください。

<https://www.support.nec.co.jp/View.aspx?id=3140107810>

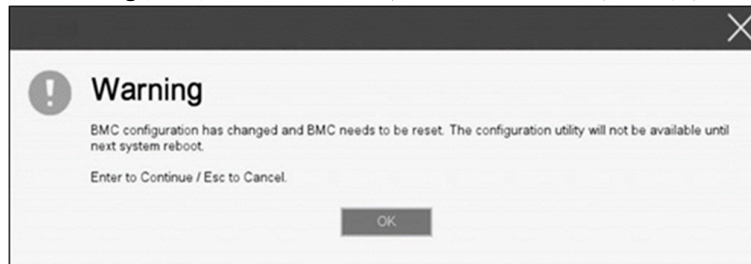
5) 全般の機能に関する注意事項

● 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

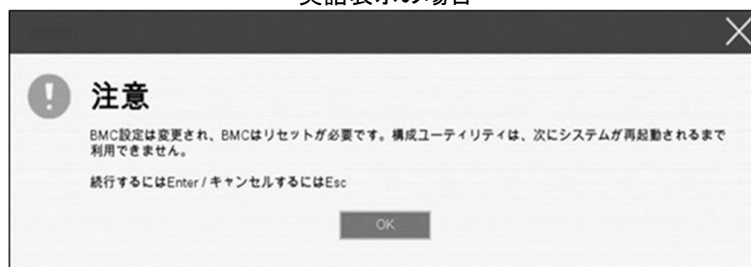
システムユーティリティの「BMC Configuration Utility」での操作において、以下の(1)のポップアップが表示された場合は(2)以降の手順を厳守してください。

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。

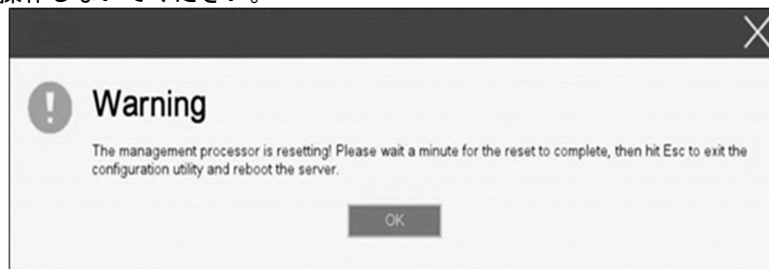


英語表示の場合

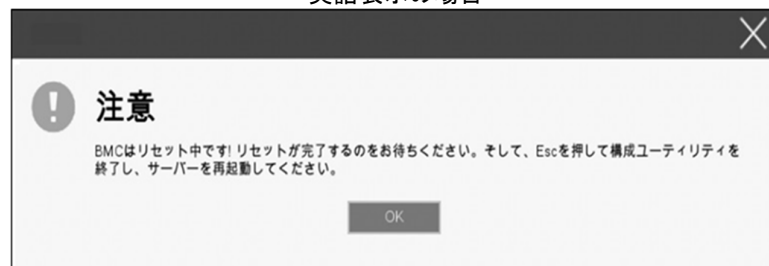


日本語表示の場合

- (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。

● Serial Number、Product ID が消失した場合の対処について

Serial Number、Product ID が消失した場合、以下の手順にて復旧することができます。

- (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します。
- (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します。
- (3) POWER スイッチで装置の電源をオンにします。
- (4) サーバーが起動し、POST 画面が表示されます。
- (5) <F9>キーを押してシステムユーティリティを起動します。もし、システムユーティリティが起動できない状態になっている場合は、メンテナンスガイドの「1 章(7.4.3 システム設定をデフォルト値に戻す)」を参照し、システムメンテナンススイッチを操作して、RBSU 設定の初期化をします。
- (6) システムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、Serial Number と Product ID の値を確認します。
- (7) Serial Number と Product ID の値が期待する値の場合は、手順 14)に進みます。
- (8) Serial Number と Product ID の値が期待する値ではない(消失している)場合は、システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options」を選択します。
- (9) 「Restore Default Manufacturing Settings」を選択します。
- (10) 「Yes, restore the default settings.」を選択します。
- (11) 自動的に装置が再起動し、POST 画面が表示されます。
- (12) <F9>キーを押してシステムユーティリティを起動します。
- (13) 装置のスライドタグに記載されている Serial Number と Product ID をシステムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、設定します。



【重要】Product ID とは、『N8100-2834Y』のような型番のことです。

- (14) RBSU 設定項目をデフォルト値から変更されている場合は、その RBSU 項目の確認と再設定をします。

● 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。

- ・ N8181-160 電源ユニット(800W/Platinum)を冗長構成で搭載している場合、以下の設定を変更してください。

System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options へと進み、「Redundant Power Supply Mode」を「High Efficiency Mode (Auto)」に設定してください。

※ High Efficiency Mode (Odd Supply Standby)、または、High Efficiency Mode (Even Supply Standby)に設定されているお客様については、上記の変更は不要です。

● N8103-240 RAID コントローラご使用時の注意事項

- 1) 新規に N8103-240 RAID コントローラをご購入される場合、及び Starter Pack (ver. S8.10-010.10) を適用された場合、RAID コントローラのファームウェアが「52.26.3-5379」となります。

本ファームウェアではアレイの拡張機能を使用しないでください。
使用した場合、実行した処理が完了しない場合があります。

アレイの拡張機能は実行するユーティリティによりメニューの名称が異なります。

System Utilities 上の名称 : Reconfigure Logical Drives
LSI Storage Authority 上の名称 : Modify Array

- 2) N8103-240 RAID コントローラ搭載済み装置のシステム ROM バージョンが 3.34 (09/30/2024) 未満の場合、まれに論理ドライブ名が保存されないことがあります。この現象が発生しても、サーバーの運用に影響はありません。発生した場合は、再度、論理ドライブ名の保存を実施してください。

システム ROM バージョン 3.34 (09/30/2024) では、この問題が修正されていますので、アップデートを推奨します。

System Utilities 上の名称 : Logical Drive Name

● N8116-51 SAS エキスパンダカード ご使用時の注意事項

Starter Pack Version S8.10-009.01 に含まれている、N8116-51 SAS エキスパンダカードの下記ファームウェアアップデートモジュール (Ver. 5.08) は、適用しないでください。

[パッケージ名称]

Supplement Update / Online ROM Flash Component for Linux (x64) ? HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
(firmware-smartarray2de15b6882-5.08-1.1x86_64)

詳細につきましては、以下の Web サイトに掲載されている内容を確認してください。

[Starter Pack Version S8.10-009.01]

<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)

● 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)

◆ 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。

● 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 のヘルプについて

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>

● ディスプレイポートについて

装置前面のディスプレイポートの動作は、サポートしていません。

● ドキュメントの型番読み替えについて

末尾が HnY (n は数字)で終わる型番の装置に添付されているドキュメント(ユーザーズガイド、メンテナンスガイド)では、記載されている N 型番に Hn を付加して読み替えてください。

例 : N8100-2834Y → N8100-2834H1Y

また、末尾が SnY (n は数字)で終わる型番の装置に添付されているドキュメントでは、記載されている N 型番に Sn を付加して読み替えてください。

例 : N8100-2834Y → N8100-2834S1Y

● N8103-239 480GB OS ブート専用 SSD ボード (RAID 1) 使用時の注意事項

装置前面のステータスランプでは N8103-239 のステータスを確認することができません。

装置背面の N8103-239 のドライブベイ LED にてステータスの確認を行ってください。

● N8103-240 RAID コントローラ (4GB, RAID 0/1/5/6)使用時の注意事項

① ドライブ位置の表示についての注意事項

iLO Web インターフェイスのストレージ情報、Server Boot Order、および System Utilities のワンタイムブートメニュー、UEFI Boot Order においてドライブの位置が Box/Bay の順番に表示されません。

順番に表示されないだけで、ステータス/容量/メディアタイプは搭載のデバイスの情報を表示していますので、問題はありません。

② ステータスランプの表示についての注意事項

装置前面のステータスランプでは N8103-240 のステータスを確認することができません。

ホットプラグ対応 SATA/SAS ドライブの、障害/特定ランプおよび認識/動作ランプにてステータスの確認を行ってください。

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) Server Availability メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability」を選択すると、「Server Availability」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
IPMI Watchdog Timer (注 1)	[Disabled] Enabled	IPMI に準拠した起動時の (POST) ウォッチドッグタイマー (WDT) を有効にできます。このタイマーは、ユーザーがシステムに対して IPMI コマンドを発行すると無効になり、自動的には無効になりません。 IPMI ウォッチドッグタイマー (WDT) は、POST 中に<F9>キー、または<F10>キーを押すと停止できます。 POST 中の<F9>キー、または<F10>キーを押した以外の場合、WDT は選択された IPMI ウォッチドッグタイマーのタイムアウト期間の後にタイムアウトし、システムは選択された IPMI ウォッチドッグタイマー動作を続行します。
IPMI Watchdog Timer Timeout (注 1)	10 Minutes 15 Minutes 20 Minutes [30 Minutes]	サーバーのロックアップが発生した場合にサーバーに対して必要なタイムアウト動作を実行するまでの待機時間を設定できます。
IPMI Watchdog Timer Action (注 1)	[Power Cycle] Power Down Warm Boot	サーバーのロックアップによってウォッチドッグタイマーが時間切れになったときのタイムアウト動作を設定できます。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.54 以降にて追加されるオプションです。

(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
Energy Performance Preference (注 1)	[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。ご使用の環境でベンチマークを実施し、パフォーマンスの向上を確認した上で、本オプションを有効にしてください。

[]: 出荷時の設定

注 1: システム ROM バージョン 2.80 以降にて追加されるオプションです。

(3) 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
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 2.54 以降にて追加されるオプションです。

(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 (注1)	[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 2.80 以降にて追加されるオプションです。

■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。

Precautions for Using Express5800/ R120h-1M (3rd-Gen), R120h-2M (3rd-Gen)

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 3.34, 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).

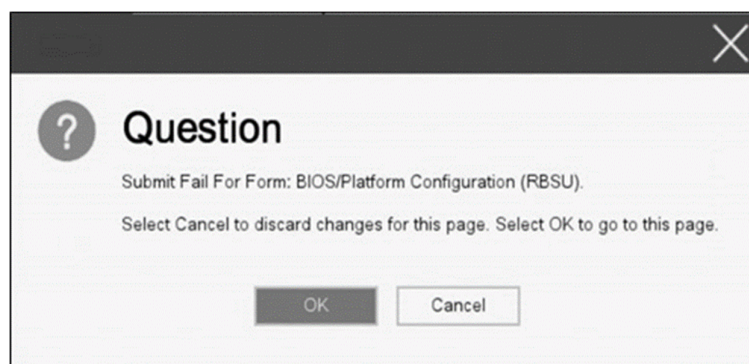
Additionally, each time you navigate to the UEFI Boot Order menu or the UEFI Boot Order Control menu, a red circle (◎) will appear in front of the "Changes Pending" string at the bottom of the screen. Press the F10 key as needed to save the settings.

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

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

● 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 RSOD(Red Screen Of Death) screen

If you have changed the server configuration/settings or the system status, a RSOD(Red Screen Of Death) 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.

```
X64 Exception Type 0x0E - Page-Fault Exception

RAX-00000000000001E9 BX-00000000000001E9 EB-0000000000000000 ED-0000000000000010
ESP-0000000059C711E9 EIP-0000000059C71238 AX-0000000000000000 EC-0000000000000000
R10-0000000037FB0790 R11-0000000059C711A8 R12-0000000059C7120C R13-0000000059C71240
R14-0000000050C16724 R15-0000000050C1E0C9 SI-0000000048D69018 DI-0000000059C711E9
CR2-0000000059C7120C CR3-0000000059B01000 CR0-00010013 CR4-00000668 CR8-00000000
CS-00000038 DS-00000030 SS-00000030 ES-00000030 RFLAGS-00210206
MSR: 0x1D9 = 00004801, 0x345=0000F4C5, 0x1C9=0000000E

LRRs From To From To
01h 0000000059C7120C->0000000053B031AE 0000000037FAF007->0000000059C7120C
03h 0000000037FAF76F->0000000037FAF77F 0000000050C16737->0000000037FAF76C
05h 00000000520EB4DA->0000000050C16733 00000000520EB4B7->00000000520EB4C3
07h 0000000059C7E0A8->00000000520EB41B 0000000059C7E094->0000000059C7E09B
09h 0000000059C7E0A8->0000000059C7E07D 0000000059C7E04D->0000000059C7E059
0Bh 0000000059C7F6E3->0000000059C7E034 0000000059C7F52C->0000000059C7F6CF
0Dh 0000000053B0D2FA->0000000059C7F52B 0000000053BDC0A1->0000000053B0D290
0Fh 0000000059C728F0->0000000059C7E3D1 0000000053B031B9->0000000053B0E0A0

CALL ImageBase ImageName+Offset
00h 0000000059B71000( h)
```

● 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 RSOD(Red Screen Of Death) 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 a RSOD(Red Screen Of Death) appears, power the device OFF and then ON. After that, 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.

● Server may become unresponsive during Network PXE Boot

If the System ROM Version is earlier than 3.10 (02/22/2024), the server may occasionally become unresponsive when booting via Network PXE Boot with an OS. If this issue occurs, please follow one of the procedures below to restart the server:

- a) Press and hold the power button to turn off the server. Then, press the power button again to turn on the server.
- b) Select "Power" -> "Press and Hold" from the iLO Web Interface to turn off the server. Then, select "Power" -> "Momentary Press" from the iLO Web Interface to turn on the server.

This issue has been fixed in System ROM Version 3.10 (02/22/2024).

● 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.

● About UEFI Serial Debug output on BIOS Serial Console

UEFI Serial Debug output could inadvertently be seen over BIOS Serial Console with System ROM Version 2.32 (03/09/2020). This issue would be seen periodically on server reboots. POST time will increase by about 2 minutes.

This issue has been fixed in System ROM Version 2.34 (04/09/2020).

● 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

● Notice of the backup and restore of RBSU Settings by RESTful Interface tool.

In the case of iLO5 Firmware Version 2.40 or later, backup and restore of RBSU Settings should be done from "Backup and Restore Settings" menu under System Utilities. (See "Backup and Restore of RBSU Settings" in Maintenance Guide (Common).)

● About the internal DVD-ROM (N8151-137/138) display

Embedded SATA Configuration setting (* 1) is set to [Smart Array SW RAID Support], two internal DVD drive information is displayed in the Disk Utilities menu (* 2) depending on the operating environment.
Both can refer to the same internal DVD information.

(*1) 「System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration」

(*2) 「System Configuration > HPE Smart Array S100i SR Gen10 > Disk Utilities」

● Factory settings on the following items of BIOS/Platform Configuration (RBSU) are as below.

(1) System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile : Custom

(2) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Core C-State : No C-states

(3) System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Package C-State : No Package States

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

When System ROM is v2.62 (03/08/2022) 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

- (1) To protect the change permissions on the menu under BMC Configuration Utility, enable BMC Configuration Utility > Setting Option > Require user login and configuration privilege for BMC Configuration.

It isn't protected by setting of BIOS/Platform Configuration (RBSU) > Server Security > Set Admin Password.

- (2) The Maximum Size and Installed Size of L2 and L3 cache in "System Information > Processor Information" are indicated by the values that a 1 MB to 1048576 bytes.

- (3) 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 v2.68 (07/14/2022).

- For N8103-240

The above problem occurs if:

The version of the RAID controller firmware is v52.16.3-4455.

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.

● About the PCIe Slot X MCTP Broadcast Support menu (X is PCIe Slot number)

In the device with the System ROM Version 2.10 (05/21/2019) or later, when the PCIe MCTP Options menu is selected (as described in *1 below) for the first time, the pop-ups (*2) informing that the settings for the device will be forcibly set to default will be displayed as many as the number of settable PCIe slots.

Meanwhile, in the device with the System ROM of the following versions, when the settings are tried to be saved, the pop-up (*3) appears and the settings are not saved. As a result, the pop-ups (*2) will be displayed as many as the number of the PCIe slots every time this menu is displayed. In this case, MCTP Broadcast always operates in an enabled state.

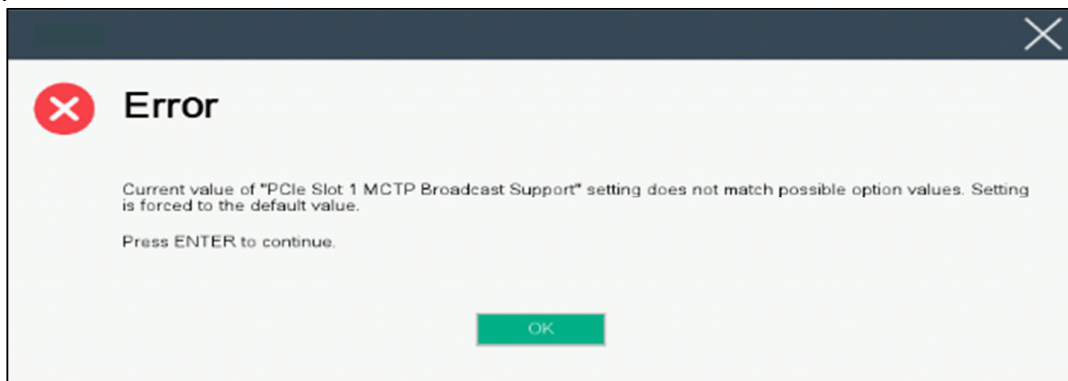
- v2.22 (11/13/2019)

- v2.30 (02/11/2020)

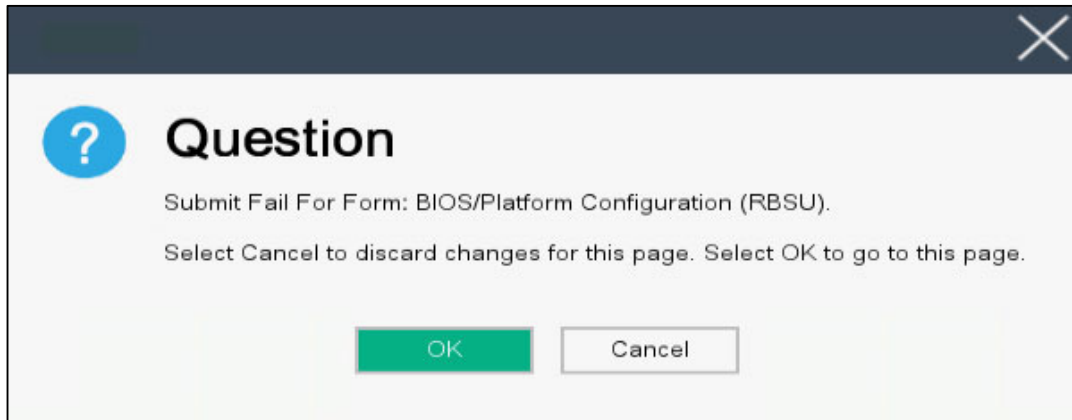
- v2.32 (03/09/2020)

*1 : System Configuration > BIOS/Platform Configuration(RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options

*2:



*3:



● About set value of Extended Memory Test option

When System ROM Version is v2.36 (07/16/2020), Extended Memory Test option is set to "Disabled" automatically after a system reboot.
System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Extended Memory Test

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 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 (*1).

(*1) 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 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.

● Caution about Virtual NIC settings on iLO Web Interface

The default value of "Virtual NIC" in [iLO] of [Security] depends on the version of the iLO5 Firmware.

If "Set to factory default" is executed in the BMC configuration utility, check the following:

- (1) If you use iLO5 Firmware Version between 2.10 and 2.18, the default value of "Virtual NIC" is "Enabled".
A warning may be displayed for "Virtual NIC" on the device manager of Windows Server 2012 R2 which does not support virtual NIC or Windows Server 2016/2019/2022 where USB CDC-EEM driver is not installed.
If you do not use the iLO virtual NIC functionality, go to [Security] > [iLO], and set "Virtual NIC" to "Disabled".
- (2) If you use iLO5 Firmware Version between 1.40 and 1.47, or 2.31 or later, the default value of "Virtual NIC" is "Disabled".

● Caution about IPv6 address of Network Adapter on iLO Web Interface if vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on Windows

If iLO5 Firmware Version between 2.10 and 2.18 below is used and vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on Windows, "IPv6 Address" of [Network Ports] in each Adapter may be not accurate on [Information] > [Network] > [Physical Network Adapters].

Please confirm The Property of each network adapter on Windows, if vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on it.

● 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.

● Displaying Device Inventory information in the iLO Web Interface

< Environment with SAS Expander card (N8116-51) >

iLO5 Firmware Version 2.31 or later, SAS Expander card information might be displayed as follows, but it does not affect server operation and SAS Expander card operation.

- Firmware Version : N/A
- Status : Disabled

● 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.

● Caution for the Security Dashboard of iLO Web Interface

If you update to iLO5 Firmware greater than or equal to 1.47 and lower than 2.10, "Last Firmware Scan Result" is displayed in "Information > Security Dashboard". Do not click this Hyperlink.

If you click this link by mistake, you won't be able to move between menus and tabs.

In that case, you need to reload the page by the reload button of the browser.

Or you log out the current session of iLO Web Interface, and please log in again.

Information - Security Dashboard

Overview **Security Dashboard** Session List iLO Event Log Integrated Management Log

Active Health System Log Diagnostics

Overall Security Status: OK

Security State: Disabled
Production: Disabled

Security Parameter	↓ Status	State	Ignore
Security Override Switch	♥ OK	Off	☐
IPMI/DCMI Over LAN	♥ OK	Disabled	☐
Minimum Password Length	♥ OK	OK	☐
Require Login for iLO RBSP	♥ OK	Enabled	☐
Authentication Failure Logging	♥ OK	Enabled	☐
Secure Boot	♥ OK	Enabled	☐
Password Complexity	♥ OK	Enabled	☐
Require Host Authentication	♥ OK	Disabled	☐
Last Firmware Scan Result	♥ OK	OK	☐

● 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-the83, 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)',

● 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 6.5/6.7

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

· 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."

● Note About Rapid Setup

If the iLO5 Firmware Version is 2.71 or 2.72:

Before using Rapid Setup for configuring the Smart Array SW RAID on your system, open the iLO Web Interface, go to [System Information] > [Device Inventory], and then confirm that "Status" of Smart Array S100i SR is "Enabled". During a POST after that, press the F10 key, select [Provisioning] > [EXPRESSBUILDER], and then run Rapid Setup.

If "Status" is "Unknown", running Rapid Setup may display "Preparing recommended RAID configuration" and then the following message:

- "Rapid Setup did not find any supported disk installed on this system.
Either there is no disk installed, or there is a cabling or other problem.
Please exit Rapid Setup and check your hardware configuration."

● Possible high-speed fan rotation and abnormal sound

If the iLO5 Firmware Version is 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 the iLO5 Firmware Version is 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

● About EXPRESSBUILDER Manual Installation

Partitions in the target disk are deleted when you install the Windows by EXPRESSBUILDER even if you select the "Manual" option.

Pay attention to the user data stored in the system drive when re-installing Windows.

● Notice of Windows Server

When the USB device is used in supported Windows Server OS, the next event log is sometimes registered.
But ignore this message since it does not cause any problem for the operation.

< Event Log >

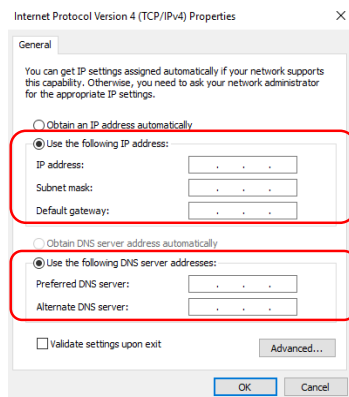
ID : 1
Source : VDS Basic Provider
Level : Error
Unexpected error occurred. Error code :32@01000004

● Notes on changing configuration of CPU board after setting up Windows Server 2019/2016/2012 R2

When a fixed IP address or DNS is set for the following options, add a CPU board by the following procedure.
(The procedure is necessary to take over the fixed IP address setting even after the CPU expansion.)

N8104-182 Dual Port 10GBASE-T Adapter (2ch)
N8104-183 Dual Port 10GBASE-T Adapter (2ch)
N8104-185 Dual Port 10GBASE SFP+ Adapter
N8104-187 Dual Port 25GBASE SFP28 Adapter
Expanded PCI Card with PCI-to-PCI bridge

- (1) Change settings such that the service that refers to the relevant option does not start up automatically and stop service. In addition, when the storage is connected to the option, remove the LAN cable from the option before the following work so that the option does not recognize the storage.
- (2) When setting LAN teaming at the option, cancel teaming.
- (3) Record IP address of the options / sub netmask / default gateway / preferred DNS server / alternate DNS server (the parts in the red frames below.)



- (4) Change the settings of the option as follows: "Obtain an IP address automatically", for IP address and "Obtain DNS server address automatically." for DNS address.
- (5) Follow the user's guide to add a CPU board.
- (6) Set IP address / sub netmask / default gateway / preferred DNS server / alternate DNS server, which are recorded in Step 3), to the option.
- (7) Set LAN teaming again.
- (8) Set up again the service whose setting was changed in Step 1) so that the service starts automatically. When the option is connected to storage, connect the LAN cable again such that the option can recognize the storage.

Tips

If you do not follow above procedure, a message appears, telling for example, that the fixed IP address is used by another device, and you may not be able to set a fixed IP address.

In that case, execute the commands below by command prompt and boot the device manager. Then, click [View] > [Show hidden devices] and expand the network adapter tree, and then delete the grayed out devices that are not in use.

```
>set devmgr_show_nonpresent_devices=1  
>Start DEVMGMT.MSC
```

When you refer to network of NEC ESMPRO Manager, a duplicate network card will be displayed after the configuration of the expanded CPU board is changed CPU processor kit. Please ignore the network device that is not displayed on the OS, and the detail information of the network device will be displayed as "Unknown".

● 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 later	Earlier 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.
	Earlier 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 later	ilo_en.mtb Earlier 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 Earlier 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 iLO5 Firmware Version

- Server Health Summary

Push the UID button on the server and check the version of the iLO5 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 iLO5 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. This caution is about the screen display of VMware vSphere : Monitor > Hardware > System Sensor > Sensor when the ESXi/ESX 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/ESX 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/ESX completes boot, this does not indicate hardware malfunction and there is no impact to the system operation.

- System Chassis 1 UID

● 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/N8103-239WBEM_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.

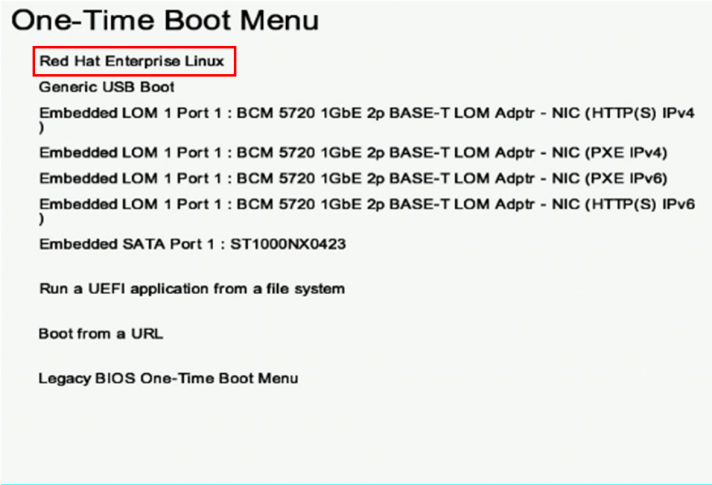
If operation using a device name based on the PCI address is required, do not add/remove the card to/from the PCI slot, or change the CPU configuration. If the PCI bus address information changes and the name of the PCI-connected device is affected, you may not be able to access the network or storage,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

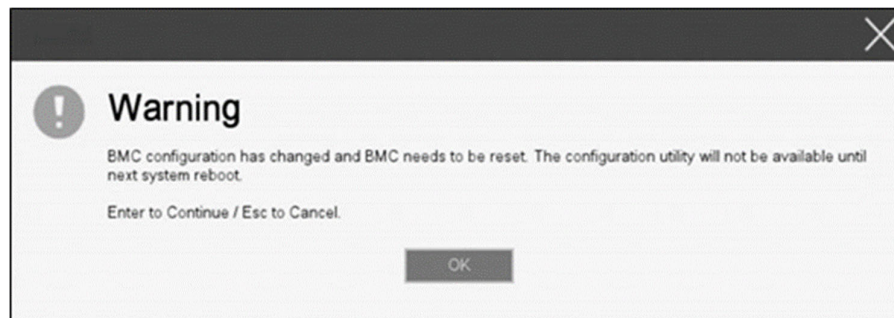
• Caution for operating BMC Configuration Utility in the System Utilities

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.

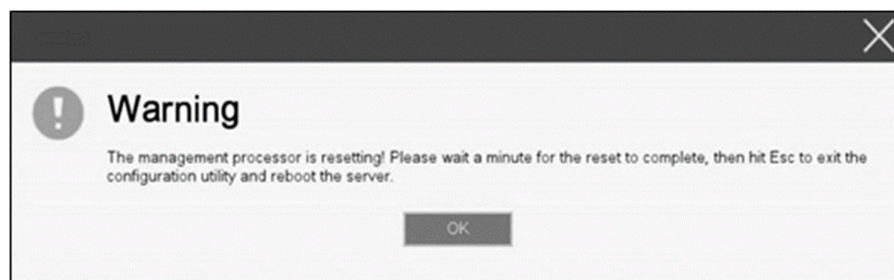
To avoid this trouble in rebooting the iLO, follow these steps:

- (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.

• How to recover lost Serial Number and Product ID

If the server loses Serial Number and Product ID, recover them as follows:

- (1) Power off the server. Then disconnect the plug from the outlet.

- (2) Wait 30 seconds. Then plug the server into the outlet again.

- (3) Turn on the server with the POWER button.

- (4) The server starts up and the POST screen appears.

- (5) Press the F9 key to enter the System Utilities.

If this fails, initialize the RBSU settings with the system maintenance switch (refer to "Chapter 1 7.4.3 Set the System Configuration Back to Default Values" of the maintenance guide).

- (6) Check the values of Serial Number and Product ID by selecting the menu of the System Utilities: **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options.**

- (7) If the values of Serial Number and Product ID are satisfactory, go to step 14.
- (8) If the values are unexpected or lost, select the menu of the System Utilities: **System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options**.
- (9) Select the Restore Default Manufacturing Settings option.
- (10) Select this option: Yes, restore the default settings.
- (11) The server restarts automatically and the POST screen appears.
- (12) Press the F9 key to enter the System Utilities.
- (13) Set the proper Serial Number and Product ID (indicated on the pull-out tab of the server) via the menu of the System Utilities: **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options**.



[Important] Product ID is the model number like "N8100-2834F". Product ID is not PID.

- (14) If the RBSU settings have been changed from the defaults, check and configure the new values.

• Note on using UPS

- When connecting UPS to a serial port, set the items to "Disabled" in the following settings as below:
 - System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > BIOS Serial Console and EMS > BIOS Serial Console Port → [Disabled]**
 - System Configuration > BMC Configuration Utility > Setting Options > Serial CLI Status → [Disabled]**
- If the N8181-160 (power supply unit [800W/Platinum]) is used by redundant configuration, change the following settings:

System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options > Redundant Power Supply Mode → [High Efficiency Mode (Auto)]

Note:

The customer set as High Efficiency Mode (Odd Supply Standby) or High Efficiency Mode (Even Supply Standby) is unnecessary for change above-mentioned.

• Note on using N8116-51 SAS Expander Card

When updating firmware from this Starter Pack (Ver S8.10-009.01), please do NOT apply the following firmware update module (Ver.5.08).

[Package Name]

Supplement Update / Online ROM Flash Component for Linux (x64) ? HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
(firmware-smartarray2de15b6882-5.08-1.1x86_64)

Please check the following Starter Pack Version S8.10-009.01 public page for detailed application procedures.

[Starter Pack Version S8.10-009.01]

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

→ Document & Software

→ Rack

→ (Select your server model)

● Changing the cooling setting

This topic pertains to the following HDDs:

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

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.

● Notes of using SAS controller (N8103-184)

- (1) 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.

● About EXPRESSBUILDER Help

If the EXPRESSBUILDER help is different from Maintenance Guide, do not use the help but the guide.

● About FCoE function in N8104-177

The FCoE function (Fibre Channel over Ethernet) isn't supported with this product as NEC.

The FCoE function is enabled in spite of the LOM firmware version, in N8104-177 with Family Firmware Version after 8.35.43. It is recognized as the FCoE device on the OS, but when not using it from OS and drivers it does not cause any problem for the operation.

Please ignore detection of the following device.

-HPE 622FLR-SFP28 FCoE Device

● About DisplayPort Connector

DisplayPort Connector at the front is not supported.

● 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.

- ◆ The status LED does not show the status of N8103-239.

Check the status with the drive bay LED of N8103-239 on the back side of the equipment.

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) Server Availability Menu

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

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

Option	Parameter	Description
IPMI Watchdog Timer *1	[Disabled] Enabled	Use this option to enable a Boot Time (POST) IPMI compliant Watchdog Timer (WDT) that is disabled when an IPMI command is issued to the system by the user and will not automatically be disabled.
IPMI Watchdog Timer Timeout *1	10 Minute 15 Minute 20 Minute [30 Minute]	Use this option to set the wait timer before performing the desired timeout action on the server in the event of a server lockup.
IPMI Watchdog Timer Action *1	[Power Cycle] Power Down Warm Boot	Use this option to set the timeout action upon expiration of the watchdog timer due to a server lockup.

[]: Default setting

*1: an option usable with System ROM Version 2.54 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.

[]: Default setting

*1: an option usable with System ROM Version 2.80 or later.

(3) Server Security Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security** > from the System Utilities, the Server Security 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 2.54 or later.

(a) Trusted Platform Module Options Menu

When you select **System Configuration > BIOS/Platform Configuration (RBSU) > Server security > Trusted Platform Module Options** from the System Utilities, the **Trusted Platform Module 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 2.80 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.