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。
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 以上、N8101-1723C など末尾が C または D であればバージョン S8.10-007.02 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、「S8.10-006」または「S8.10-007」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「Agentless Management Service および iLO Channel Interface Driver (VMware ESXi 6.x 版(x=5 または 7), 7.0 版, 8.0 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 6.x 版(x=5 または 7), 7.0 版, 8.0 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。

● **Linuxのサポートについて**

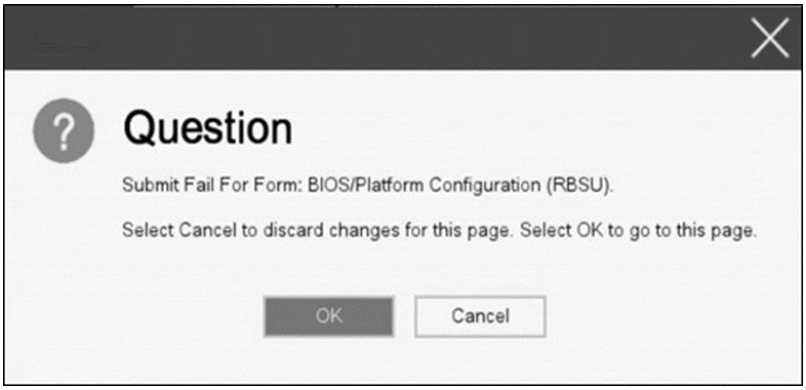
RHEL のサポート状況については、以下の Web サイトをご確認していただくか、ファーストコンタクトセンターまでお問い合わせください。

NEC Linux サービスセット対応モデル
https://jpn.nec.com/linux/linux-os/ss/model.html

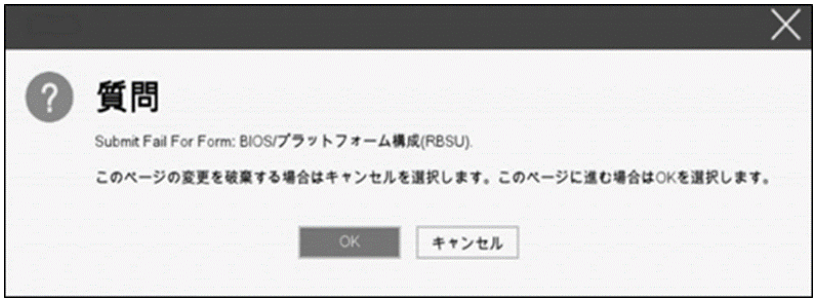
2) システムROMの機能に関する注意事項

● **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、保守サービス会社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。

● **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 v2.32 (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 v2.34 (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以上の場合、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 v2.32 (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 v2.62 (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

(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。
(*)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 以上、または v3.01.04.072 以上
2. システム ROM が v2.68 (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

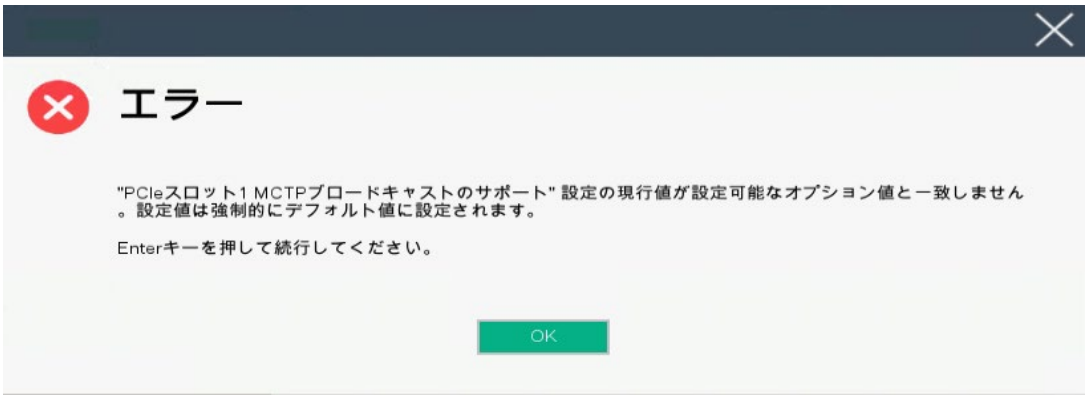
● PCIe Slot X MCTP Broadcast Supportメニューについて　(X はPCIe Slot番号)

システム ROM v2.10 (05/21/2019)以上の装置において、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。

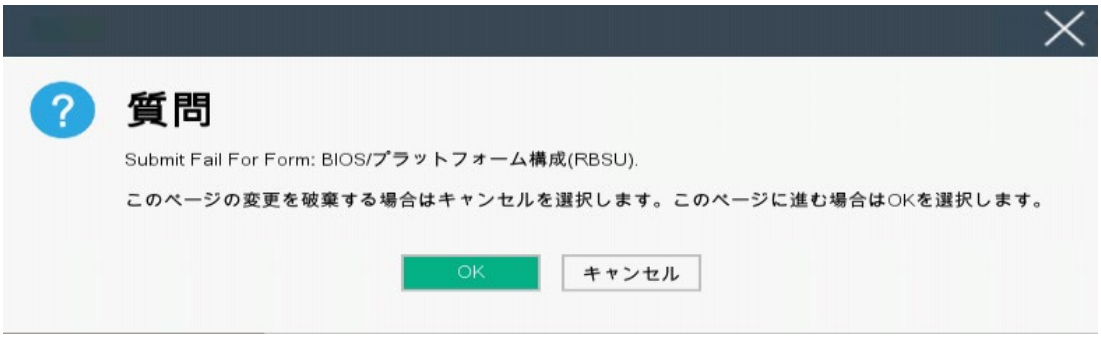
- v2.22 (11/13/2019)
- v2.30 (02/11/2020)
- v2.32 (03/09/2020)

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

*2 :



*3 :



● Extended Memory Testオプションの設定値について

システム ROM v2.36 (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) 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設定を行った場合も、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常に表示されます。
RBSUの設定やiLOの設定の内容次第で、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 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 Autheentication]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。

● **iLO Webインターフェースの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) iLO 5ファームウェア2.10以上、2.18以下でご使用の場合、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) iLO 5ファームウェア1.40以上、1.47以下、または2.31以上でご使用の場合、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インターフェー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**

iLO 5ファームウェア2.10以上、2.18以下でご使用の場合、Windows OS上でvEthernet (Hyper-V Virtual Ethernet Adapter)が構成されている場合、iLO Webインターフェースの[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。

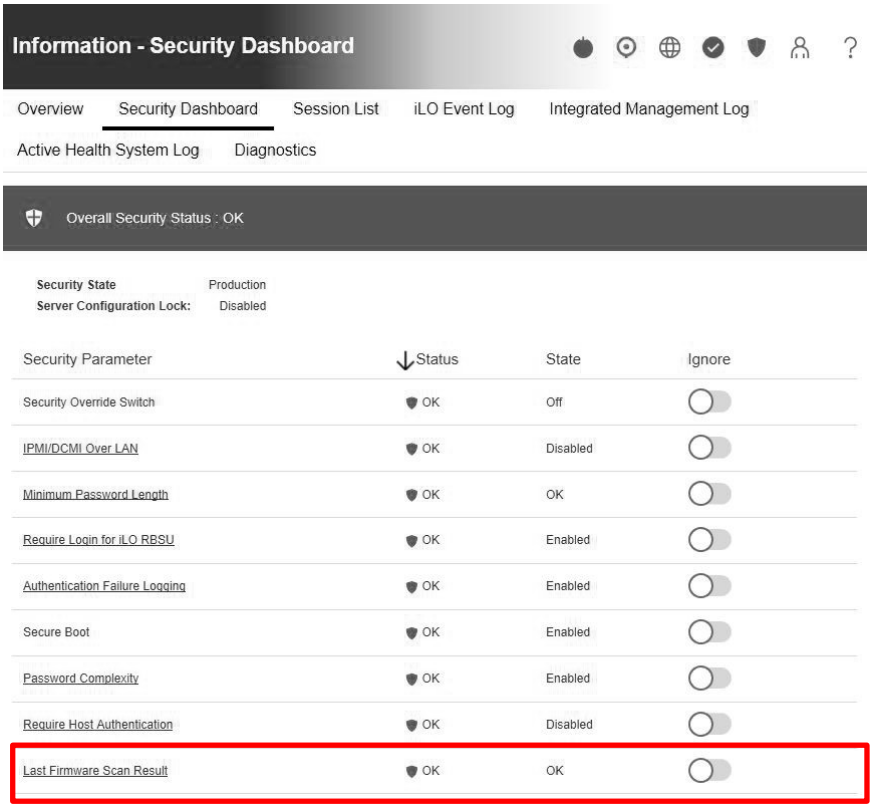
● **ネットワークブリッジ構成時のiLO Webインターフェースのネットワーク情報の表示について**

ネットワークをブリッジ設定で構成し、iLO 5ファームウェア2.31以上でご使用の場合、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インターフェースのセキュリティダッシュボードの注意事項

iLO 5ファームウェア1.47以上、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出来なくなります。その場合、ブラウザー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インターフェースのログアウトを実行して再度ログインしてください。

日本語表示の場合



英語表示の場合

● iLO Webインターフェースの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〉
iLO 5ファームウェア2.31以上でご使用の場合、iLO Webインターフェースの[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

● 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。

● **Java IRCのセッションタイムアウト時に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インターフェースの[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、稀にFANの高速回転やうなり音が7分以上継続する場合があります。

この場合は、再度サーバーの再起動を実施してください。

● **通報に関する注意事項について**

iLO5ファームウェアバージョン3.00以降をご使用の場合:
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

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**

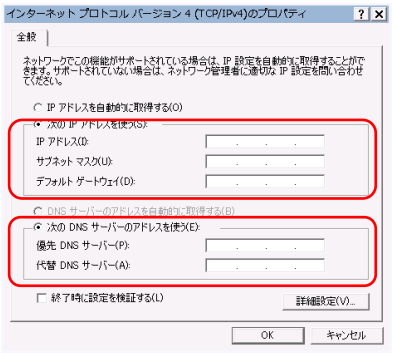
サポート対象の Windows Server OS で USB デバイスをお使いの場合、以下のシステムイベントログが採取されることがあります。
これについては、システム動作上問題ありません。

〈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 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 (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。

◆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 の Web サイトにログインします。
(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を使用する場合の注意事項

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

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

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

● VMware ESXiでTPMキットを使用する場合の注意事項

システム ROM v2.00 (02/02/2019)以上、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 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、N8103-189/190/191/192/193/194/195/196/201/237/238/240 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

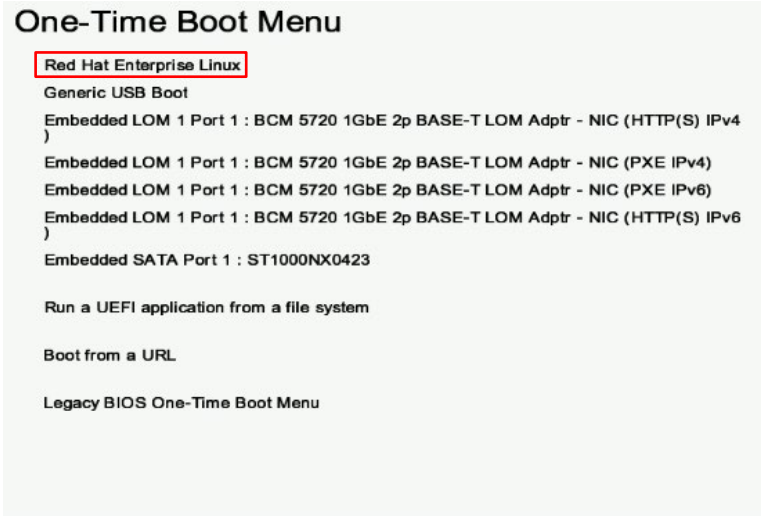
● Linux OSを使用する場合の注意事項

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以前を使用する場合の注意事項

ワンタイムブートメニューから起動する場合、OSブートマネージャー(例: Red Hat Enterprise Linux)を選択してください。
OSがインストールされたHDDやSSDなどのブートデバイスを選択した場合、Red Screen of Death(RSoD)が発生することがあります。



ワンタイムブートメニュー画面

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

N8100-2834S1Y/2834S2Y/2837S1Y/2837S2Y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。

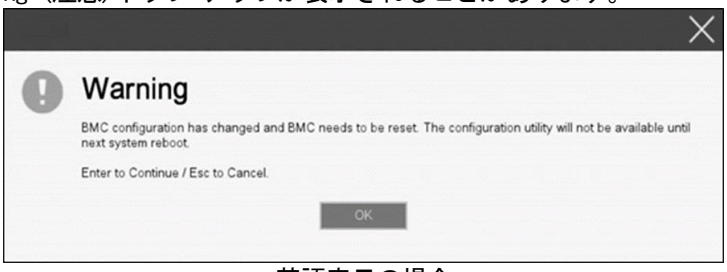
https://www.support.nec.co.jp/View.aspx?id=3140107810

5) 全般の機能に関わる注意事項

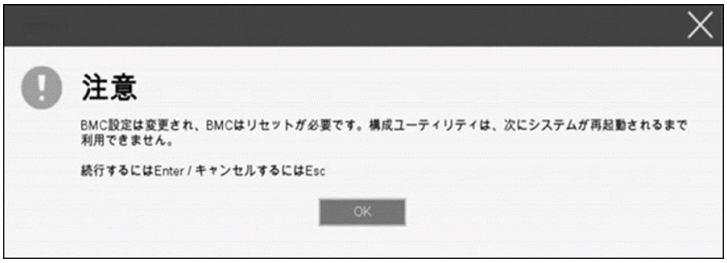
● **システムユーティリティの「BMC Configuration Utility」の操作についての注意事項**

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。

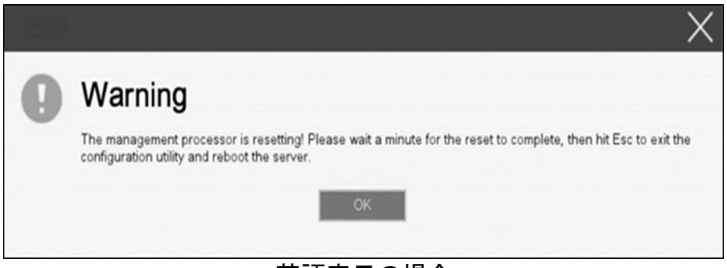


英語表示の場合

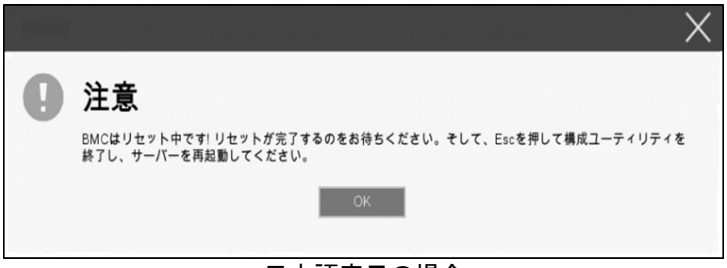


日本語表示の場合

(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。

● **Serial Number、Product IDが消失された場合の対処について**

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

(1) 装置の電源を切り、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ON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、「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。

● **N8116-51 SAS エキスパンダカード使用時の注意事項**

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、System Utilities 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インターフェースの[System Information] - [Storage] - [Storage Controller]のStatusが“不明(Unkown)”と表示される場合がありますが動作に影響はありません。

● **EXPRESSBUILDERヘルプについて**

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

● サーバ診断カルテについて

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

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

■Windows 対応版

NEC サポートポータル（Windows 対応版）

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

■VMware ESXi 対応版

NEC サポートポータル（VMware ESXi 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インタフェー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。

項目	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 以降にて利用できるオプションです。

(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。

項目	パラメーター	説明
Energy Performance Preference	[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。

[ ]: 出荷時の設定

注1:システムROM Version 2.80以降にて利用できるオプションです。

(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。

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。

(a) 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」を選択すると、「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 バージョン 2.80 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。

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

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 web site 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

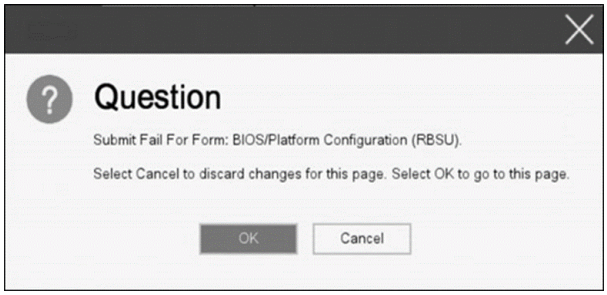
● Notice about service operation time of this product

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

● 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 - 7.4.3 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 v2.32 (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 v2.34 (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 REST ful 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

●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

● **"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)

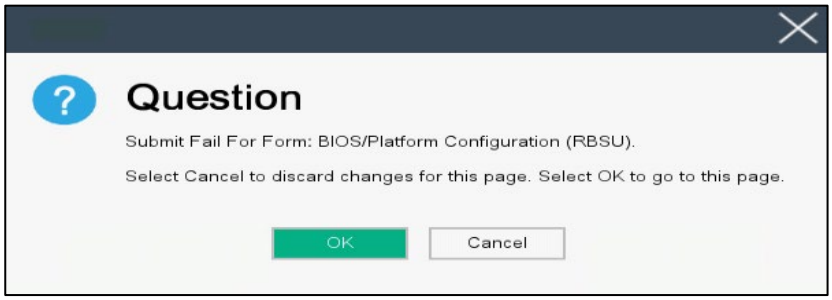
In the device with the system ROM version v2.10 (05/21/2019) or later, when the PCIe MCTP Options menu is selected (as described in *1 below) for the first time, the pop-ups (*2) informing that the settings for the device will be forcibly set to default will be displayed as many as the number of settable 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 :



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 (*).

(*) Don’t 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 iLO 5 firmware.
If "Set to factory default" is executed in the BMC configuration utility, check the following:

(1) If you use iLO 5 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 iLO 5 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 iLO 5 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 comfirm The Property of each network apater on Windows, if vEthernet(Hyper-V Virtual Ethernet Adapter) is configured on it.

● **Display of Network information on iLO Web interface**

If iLO 5 firmware version 2.31 or later is used and 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.

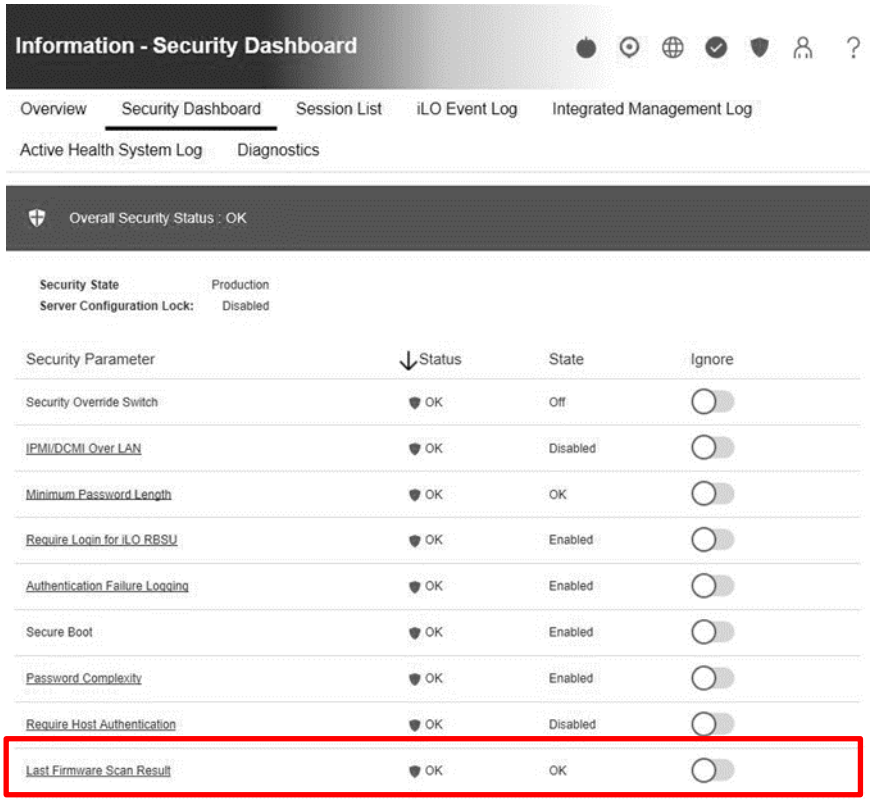
● **Displaying Device Inventory information in the iLO web interface**

< Enviroment with SAS Expander card (N8116-51) >
iLO 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

● 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.



● 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

● 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 you are using the iLO5 firmware 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 you are using the iLO5 firmware 2.90 or later

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

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

●SNMP Alert

If you are using the iLO5 firmware 3.00 or later

For NEC ESMPRO Manager, the Alert Viewer notifies you of a change in a physical-drive status when it is detected. Depending on the status, the location information is displayed in either of the following two patterns:

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

A: Controller location (slot number)
B: The port number of the physical drive
C: box number of the physical drive
D: The bay number of the physical drive

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

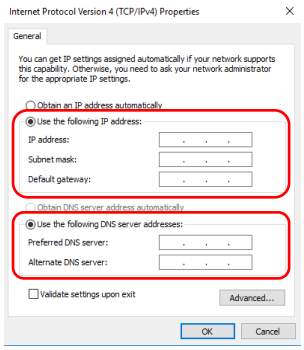
When a fixed IP address or DNS is set for the following options, add a CPU board by the following procedure.
(The procedure is necessary to take over the fixed IP address setting even after the CPU expansion.)

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 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 (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)".

● Note on using 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

● Notes for using TPM in VMware ESXi

If your system has TPM kit (N8115-35) and OS is VMware ESXi with System ROM Version v 2.00 (02/02/2019) or later, 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

● Change of RAID monitoring and reporting method

If VMware ESXi uses N8103-189/190/191/192/193/194/195/196/201/237/238/240 RAID controller and N8103-239 SSD Adapter for OS Boot, the RAID monitoring report will be changed to snmp trap reporting.
For details, please check the following website.
NEC Support Portal
http://www.58support.nec.co.jp/global/download/N8103-239/WBEM_uninstall_en.pdf

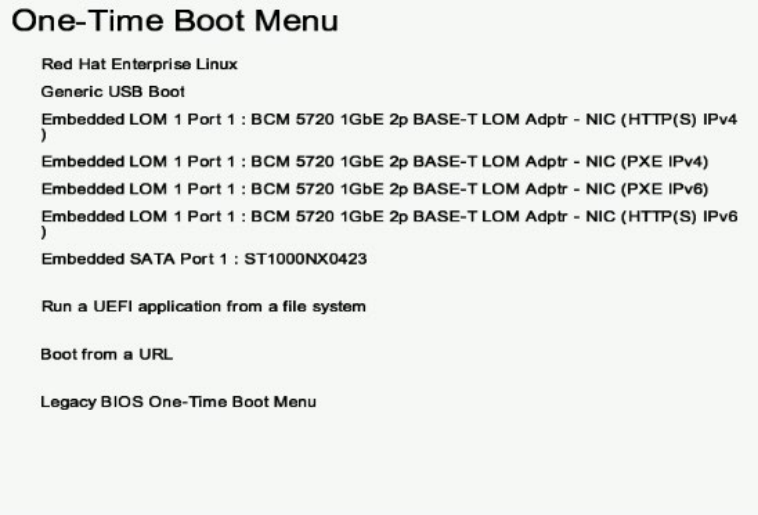
● Cautions on using Linux OS

Use the device name of LOM or optional NIC which the OS automatically recognizes. When adding a unique udev rule, do not change or fix the NIC device name based on the PCI address.
In addition, do not use the storage device name under /dev/disk/by-path/ that includes the PCI address.

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

● Cautions on using Red Hat Enterprise Linux 8.5 or earlier

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).



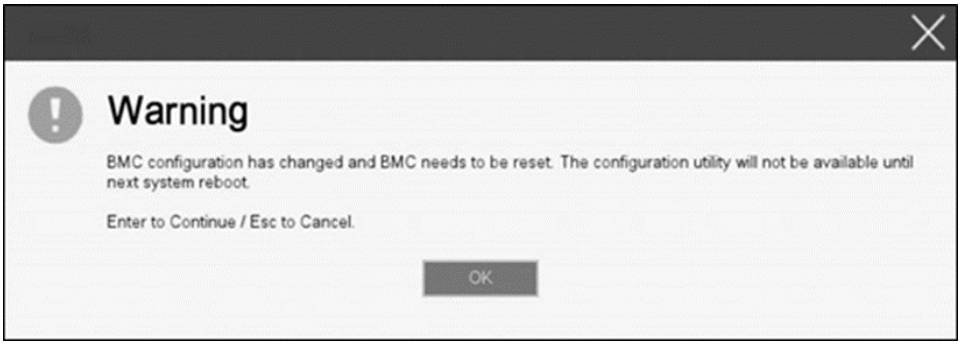
One-Time Boot Screen

5) Notice of the function in general

● Caution for operating BMC Configuration Utility in the System Utilities

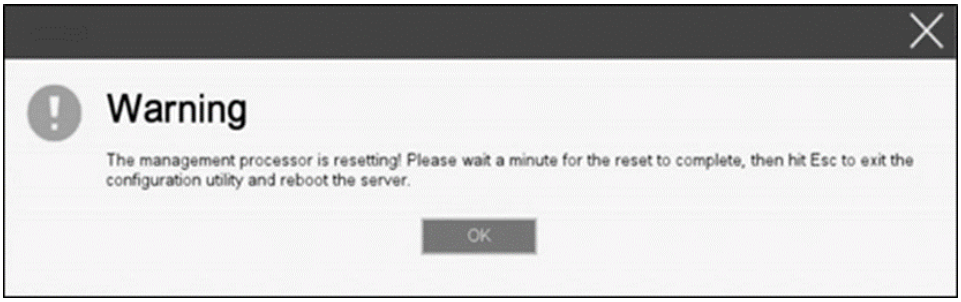
If you execute POST or change the BMC configuration while rebooting the iLO, some server settings such as Serial Number and Product ID may be lost.
In addition, there is a possibility that it does not operate normally in the restart process immediately after.
To avoid this trouble in rebooting the iLO, 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:
(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]

・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)]

※ 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 Upate / 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)

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.

● 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

When you select S**ystem Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options** from the System Utilities, the Power and Performance Options menu appears.
For details about the additional options, see the table below.

Option	Parameter	Description
Energy Performance Preference	[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	[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	[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.

NEC
Feb 2024 18th Edition

* CBZ-036500-001-16 *