Express5800/R120h-1M, R120h-2M　ご使用時の注意事項

このたびは弊社製品をお買い上げいただき、誠にありがとうございます。
本製品のご使用において、ご注意いただくことがあります。誠におそれ入りますが、ご使用前に下記内容を必ずご一読ください。
なお、本書は必要なときにすぐに参照できるよう大切に保管してください。

1) はじめに

● 本製品のマニュアルについて

本製品に関する詳細は、以下の Web サイトに掲載しているマニュアルに記載しています。
https://www.support.nec.co.jp/
「NEC サポートポータル内検索」より、以下の ID で検索してください。
R120h-1M : 3170101948
R120h-2M : 3170101949

また、ESMPRO/ServerManager、ESMPRO/ServerAgentService、エクスプレス通報サービス/エクスプレス通報サービス(HTTPS)/エクスプレス通報サービス(MG)に関しては、
ESMPRO 日本語ポータルサイト<https://jpn.nec.com/esmsm/>
NEC サポートポータル　<https://www.support.nec.co.jp/View.aspx?id=9010102124>
の最新の情報およびバージョンをご確認のうえ、ご利用ください。

● Starter Pack について

本製品で使用する Starter Pack は、以下の Web サイトに最新版が掲載されています。
Web サイトに掲載されている内容を確認し、バージョン S8.10-001.01 以降を適用してください。
https://www.support.nec.co.jp/
(「NEC サポートポータル内検索」より、「S8.10-001」を検索)

● VMware ESXi のドライバ・サービスモジュールについて

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

(1) Agentless Management Service および iLO Channel Interface Driver
https://www.support.nec.co.jp/
(「NEC サポートポータル内検索」より、「Agentless Management Service」を検索し、【最新版】と表示される「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=0, 5 または 7), 7.0 版)」を適用してください)

(3) VMware ESXi デバイスドライバ
https://www.support.nec.co.jp/View.aspx?id=3140105866
（「PC サーバ/ブレードサーバ(Express5800 シリーズ)」から対象 OS の「デバイスドライバー覧」を選択）

● 本製品の保守作業時間に関して

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

2) システム ROM の機能に関する注意事項

● **UEFI Boot Order Control の注意事項**

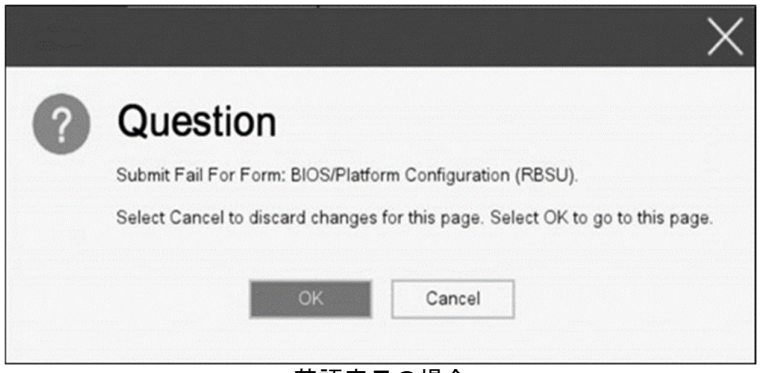
システム ROM バージョン 3.34 の場合、UEFI Boot Order Control メニュー(*1)で新たなブートデバイスの有効化、または無効化の設定や保存ができません。
詳細は以下の Web サイトを確認してください。
https://www.support.nec.co.jp/View.aspx?id=3140109992

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。

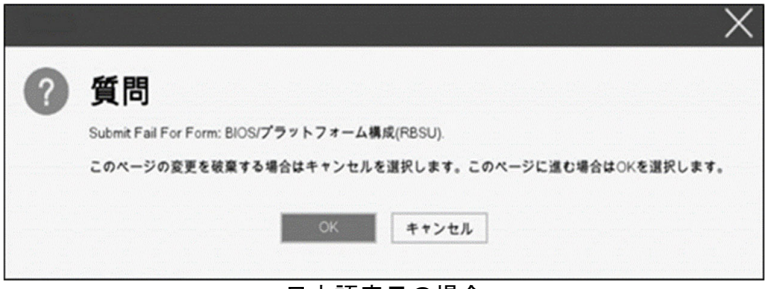
(*1)BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control
(*2)BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order

● **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

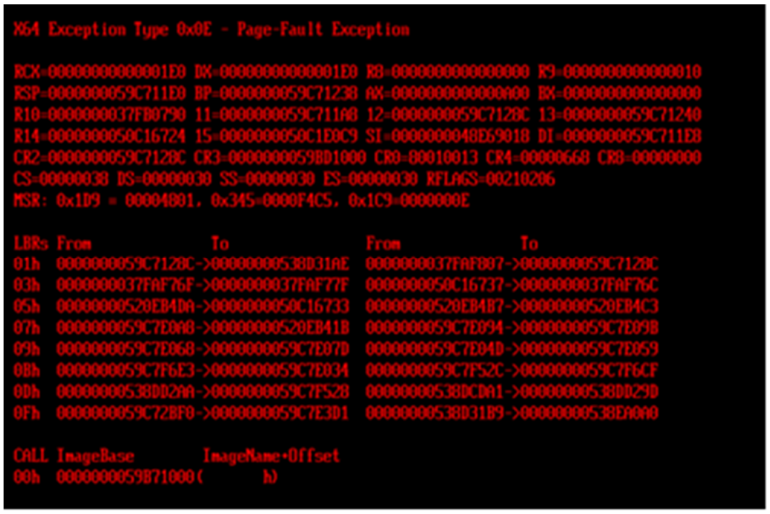


日本語表示の場合

● **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 OFF/ON によって回復します。

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



赤文字画面の例

● **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し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。

a) 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。
b) 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(7.3.3 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)。

● フォールトトレラントメモリ機能(ADDDC)の仕様変更について

本製品の搭載ファームウェアの更新に伴い、フォールトトレラントメモリ機能(ADDDC)の仕様に変更があります。
下記、変更点を記載します。

- システム ROM バージョン 2.00 (02/02/2019)以降、CPU あたり DIMM 8 枚、もしくは DIMM 12 枚以外の構成であっても、フォールトトレラントメモリ機能(ADDDC)が使用できる構成であれば、本機は自動的に設定変更し、同機能の使用を始めます。
- システム ROM バージョン 2.10 (05/21/2019)以降、各チャネルあたりの RANK 数の合計が 2 以上になるようにメモリを搭載しなくても、フォールトトレラントメモリ機能(ADDDC)は利用できます。
- システム ROM バージョン 2.10 (05/21/2019)以降、フォールトトレラントメモリ機能(ADDDC)が使用可能な DIMM として、N8102-709 が加わります。

● 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 2.00 (02/02/2019)以降、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 1024000 バイトに換算した数値で表示されます。
システム ROM バージョン 2.00 (02/02/2019)以降の場合は、1MB を 1048576 バイトに換算した数値で表示されます。
(3) システム ROM バージョン 1.36 (02/14/2018)、またはバージョン 1.36 (02/15/2018)の場合、システムユーティリティ、またはワンタイムブートメニューを表示したとき、まれにマウスカーソルが黒い四角形の表示となることがあります。
これは、表示のみの問題であり、システムユーティリティ上の操作は正常に機能します。
また、この状態はマウスを操作することで解消します。
(4) 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

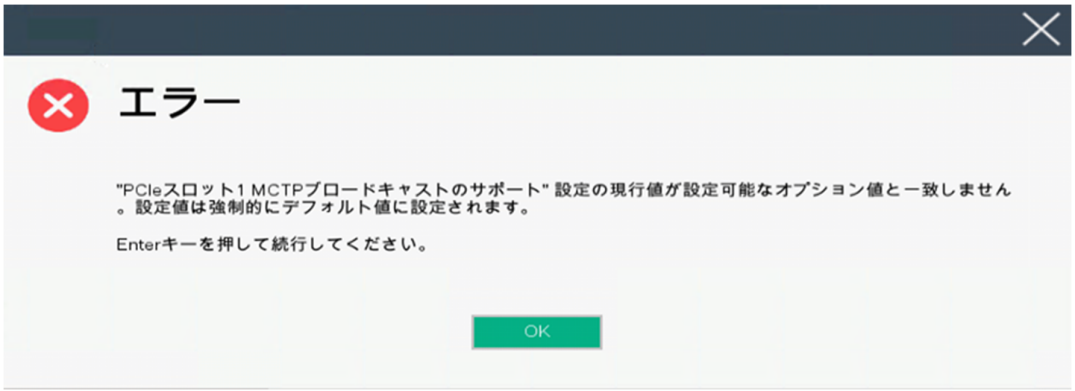
【発生条件】
・N8103-189、N8103-190、N8103-191、N8103-192、N8103-193、N8103-194、N8103-195、N8103-196、N8103-197、N8103-201、N8103-237、N8103-238 の場合
以下 2 つの条件をすべて満たす場合、発生します。
1. RAID コントローラファームウェアが v4.11 以降、または v3.01.04.072 以降
2. システム ROM がバージョン 2.68 (07/14/2022)未満

● **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

iLO5 ファームウェアバージョン 1.40 以降で iLO の拡張ライセンスがインストールされている場合、[Security] > [Access Settings] > [Update Service] > [Downgrade Policy]の設定を『Permanently disallow downgrades』に変更しないでください。
『Permanently disallow downgrades』に設定した場合、ファームウェアのダウングレードを行うことができなくなります。また、iLO に対して永続的な変更が行われるため、『Permanently disallow downgrades』に設定後は、iLO の各種インターフェイスや各種ユーティリティから本設定の変更を行おうとしても変更することができません。
なお、本設定は Set to factory defaults オプションから iLO を出荷時のデフォルト設定にリセットを行った場合においても、リセットされず『Permanently disallow downgrades』を維持します。

● iLO のセキュリティ機能の注意事項

iLO5 ファームウェアバージョン 1.40 以降をご使用の場合、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「**システムユーティリティより、Admin Password を設定(※1)した場合や、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(※2)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。
iLO5 ファームウェアのバージョンによって該当する条件が異なります。

iLO5 ファームウェアバージョン	該当条件
バージョン 1.40	(※1)、および(※2)
バージョン 1.43 以降	(※2)

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。

● **システムユーティリティより、Admin Password を設定(※1)した場合や、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(※2)に設定した場合の注意事項**

(※1) iLO5 ファームウェアバージョン：1.43 未満を適用した環境の場合が対象となります。
[System Configuration] > [BIOS/Platform Configuration (RBSU)] > [Server Security]より、Set Admin Password オプションにてパスワードを設定する。
(※2) 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 の時刻についての注意事項**

iLO5 ファームウェアバージョン 1.45 未満で iLO の SNTP の設定が無効の場合、iLO の再起動を行うと iLO の時刻がずれてしまう場合があります。
iLO の時刻設定は、iLO Web インターフェイスにて 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、iLO5 ユーザーズガイドを参照してください。

● **iLO Web インターフェイスのネットワーク情報の表示について**

iLO5 日本語言語パック：1.40 をご使用の場合、ファイバーチャネルコントローラーが実装されているシステムで、iLO Web インターフェイスの言語に日本語が選択されていると、[システム情報] > [ネットワーク]で表示されるファイバーチャネルコントローラーの"ポートのステータス"が『下へ』と表示されます。
これはファイバーチャネルコントローラーの接続が『ダウン』の状態であることを示しますので、読み替えてご利用ください。

● **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。

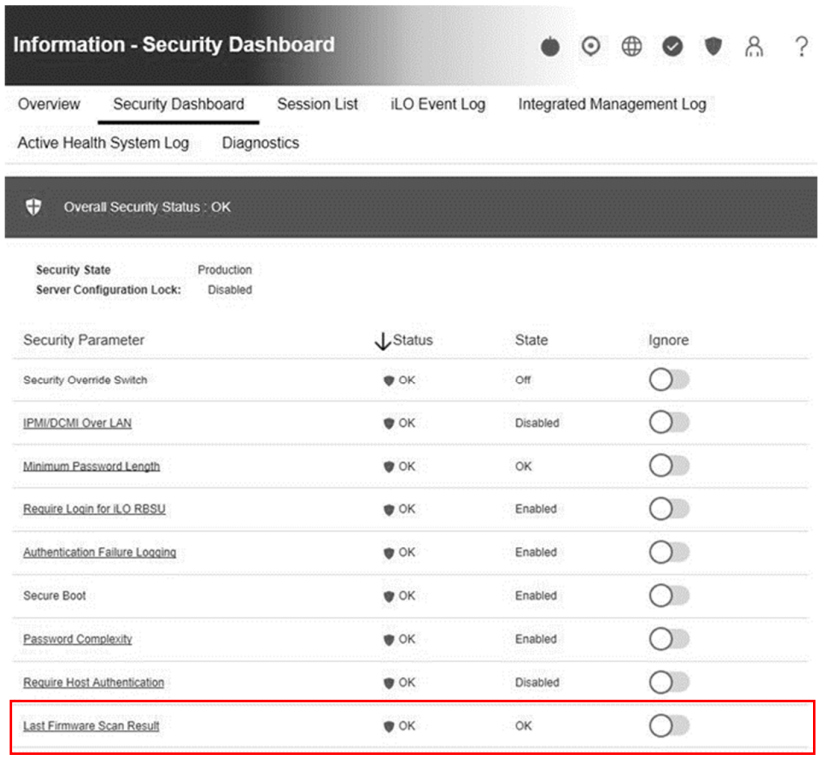
"Failed to retrieve complete storage device information. Refresh the page in a few minutes. "

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 1.43 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。

日本語表示の場合



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: 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
```

・ 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。

・ ESXi 7.0/8.0 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 環境での Agentless Management Service (AMS)の注意事項**

Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 の環境に Agentless Management Service (AMS) version 1.40.0.0 がインストールされている場合、ams.exe プロセスがハンドル数の増加を示します。
ハンドルリークはメモリの過剰消費により時間の経過とともにパフォーマンスの問題を引き起こす可能性があります。

◆本事象は Agentless Management Service (AMS) 1.43.0.0 で修正されています。
AMS は Starter Pack に含まれています。Starter Pack Version S8.10-006.03 以降を適用してください。
すでに AMS 1.40.0.0 がインストールされている環境で Starter Pack Version S8.10-006.03 を使用する場合は、個別に AMS をアップデートする必要があります。Starter Pack が掲載されている Web サイトの内容を確認してアップデートしてください。

◆Agentless Management Service (AMS) 1.40.0.0 を使用される場合は、一度以下の手順を実施することでハンドル数は増加しなくなります。
(1) 以下のコマンドをコマンドプロンプトで実行して AMS を停止します。
　>net stop ams
(2) "C:¥Program Files¥OEM¥AMS¥Service"ディレクトリをエクスプローラで開きます。
(3) "storelib.dll"のファイル名を"storelib.dll.bak"に変更します。
(4) 以下のコマンドをコマンドプロンプトで実行して AMS を開始します。
　>net start ams

(※1) AMS 停止時に以下のメッセージが表示されることがありますが問題ありません。
　Agentless Management Service サービスを停止中です..
　システム エラーが発生しました。
　システム エラー 1067 が発生しました。
　プロセスを途中で強制終了しました。
　Agentless Management Service サービスは正常に停止されました。
(※2) AMS 起動時に以下のメッセージが表示されることがありますが問題ありません。
　要求したサービスは既に開始されています。

◆Agentless Management Service (AMS)のバージョンの確認方法には以下の 2 つの方法があります。
・対象装置の OS 上で確認する方法
(1) Windows PowerShell を起動して以下のコマンドを実行します。
　> Get-WmiObject Win32_Product | Select-Object Name,Version | Select-String "Agentless Management Service"
(2) コマンド実行結果からバージョンを確認します。

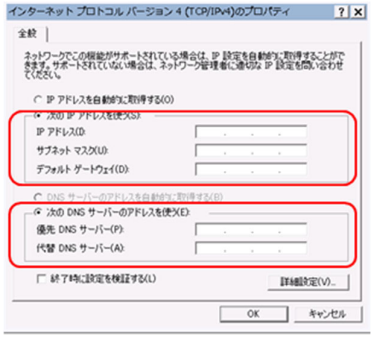
・iLO Web インターフェイスを利用して、リモートから確認する方法
(1) リモート環境において、Web ブラウザーから iLO Web インターフェイスにログインします。
(2) 左メニューの「ファームウェア & OS ソフトウェア」を選択し、「ソフトウェア」を選択します。
(3) 画面の「Product Related Software」の「ams.exe」のバージョンを確認します。

● **Windows Server 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)。

N8104-173 10GBASE-T 接続 LOM カード(2ch)
N8104-177 25GBASE 接続 LOM カード(SFP28/2ch)
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。

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

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

(1) 以下の Web サイトより ESMPRO Platform Management Kit をダウンロードします。
https://www.support.nec.co.jp/View.aspx?id=9010109532
ESMPRO/ServerManager Ver.7 は ESMPRO Platform Management Kit に含まれています。
(2) ESMPRO Platform Management Kit の ESMPRO インストールツールを起動します。
(3) インストールツール画面の説明書をクリックし、Software Manuals から ESMPRO/ServerManager をクリックします。
(4) 「ESMPRO/ServerManager Ver.7 インストレーションガイド(Windows 編)」をクリックします。
(5) 「ESMPRO/ServerManager Ver.7 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager を Ver.6 から Ver.7 へアップデートします。

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

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

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

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

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

◆iLO 管理機能向けの受信情報設定ファイルのバージョン確認方法
「エクスプレス通報サービス(MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で「詳細情報」の「iLO SNMP Trap」のバージョン情報を確認します。

● 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) 下記のような Heartbeat Lost センサーの表示が『警告(黄色)』となる場合があります。
[Device] I/O Module (n) LOM_Link_P (n) : Heartbeat Lost-Assert
[Device] I/O Module (n) NIC_Link_P (n) : Heartbeat Lost-Assert
※n : LAN ポート番号の P1～4 を示します。

<iLO5 ファームウェアバージョン 1.30、1.35、1.38 が適用された環境>
ESXi 起動完了後、Heartbeat Lost 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、LAN ケーブルが接続されたポートは数分お待ちいただくと『警告(黄色)』から『正常(緑色)』に遷移しますので、しばらくお待ちください。LAN ケーブルが接続されていないポートは『警告(黄色)』を継続しますが、運用上問題ありませんのでそのままご使用ください。
なお、LAN ケーブルが接続された環境で『警告(黄色)』が表示され続けた場合は、LAN ケーブルの接続不良の可能性が考えられますので LAN 結線等を再確認してください

<iLO5 ファームウェアバージョン 1.40 以降が適用された環境>
ESXi 起動完了後、Heartbeat Lost 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、数分お待ちいただくと『警告(黄色)』から『標準(緑色)』に遷移しますので、しばらくお待ちください。

(2) システム ROM バージョン 2.16 (05/25/2020)未満の場合、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

(3) 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 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 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 において、N8103-189/190/191/192/193/194/195/196/201/237/238 RAID コントローラと N8103-239 OS ブート専用 SSD ボードをご使用されている場合、RAID 監視通報は SNMP Trap による通報に変更になります。
詳細は、下記の Web サイトをご確認ください。
・NEC サポートポータル
https://www.support.nec.co.jp/View.aspx?&id=3140108419

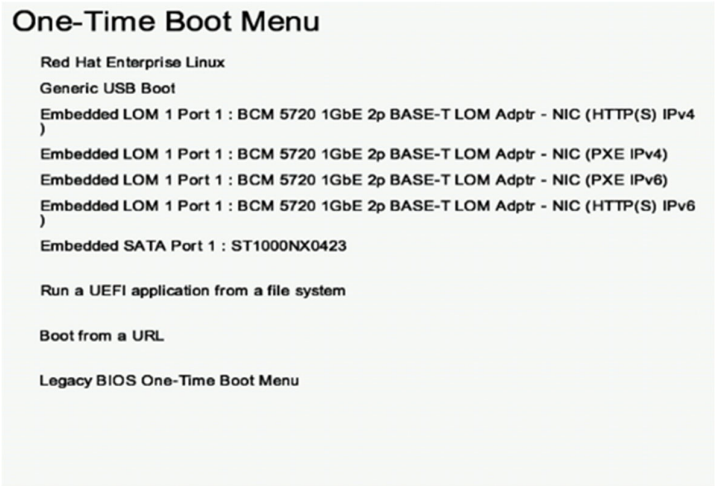
● **Linux OS を使用する場合の注意事項**

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

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

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

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



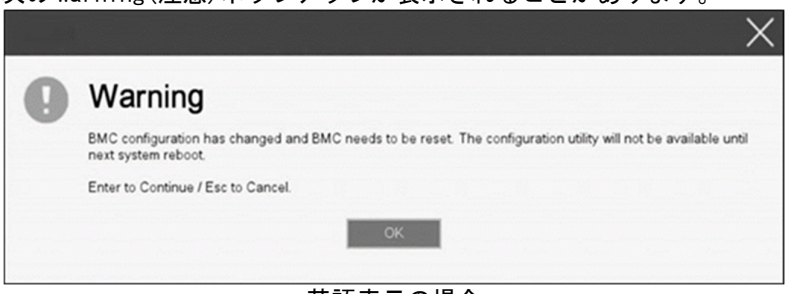
ワンタイムブートメニュー画面

5) 全般の機能に関する注意事項

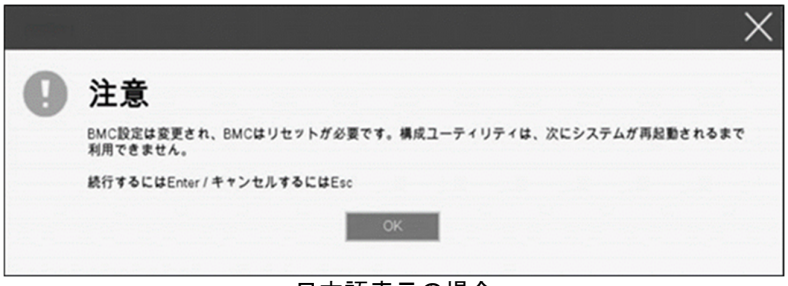
● **システムユーティリティの「BMC Configuration Utility」の操作についての注意事項**

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。

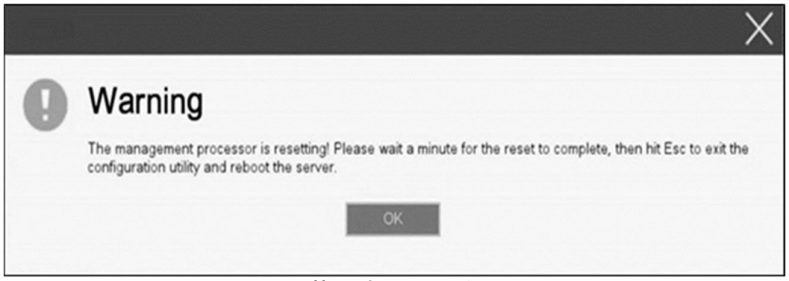


英語表示の場合

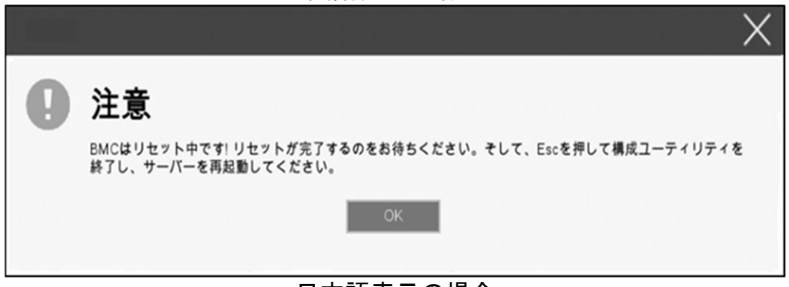


日本語表示の場合

(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(7.3.3 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、『N8100-2557Y』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 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

◆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。

● **Smart Storage Battery について**

Smart Storage Battery は、RBSU メニューなどで Energy Pack と表示されることがあります。
適宜、読み替えてください。

● **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 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

● **データバックアップ時の注意事項**

FC コントローラ配下に接続されたデバイスが誤って本体内蔵のマイクロ SD カードスロットとして認識されてしまう場合や、iStorage を接続しての自動バックアップ中に空の本体内蔵のマイクロ SD カードスロットを検出して認識されてしまい警告メッセージをポップアップして一時停止する場合があります。
これらにより正常にデータのバックアップを行えないことがありますので、工場出荷時に以下の手順によって、本体内蔵のマイクロ SD カードスロットを無効化しています。
本体内蔵の SD カードスロットは使用しませんので、無効化しても通常のサーバー動作には支障ありません。

◆設定手順

システムユーティリティの BIOS/Platform configuration (RBSU)メニューから System Options > USB Options > Internal SD Card Slot を「Disabled」に設定。

● **LOM カード FCoE 機能のサポートについて**

本製品では FCoE (FibreChannel over Ethernet)機能を NEC としてサポートしておりません。
N8104-173 では LOM カードに適用されているファームウェアバージョンに関わらず、N8104-177 では Family Firmware Version 8.35.43 以降で FCoE 機能が有効化されています。
OS 上で FCoE デバイスとして認識されますが、OS やドライバで機能利用の設定をしないことで、運用上の影響はありません。
以下のデバイスの検出は無視していただいて構いません。

-HPE 533FLR-T FCoE Device
-HPE 622FLR-SFP28 FCoE Device

● **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：N8100-2557Y → N8100-2557H1Y

● **N8104-173 10GBASE-T 接続 LOM カード(2ch) Wake On LAN 機能のサポートについて**

N8104-173 10GBASE-T 接続 LOM カード(2ch)のポート 2 側で Wake On LAN 機能を使用する場合は、ファームウェアバージョン 7.19.2 以降をご使用ください。

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 以降にて利用できるオプションです。

(2) Memory Options メニュー
システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options」を選択すると、「Memory 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
Memory Controller Interleaving(注1)	[Auto] Disabled	メモリコントローラー間のインターリーブ動作を選択します。 「Auto」を選択した場合、メモリコントローラー間のインターリーブ動作は本機のメモリ構成に応じて自動的に設定されます。 「Disabled」を設定した場合、メモリコントローラー間のインターリーブ動作は強制的に無効に設定されます。 本オプションは、「Auto」で利用することを推奨します。
Opportunistic Self-Refresh(注2)	[Disabled] Enabled	「Opportunistic Self-Refresh」を「Enabled」に設定した場合、メモリがアイドル状態になった場合にメモリのセルフリフレッシュを行います。 [Disabled」の場合は通常のリフレッシュを行います。

[ ]: 出荷時の設定

注 1：システム ROM バージョン 1.40 以降にて追加されるオプションです。
注 2：システム ROM バージョン 1.36 以降にて追加されるオプションです。

(3) 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3.34以降にて利用できるパラメーターです。

(4) Intel UPI 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 > Intel UPI Options」を選択すると、「Intel UPI 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
Direct To UPI (D2K) (注1)	[Auto] Enabled Disabled	「Direct To UPI (D2K)」を「Enabled」にすると、Last Level Cacheのキャッシュミスによるレイテンシーを軽減します。指定されないかぎり、設定変更しないでください。 複数プロセッサー構成の場合のみ表示されます。

[ ]: 出荷時の設定

注1：システムROMバージョン1.36以降にて追加されるオプションです。

(5) Advanced Performance Tuning Options メニュー

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

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Processor Jitter Control Optimization (注1)	Optimized for Throughput Optimized for Latency [Zero Latency]	本オプションは指定がある場合を除いて、出荷時設定から変更しないでください。 このオプションは、プロセッサー周波数変動の自動調整機能の閾値を最適化します。 「Optimized for Throughput」を選択すると、総合的な計算処理能力に影響しない変動を許容した制御をします。 「Optimized for Latency」を選択すると、プロセッサー周波数を下げるときに微小変動があることを許容した制御をします。 「Zero Latency」を選択すると、周波数変動を取り除くように制御します。
IODC Configuration (注2)	[Auto] Enable for Remote InvItoM Hybrid Push InvItoM AllocFlow InvItoM Hybrid AllocFlow Enable for Remote InvItoM and Remote WCiLF	本オプションは指定ある場合をのぞいて、出荷時設定から変更しないでください。 IODC (IO Direct Cache)の構成を設定します。 このオプションにより、I / O トランザクションがプロセッサキャッシュと通信するためのポリシーを調整できます。

[ ]: 出荷時の設定

注1：システムROMバージョン1.40以降にて追加されるオプションです。
注2：システムROMバージョン2.10以降にて追加されるオプションです。

(6) 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 バージョン 2.54 以降にて利用できるパラメーターです。

(a) Advanced Trusted Platform Module Options メニュー

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

追加のオプションについて、次の表を参照してください。

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

[ ]: 出荷時の設定

注 1:システム ROM バージョン 2.80 以降にて利用できるパラメーターです。

(7) PCIe Device Configuration メニュー

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

追加のメニューについて、次の表を参照してください。

オプション	パラメーター	説明
Advanced PCIe Configuration (注1)	-	-

注1:システムROMバージョン1.40以降にて追加されるオプションです。

(a) Advanced PCIe Configuration メニュー

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

追加のメニューについて、次の表を参照してください。

オプション	パラメーター	説明
PCIe Bifurcation Options (注1)	-	-
PCIe MCTP Options (注2)	-	-

注1:システムROMバージョン1.36以降にて利用できるメニューです。
注2:システムROMバージョン2.10以降にて利用できるメニューです。

① PCIe Bifurcation Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Bifurcation Options」を選択すると、「PCIe Bifurcation 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
PCIe Slot XX Bifurcation (注1)	[Auto] Slot Bifurcated	PCIe Slotに実装するPCIe拡張カードがSlot Bifurcation機能をサポートする場合、必要に応じて「Slot Bifurcated」を設定してください。 「Auto」を設定すると、PCIe Slotは、サポートされる最大幅で接続されます。 「Slot Bifurcated」を設定すると、PCIe Slotと拡張カード間の接続が、2個に分割されます。 XX: 1/2/3... (CPU数やライザーカード種類に応じて表示が変わります。)

[ ]: 出荷時の設定

注1:システムROMバージョン1.36以降にて利用できるメニューです。

② PCIe MCTP Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options」を選択すると、「PCIe MCTP 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
PCIe Slot XX MCTP Broadcast Support (注1)	[Enabled] Disabled	PCIe Slotに実装するPCIe拡張カードがSlot Bifurcation機能をサポートする場合、必要に応じて「Slot Bifurcated」を設定してください。 「Auto」を設定すると、PCIe Slotは、サポートされる最大幅で接続されます。 「Slot Bifurcated」を設定すると、PCIe Slotと拡張カード間の接続が、2個に分割されます。 XX: 1/2/3... (CPU数やライザーカード種類に応じて表示が変わります。)

[ ]: 出荷時の設定

注1:システムROMバージョン2.10以降にて利用できるメニューです。

(8) Fan and Thermal Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options」を選択すると、「Fan and Thermal Options」メニューが表示されます。
オプションのパラメーター追加について、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
Thermal Configuration (注1)	[Optimal Cooling] Increased Cooling Maximum Cooling Enhanced CPU Cooling	本機のファン冷却方法を選択します。 「Optimal Cooling」は、適切な冷却を可能にする必要最小限のファン速度に設定することで、最も効率的な冷却方法を実現します。 「Increased Cooling」ではファンを高速で回転させ、冷却能力を高めます。「Increased Cooling」は、他社製のストレージコントローラーが内蔵ハードドライブケージにケーブル接続されている場合、または本機の高温の問題をほかの方法で解決できない場合に使用します。 「Maximum Cooling」は、ファンを最高速で回転させ、最も高い冷却方法を実現します。 「Enhanced CPU Cooling」は、プロセッサーの冷却をより強化します。プロセッサーに負荷のかかるワークロードを実行する場合、プロセッサーの冷却強化により、 パフォーマンスが改善する場合があります。

[ ]: 出荷時の設定

注 1:システム ROM バージョン 1.36 以降にて追加されるオプションです。

(9) Advanced Debug Options メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Debug Options」を選択すると、「Advanced Debug 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
Advanced Crash Dump Mode(注1)	[Disabled] Enabled	本オプションは指定ある場合を除き、出荷時設定から変更しないでください。 「Enabled」に設定した場合、システムがクラッシュした場合に、AHS ログに追加のデバッグ情報を記録するようにシステムを構成します。

[ ]: 出荷時の設定

注 1:システム ROM バージョン 1.40 以降にて追加されるオプションです。

(10) Embedded Applications メニュー

システムユーティリティから、「Embedded Applications」を選択すると、「Embedded Applications」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
Embedded Diagnostics(注1)	ー	本機ではサポートされません。

[ ]: 出荷時の設定

注 1:システム ROM バージョン 1.36 以降にて追加されるオプションです。

B) 誤記訂正

■ Express5800/R120h-1M　ユーザーズガイドについて

ユーザーズガイドに誤記がありましたので、以下に訂正いたします。

<table>
<tr><th></th><th>誤</th><th>正</th></tr>
<tr><td>2章 準備
1.10.7 メモリ機能について
(1) メモリミラーリング機能</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Advanced Memory Protection」を「Mirrored Memory with Advanced ECC Support」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection」を「Mirrored Memory with Advanced ECC Support」に設定してください。</td></tr>
<tr><td>2章 準備
1.10.7 メモリ機能について
2) メモリスペアリング機能</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection」を「Online Spare with Advanced ECC Support」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection」を「Online Spare with Advanced ECC Support」に設定してください。</td></tr>
<tr><td>2章 準備
1.10.7 メモリ機能について
(3) フォールトトレラントメモリ機能(ADDDC)</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection」を「Fault Tlerant Memory ADDDC)」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection」を「Fault Tolerant Memory (ADDDC)」に設定してください。</td></tr>
<tr><td>2章 準備
1.32.1 RAID システム構築時の注意事項</td><td>● オプションのRAID コントローラー(N8103-189/195)を使用する場合、RAID 5、RAID 6、RAID 50、RAID 60のRAIDシステムは構築できません。
<table><tr><th rowspan="2">RAID レベル</th><th colspan="2">RAIDシステム構築に必要となるハードディスクドライブの最小数</th></tr><tr><th>N8103-189/192/195</th><th>N8103-190/191/193/194/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td></td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>3</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>6</td></tr></table></td><td>オプションのRAID コントローラー(N8103-189/192/195)を使用する場合、RAID 6、RAID 50、RAID 60のRAIDシステムは構築できません。
<table><tr><th rowspan="2">RAID レベル</th><th colspan="2">RAIDシステム構築に必要となるハードディスクドライブの最小数</th></tr><tr><th>N8103-189/192/195</th><th>N8103-190/191/193/194/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td>3</td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>4</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>8</td></tr></table></td></tr>
<tr><td>3章 セットアップ
2.4 設定が必要なケース
>メモリ関連
>メモリ RAS 機能を使う</td><td>[System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Oprations] - [Advanced Memory Protection]を設定してください。</td><td>[System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options] > [Advanced Memory Protection]を設定してください。</td></tr>
<tr><td>サポート OS</td><td>VMware ESXi™ 6.7 Update1 以降</td><td>VMware ESXi™ 6.7 Update2 以降</td></tr>
<tr><td>搭載 CPU</td><td>Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td><td>Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td></tr>
</table>

■ Express5800/R120h-1M　ユーザーズガイドについて

ユーザーズガイドに誤記がありましたので、以下に訂正いたします。

<table>
<tr><th></th><th>誤</th><th>正</th></tr>
<tr><td>2章 準備
1.11.7 メモリ機能について
(1) メモリミラーリング機能</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Advanced Memory Protection」を「Mirrored Memory with Advanced ECC Support」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection」を「Mirrored Memory with Advanced ECC Support」に設定してください。</td></tr>
<tr><td>2章 準備
1.11.7 メモリ機能について
2) メモリスペアリング機能</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection」を「Online Spare with Advanced ECC Support」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Opions > Advanced Memory Protection」を「Online Spare with Advanced ECC Support」に設定してください。</td></tr>
<tr><td>2章 準備
1.11.7 メモリ機能について
(3) フォールトトレラントメモリ機能(ADDDC)</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection」を「Fault Tlerant Memory ADDDC)」に設定してください。</td><td>システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection」を「Fault Tolerant Memory ADDDC)」に設定してください。</td></tr>
<tr><td>2章 準備
1.32.1 RAID システム構築時の注意事項</td><td>● オプションのRAID コントローラー(N8103-189/195)を使用する場合、RAID 5、RAID 6、RAID 50、RAID 60のRAIDシステムは構築できません。
<table><tr><th rowspan="2">RAID レベル</th><th colspan="2">RAIDシステム構築に必要となるハードディスクドライブの最小数</th></tr><tr><th>N8103-189/195</th><th>N8103-190/191/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td></td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>3</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>6</td></tr></table></td><td>オプションのRAID コントローラー(N8103-189/192/195)を使用する場合、RAID 6、RAID 50、RAID 60のRAIDシステムは構築できません。
<table><tr><th rowspan="2">RAID レベル</th><th colspan="2">RAIDシステム構築に必要となるハードディスクドライブの最小数</th></tr><tr><th>N8103-189/195</th><th>N8103-190/191/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td>3</td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>4</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>8</td></tr></table></td></tr>
<tr><td>3章 セットアップ
2.4 設定が必要なケース
>メモリ関連
>メモリ RAS 機能を使う</td><td>[System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Oprations] - [Advanced Memory Protection]を設定してください。</td><td>[System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options] > [Advanced Memory Protection]を設定してください。</td></tr>
<tr><td>サポート OS</td><td>VMware ESXi™ 6.7 Update1 以降</td><td>VMware ESXi™ 6.7 Update2 以降</td></tr>
<tr><td>搭載 CPU</td><td>Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td><td>Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td></tr>
</table>

■ Express5800/R120h-1M,R120h-2M,　メンテナンスガイドについて

メンテナンスガイドに誤記がありましたので、以下に訂正いたします。

	誤	正
2章 便利な機能 1.2.2 BIOS/Platform Configuration (RBSU) (3) Memory Options 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 > Memory Oprations」を選択すると、「Memory Options」メニューが表示されます。	システムユーティリティから、 「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options」を選択すると、 「Memory Options」メニューが表示されます。
2章 便利な機能 1.2.2 BIOS/Platform Configuration (RBSU) (3) Memory Options メニュー (a) Persistent Memory Options 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 > Memory Oprations > Persistent Memory Options」を選択すると、 「Persistent Memory Options」メニューが表示されます。	システムユーティリティから、 「System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options」を選択すると、 「Persistent Memory Options」メニューが表示されます。
2章 便利な機能 1.2.2 BIOS/Platform Configuration (RBSU) (8) Power and Performance Optionsメニュー (e) Advanced Power Optionsメニュー Redundant Power Supply Mode	システムによる電源の冗長構成の処理方法を設定するには、このオプションを使用します。 「Balanced Mode」では、搭載されているすべての無停電電源装置(UPS)間で電源供給を等しく共有します。すべての「High Efficiency Mode」パラメーターは、スタンバイモードのUPS の半分を低消費電力レベルに保つことで、電源効率の高い動作のほとんどに冗長化電源を提供します。「High Efficiency Mode」のパラメーターでは、スタンバイにするUPS をシステムが選択することを可能にします。 「Auto」では、システムグループ内のセミランダムな分布に基づいて奇数または偶数のUPS をシステムが選択することを可能にします。	システムの電源冗長構成の効率モードの設定を行うには、本オプションを使用します。 「Balanced Mode」では、搭載されているすべて(本モデルは最大2台)の電源間で電源供給を等しく共有します。 「High Efficiency Mode」では、搭載されている片側の電源をスタンバイモードにすることにより、低消費電力レベルを保ち、冗長化電源の効率を向上させます。 「High Efficiency Mode」は、スタンバイモードに設定する電源を電源ユニット番号の「奇数(Odd Supply Standard)」、「偶数(Even Supply Standard)」を選択することで指定することができます。 「Auto」設定では、システムグループ内のセミランダムな分布に基づいて、システムが電源ユニット番号の「奇数」、「偶数」を自動で指定します。

■ メモリ搭載順序の訂正

2019年2月版より旧版のユーザーズガイドにおいて、メモリの搭載順序について、誤記がありました。
ついては、下記のように訂正いたします。

修正箇所

・Express5800/R120h-1M ユーザーズガイド
2章 準備 1.10 DIMM 1.10.2 ＤＩＭＭの増設順序

・Express5800/R120h-2M ユーザーズガイド
2章 準備 1.11 DIMM 1.11.2 ＤＩＭＭの増設順序

メモリの搭載順序について

メモリの搭載位置、搭載順序は1CPU構成と2CPU構成、また、メモリの搭載枚数によって異なります。

・CPU1だけ実装している場合のメモリ搭載位置、搭載順序

DIMMスロット番号		1	2	3	4	5	6	7	8	9	10	11	12
メモリ搭載枚数と搭載順序	DIMM 1枚								1				
	DIMM 2枚								1		2		
	DIMM 3枚								1		2		3
	DIMM 4枚			4		3			1		2		
	DIMM 5枚			5		4			1		2		3
	DIMM 6枚	6		5		4			1		2		3
	DIMM 7枚	6		5		4		7	1		2		3
	DIMM 8枚			4	8	3	7	5	1	6	2		
	DIMM 9枚	6		5		4		7	1	8	2	9	3
	DIMM 10枚	6		5	10	4	9	7	1	8	2		3
	DIMM 11枚	6		5	11	4	10	7	1	8	2	9	3
	DIMM 12枚	6	12	5	11	4	10	7	1	8	2	9	3

・CPU1とCPU2を実装している場合のメモリ搭載位置、搭載順序

	DIMM スロット番号	CPU2												CPU1											
		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
メモリ搭載枚数と搭載順序	DIMM 2枚		■		■		■	■	2	■		■			■		■		■	■	1	■		■	
	DIMM 3枚		■		■		■	■	2	■		■			■		■		■	■	1	■	3	■	
	DIMM 4枚		■		■		■	■	2	■	4	■			■		■		■	■	1	■	3	■	
	DIMM 5枚		■		■		■	■	2	■	4	■			■		■		■	■	1	■	3	■	5
	DIMM 6枚		■		■		■	■	2	■	4	■	6		■		■		■	■	1	■	3	■	5
	DIMM 7枚		■		■		■	■	2	■	4	■	6		■	7	■	5	■	■	1	■	3	■	
	DIMM 8枚		■	8	■	6	■	■	2	■	4	■			■	7	■	5	■	■	1	■	3	■	
	DIMM 9枚		■	8	■	6	■	■	2	■	4	■			■	9	■	7	■	■	1	■	3	■	5
	DIMM10枚		■	10	■	8	■	■	2	■	4	■	6		■	9	■	7	■	■	1	■	3	■	5
	DIMM11枚		■	10	■	8	■	■	2	■	4	■	6	11	■	9	■	7	■	■	1	■	3	■	5
	DIMM12枚	12	■	10	■	8	■	■	2	■	4	■	6	11	■	9	■	7	■	■	1	■	3	■	5
	DIMM13枚	12	■	10	■	8	■	■	2	■	4	■	6	11	■	9	■	7	■	13	1	■	3	■	5
	DIMM14枚	12	■	10	■	8	■	14	2	■	4	■	6	11	■	9	■	7	■	13	1	■	3	■	5
	DIMM15枚	12	■	10	■	8	■	14	2	■	4	■	6		■	7	15	5	13	9	1	11	3	■	
	DIMM16枚		■	8	16	6	14	10	2	12	4	■			■	7	15	5	13	9	1	11	3	■	
	DIMM17枚		■	8	16	6	14	10	2	12	4	■		11	■	9	■	7	■	13	1	15	3	17	5
	DIMM18枚	12	■	10	■	8	■	14	2	16	4	18	6	11	■	9	■	7	■	13	1	15	3	17	5
	DIMM19枚	12	■	10	■	8	■	14	2	16	4	18	6	11	■	9	19	7	17	13	1	15	3	■	5
	DIMM20枚	12	■	10	20	8	18	14	2	16	4	■	6	11	■	9	19	7	17	13	1	15	3	■	5
	DIMM21枚	12	■	10	20	8	18	14	2	16	4	■	6	11	■	9	21	7	19	13	1	15	3	17	5
	DIMM22枚	12	■	10	22	8	20	14	2	16	4	18	6	11	■	9	21	7	19	13	1	15	3	17	5
	DIMM23枚	12	■	10	22	8	20	14	2	16	4	18	6	11	23	9	21	7	19	13	1	15	3	17	5
	DIMM24枚	12	24	10	22	8	20	14	2	16	4	18	6	11	23	9	21	7	19	13	1	15	3	17	5

・DIMM混在時の注意

複数種のDIMMを混在させる場合、下記に示す優先度の高いDIMMから、上記表に示した搭載順序に従って、DIMMスロットに実装してください。

（優先度高） N8102-711 → N8102-710 → N8102-714 → N8102-709 → N8102-708（優先度低）

■商標について

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

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

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

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

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

その他、記載の会社名および商品名は各社の商標または登録商標です。

■ 本件に関するお問い合せについて

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

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

NEC

2026年　3月　25版

Precautions for Using Express5800/R120h-1M, R120h-2M

Thank you for purchasing our products.
This document provides the precautions on the use of this product.
Please read through the instructions below and keep this document in a safe place for your future reference.

1) Introduction

● About the manual of this product.

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

< **https://www.58support.nec.co.jp/global/download/** >
-> Document & Software
-> Rack
-> (Select your server model)

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

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

● About Starter Pack

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

< **https://www.58support.nec.co.jp/global/download/** >
-> Document & Software
-> Rack
-> (Select your server model)

● About service and driver modules for VMware ESXi

Please see the following website to check the latest modules.

(1) Agentless Management Service and iLO Channel Interface Driver

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

(2) WBEM Provider and CLI tool

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

● Notice about service operation time of this product

The service operation 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

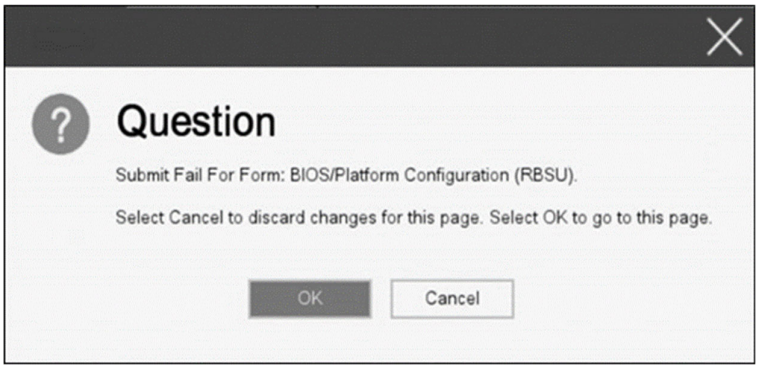
● Note for UEFI Boot Order Control

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

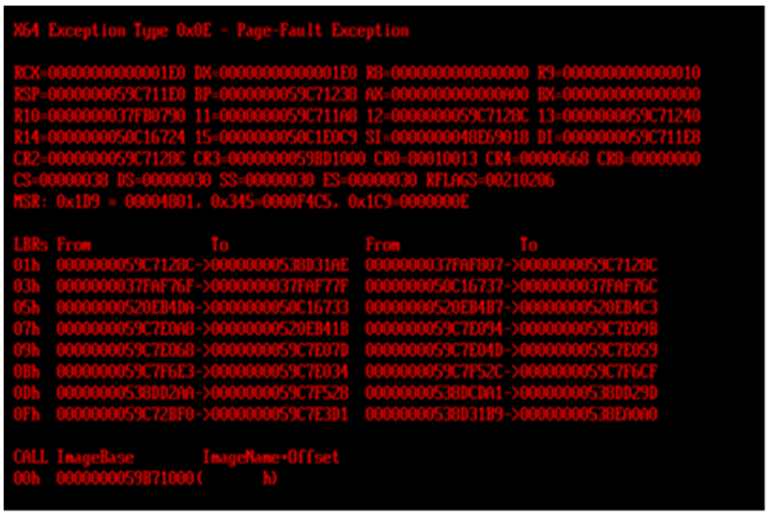
If you encounter the "Submit Fail For Form" Question pop-up while changing the configuration in the System Utilities, **discard the changes by pressing Cancel**. To apply the desired changes after that, reboot the server and re-enter the System Utilities. Selecting OK to continue the changes may cause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



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

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

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



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

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

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

If the RSOD is displayed, power the system OFF/ON, then resolve the cause of the Secure Boot failure (e.g., the boot loader/OS components are outdated and fail verification under the current Secure Boot policy), and then boot from the boot device.
As an example workaround, set Attempt Secure Boot to Disabled, update the OS (or the boot loader/recovery environment) to the latest version, then set Attempt Secure Boot back to Enabled and confirm that the OS starts successfully.
If the issue is not resolved, please contact the First Contact Center.

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

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

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

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

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

This issue has been fixed in System ROM v2.00 (03/06/2024).

● Notes on Boot Order Policy options

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

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

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

● Notes on the Server Configuration Lock (SCL)

(1) Set SCL function to disabled and operate the system.
(2) Set the password when the SCL function is enabled and keep the password in a safe place. If you lose your SCL password and it is locked by the SCL function (stopped before booting the OS), you will not be able to unlock it and you will not be able to boot the server OS again.
You will be charged for recovery / recovery to the bootable state.
If you lose your SCL password, there is no way to clear it.
(3) When you will be requesting maintenance, it is necessary to disable the SCL function.
If you cannot be disabled the SCL function, **maintenance will be a charged one.**
(4) Set "Halt on Server Configuration Lock failure detection." option to disabled and operate the system. If it was enabled, when the SCL function detects an unrecoverable condition and is locked (stopped before the OS boots), the system utility will not be able to start and the server configuration lock will never be disabled.
You will be charged for recovering to the bootable state.
Unrecoverable conditions of SCL function:
- When the server boot is locked by the SCL function due to change in the RBSU settings.
- When the server boot is locked by the SCL function due to the update of firmware, and the original Firmware Version cannot be restored.
- When the server boot is locked by the SCL function due to a failure of the DIMM or PCI option card

● 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 change of specification in Fault tolerant memory function (ADDDC)

Specification of the Fault tolerant memory function (ADDDC) has been changed by firmware update. Change points are below.

- For the System ROM Version 2.00 (02/02/2019) or later
  Even if the system has other than 8 or 12 DIMMs per channel but has the fault tolerant memory function (ADDDC) available configuration, the system will change its setting automatically and starts to use this function.

- For the System ROM Version 2.10 (05/21/2019) or later
  · The Fault tolerant memory function (ADDDC) can be used even if the amount of RANK number per channel does not exceed 2.
  ·N8102-709 becomes ready for use of the fault tolerant memory function (ADDDC).

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

When System ROM Version 2.00 (02/02/2019) or later and 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 1MB is converted into 1024000 bytes.
When the version of System ROM is v2.00 (02/02/2019) or later, it is indicated by converting 1 MB to 1048576 bytes.

(3) In System ROM Version 1.36 (02/14/2018) or 1.36 (02/15/2018), the mouse cursor may be displayed as a black square on rare occasions when System Utilities screen or One-Time Boot menu is shown.
This is merely a problem with indication, and the operation on the System Utilities works normally.
This symptom can be solved by moving the mouse in a usual way.

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

- For N8103-189, N8103-190, N8103-191, N8103-192, N8103-193, N8103-194, N8103-195, N8103-196, N8103-197, N8103-201, N8103-237, or N8103-238
  The above problem occurs if both of the following conditions are met:
  1. The version of the RAID controller firmware is v4.11 or higher, or v3.01.04.072 or higher.
  2. The version of System ROM is lower than v2.68 (07/14/2022).

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

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

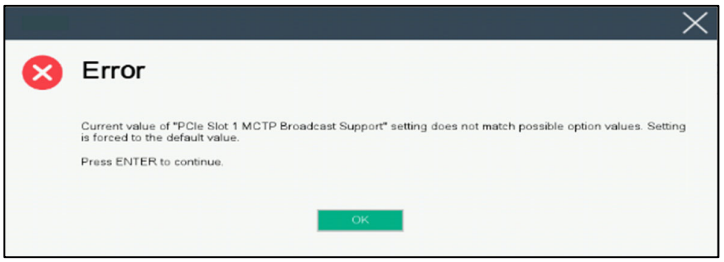
● About the PCIe Slot X MCTP Broadcast Support menu (X is PCIe Slot number)

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.

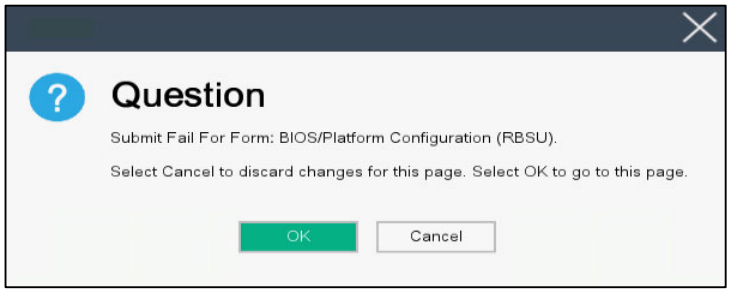
- v2.22 (11/13/2019)
- v2.30 (02/11/2020)
- v2.32 (03/09/2020)

*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 with iLO5 Firmware 1.40 or latest, 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

In case that ILO5 Firmware 1.40 or latest is used,  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 Admin Password is set from System Utilities(*1), or the case where the setting "Require Host Authentication" is enabled from iLO Web Interface(*2)**.

The matching condition is different by iLO5 Firmware Version.

iLO5 Firmware	matching condition(s)
Version 1.40	(*1), and (*2)
Version 1.43 and later	(*2)

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

● Caution for the case where Admin Password is set from system utility (*1), or the case where the setting "Require Host Authentication" is enabled from iLO Web Interface (*2).

(*1) This caution is for iLO5 Firmware Version lower than 1.43.
"System Configuration > BIOS/Platform Configuration (RBSU) > Server Security"
Set password by "Set Admin Password option"

(*2) This caution is for iLO5 Firmware Version 1.40 and higher.
Set "Require Host Authentication" Enabled in "Security > Access settings > 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

● Caution about iLO time function

This caution is for iLO5 Firmware Version lower than 1.45.
In case that SNTP setting is disabled, and if the iLO is reset, iLO time may be slipped.
It is recommended that SNTP is set enabled at iLO Web Interface.
For the details of iLO SNTP setting, please refer to iLO5 User's Guide.

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

If the iLO is reset during POST execution, the display of UUID and UUID logic in iLO Web Interface：[Information] > [Overview] page may be corrupted.
When any corrupted texts are displayed, please turn off and on the system.

● 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**

If iLO5 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**

< 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**

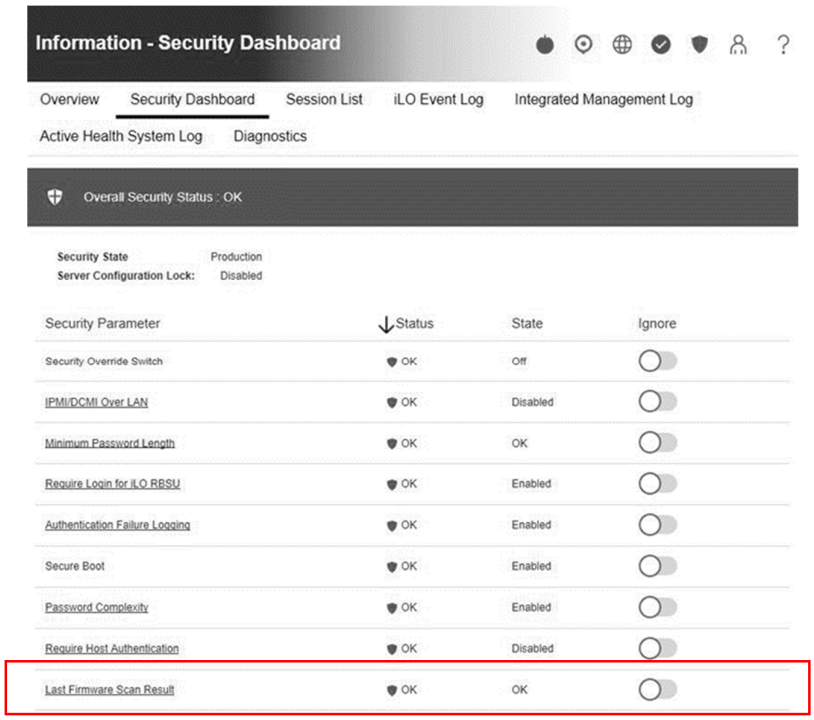
If you are using the iLO5 Firmware Version 3.00 or later

iLO 5 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 1.43 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.



● 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/ 7.0/8.0
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

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

iLO 5 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 iLO 5, 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

● Notice of Agentless Management Service (AMS) on the server running Windows Server OS

The server running a Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 operating system with Agentless Management Service (AMS) version 1.40.0.0 installed, the ams.exe process will exhibit an increasing handle count. Handle leaks can cause performance issues overtime due to over consumption of memory.

◆This symptom is fixed in the Agentless Management Service (AMS) 1.43.0.0.
This AMS is included in the Starter Pack. Please apply the Starter Pack Version S8.10-006.03 or later. If the AMS 1.40.0.0 is already installed in your server, and you want to apply Starter Pack Version S8.10-006.03, you need to update the AMS separately. For further explanation about the updating, please check the Starter Pack website.

◆If you want to use Agentless Management Service (AMS) 1.40.0.0, please do the following steps to stop the increasing of the handle count.

(1) Stop the AMS service by typing "net stop ams" in a command prompt.

(2) Explore to C:\Program Files\OEM\AMS\Service folder.

(3) Rename the file storelib.dll to storelib.dll.bak

(4) Start the AMS service by typing "net start ams" in a command prompt.

(*1) The following message may be displayed when stopping AMS, but there is no problem.
A system error has occurred.
System error 1067 has occurred.
The process terminated unexpectedly.
The Agentless Management Service service was stopped successfully.

(*2) The following message may be displayed when starting AMS, but there is no problem.
The requested service has already been started.

◆There are 2 ways to check the version of Agentless Management Service (AMS).
- The way to confirm on the OS of the target system.
(1) Run the following command on Windows PowerShell.
> Get-WmiObject Win32_Product | Select-Object Name,Version | Select-String "Agentless Management Service"

(2) Check the version from the command result.

- The way to confirm on the remote system with using iLO Web Interface.
(1) Login to iLO Web Interface with Web browser on the remote system.

(2) Select the "Firmware & OS Software" on the left menu, and then select "Software".

(3) Check the version of "ams.exe" displayed in "Product Related Software".

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

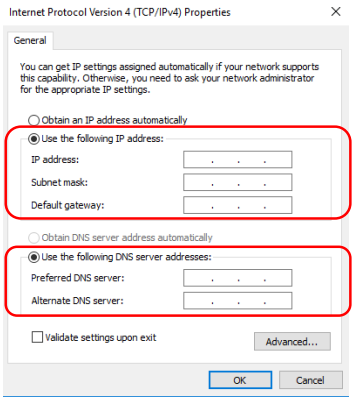
When a fixed IP address or DNS is set for the following options, add a CPU board by the following procedure.
(The procedure is necessary to take over the fixed IP address setting even after the CPU expansion.)

N8104-173 Dual Port 10GBASE-T LOM Card
N8104-177 Dual Port 25GBASE SFP+ LOM Card
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 iml_en.mtb Earlier 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.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 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

This caution is about the screen display of VMware vSphere : Monitor > Hardware > System Sensor > Sensor when the ESXi is booted.

(1) There are cases where the following Heartbeat Lost sensor displays "Warning(Yellow)".

[Device] I/O Module (n) LOM_Link_P (n) : Heartbeat Lost-Assert
[Device] I/O Module (n) NIC_Link_P (n) : Heartbeat Lost-Assert
*n represents LAN port number P1-P4

<Environment :iLO5 Firmware 1.30、1.35、1.38 is applied >
In case that the screen display of Heartbeat Lost sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, for the ports whose cables are connected, the "Warning (Yellow)" will disappear and turn to "Normal (Green)" within a couple of minutes after connecting LAN cable. Please wait for a couple of minutes. For the ports without LAN cables, the "Warning (Yellow)" will be continuously displayed, but this does not indicate hardware malfunction and there is no impact to the system operation. Please continue operating the system as is.
If a LAN cable is connected and the "Warning (Yellow)" does not disappear, there is a possibility that the connection of the cable is bad, so please check the LAN cable connection.

<Environment iLO5 Firmware : 1.40 or latest is applied>
In case that the screen display of Heartbeat Lost sensor Health (vCenter : Status) shows "Warning (Yellow)" after ESXi completes boot, the "Warning (Yellow)" will disappear and turn to "Normal (Green)" within a couple of minutes. Please wait for a couple of minutes.

(2) 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

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

● **Cautions on using Linux OS**

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

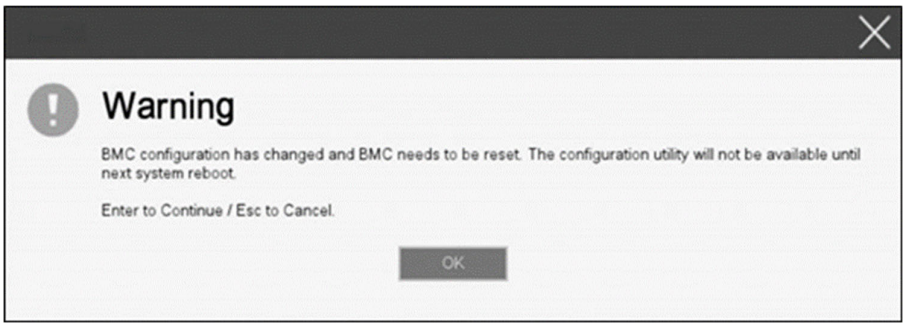
If operation using a device name based on the PCI address is required, do not add/remove the card to/from the PCI slot, or change the CPU configuration. If the PCI bus address information changes and the name of the PCI-connected device is affected, you may not be able to access the network or storage,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

5) Notice of the function in general

● Caution for operating BMC Configuration Utility in the System Utilities

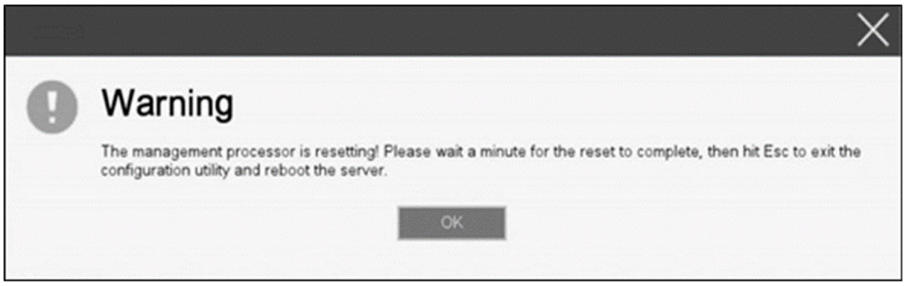
If you execute POST or change the BMC configuration while rebooting the iLO, some server settings such as Serial Number and Product ID may be lost.
In addition, there is a possibility that it does not operate normally in the restart process immediately after.
To avoid this trouble in rebooting the iLO, 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 7.3.3 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: S**ystem 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 "N8100-2557F". 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)**]

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)

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 Smart Storage Battery

Smart Storage Battery is indicated with Energy Pack on the RBSU menu. Please paraphrase.

● About EXPRESSBUILDER Help

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

● **Precautions on data backup**

There are cases that the device connected to FC controller may be misrecognized as an internal micro SD card slot, or that the empty internal micro SD card slot is misrecognized during auto backup with NEC Storage causing a pop-up error message and suspension of backup.
Due to such causes, there may be cases that data backup cannot be normally performed.
To prevent this to happen, the setting of this product is modified at the factory for disable internal micro SD card slot by the following procedure.
There is no influence on usual server operation since internal micro SD card slot is not to be used.

<Procedure>
From **System Utilities** > **BIOS/Platform Configuration (RBSU)** menu > **System Options** > **USB Options**, set **Internal SD Card Slot** to **Disabled**.

● **About FCoE function in N8104-173/177**

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

The FCoE function is enabled in N8104-173 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 533FLR-T FCoE Device
-HPE 622FLR-SFP28 FCoE Device

● **About DisplayPort Connector**

DisplayPort Connector at the front is not supported.

● **About Wake On LAN function in N8104-173**

When using the Wake On LAN function with PORT2 in N8104-173 (Dual Port 10GBASE-T LOM Card), update the firmware version to 7.19.2 or higher in advance.

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) Memory Options Menu

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

Option	Parameter	Description
Memory Controller Interleaving *1	[Auto] Disabled	Use this option to control the Memory Controller Interleaving option. When set to Auto, the system will automatically enable or disable memory controller interleaving based on the configuration of the system. When set to disabled, the user may force disable memory controller interleaving. In certain memory configurations, setting this option to disabled has showed a performance benefit across all memory in the system. It is recommended to leave this option to set to Auto.
Opportunistic Self-Refresh *2	[Disabled] Enabled	When "Enabled" is selected, self-refresh of memory is performed when the main memory is in the idle state. When "Disabled" is selected, regular-refresh of memory is performed.

[ ]: Default setting

*1: an option usable with System ROM Version 1.40 or later.
*2: an option usable with System ROM Version 1.36 or later.

(3) 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 1.72 or later.

(4) Intel UPI Options Menu

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

Option	Parameter	Description
Direct To UPI (D2K) *1	[Auto] Enabled Disabled	When "Enabled" is selected, Latency of the last level cache is reduced. Please don't change this setting unless it's designated. This options appears on only dual processor configuration.

[ ]: Default setting

*1: an option usable with System ROM Version 1.36 or later.

(5) Advanced Performance Tuning Options Menu

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

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

Option	Parameter	Description
Processor Jitter Control Optimization *1	Optimized for Throughput Optimized for Latency [Zero Latency]	This option optimizes the thresholds used when the Auto-tuned function detects fluctuations in processor frequency. Optimized for throughput allows only the amount of fluctuations that doesn't impact overall compute throughput. Optimized for Latency allows for a very small amount of occasional fluctuations to occur before reducing processor frequency. Zero Latency attempts to eliminate any frequency fluctuations.
IODC Configuration *2	[Auto] Enable for Remote InvItoM Hybrid Push InvItoM AllocFlow InvItoM Hybrid AllocFlow Enable for Remote InvItoM and Remote WViLF	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)

[ ]: Default setting

*1: an option usable with System ROM Version 1.40 or later.

*2: an option usable with System ROM Version 2.10 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 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.

(6) 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.

(7) PCIe Device Configuration Menu

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

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

Option	Parameter	Description
Advanced PCIe Configuration *1	-	-

*1: an option usable with System ROM Version 1.40 or later.

(a) Advanced PCIe Configuration Menu

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

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

Option	Parameter	Description
PCIe Bifurcation Options *1	-	-
PCIe MCTP Options *2	-	-

*1: an option usable with System ROM Version 1.36 or later.

*2: an option usable with System ROM Version 2.10 or later.

i. PCIe Bifurcation Options

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

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

Option	Parameter	Description
PCIe Slot XX Bifurcation *1	[Auto] Slot Bifurcated	If the device installed in the slot supports this capability, the "Slot Bifurcated" can be selected. When "Auto" is selected, the PCIe slot will train at the maximum width supported by the slot and end point. When "Slot Bifurcated" is selected, the PCIe slot will be bifurcated into two equal width slots. XX: 1/2/3... (XX appears as specific slot number by the processor or the riser card configuration.)

[ ]: Default setting

*1: an option usable with System ROM Version 1.36 or later.

ii. PCIe MCTP Options

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

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

Option	Parameter	Description
PCIe Slot XX MCTP Broadcast Support *1	[Enabled] Disabled	Use this option to control the PCIe Management Component Transport Protocol (MCTP) Support for a given slot. This option can be used to disable MCTP support to a given PCIe endpoint that may not properly support this protocol. It is recommended that this option remain enabled for full system functionality. XX: 1/2/3... (XX appears as specific slot number by the processor or the riser card configuration.)

[ ]: Default setting

*1: an option usable with System ROM Version 2.10 or later.

(8) Fan and Thermal Options Menu

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

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

Option	Parameter	Description
Thermal Configuration *1	[Optimal Cooling] Increased Cooling Maximum Cooling Enhanced CPU Cooling	Use this option to select the fan cooling solution for the system. "Optimal Cooling" provides the most efficient solution by configuring fan speeds to the minimum required speed to provide adequate cooling. "Increased Cooling" runs fans at higher speeds to provide additional cooling. Select "Increased Cooling" when third-party storage controllers are cabled to the embedded hard drive cage, or if the system is experiencing thermal issues that cannot be resolved. "Maximum Cooling" provides the maximum cooling available on this platform. "Enhanced CPU Cooling" provides additional cooling to the processors. When running certain processor intensive workloads, this option can provide additional cooling to the processors which can result in improved performance.

[ ]: Default setting

*1: an option usable with System ROM Version 1.36 or later.

(9) Advanced Debug Options Menu

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

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

Option	Parameter	Description
Advanced Crash Dump Mode *1	[Disabled] Enabled	Use this option to enable the Advanced Crash Dump Mode. When enabled, the system will be configured to log additional debug information to the Active Health System logs when an unexpected system crash is experienced. This option should only be enabled when directed by qualified service personnel.

[ ]: Default setting

*1: an option usable with System ROM Version 1.40 or later.

(10) Embedded Applications Menu

When you select Embedded Applications from the System Utilities, the Embedded Applications menu appears. For details about the options, see the table below.

Option	Parameter	Description
Embedded Diagnostics *1	-	This product does not support it.

[ ]: Default setting

*1: an option usable with System ROM Version 1.36 or later.

B) Errata Information

■ Errata Information for Express5800/R120h-1MUser's Guide

The following table covers corrections for User's Guide.
Please read the following information and use it as reference.

<table>
<tr><th></th><th>Error</th><th>Correct</th></tr>
<tr><td>Chapter 2 Preparations
1.10.7 Memory Function
(1) Memory Mirroring Function</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Advanced Memory Protection" to "Mirrored Memory with Advanced ECC Support".</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection" to "Mirrored Memory with Advanced ECC Support".</td></tr>
<tr><td>Chapter 2 Preparations
1.10.7 Memory Function
(2) Memory Sparing Function</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection" to "Online Spare with Advanced ECC Support".</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection" to "Online Spare with Advanced ECC Support".</td></tr>
<tr><td>Chapter 2 Preparations
1.10.7 Memory Function
(3) Fault tolerant memory function (ADDDC)</td><td>From the System Utilities, select "System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations to set Advanced Memory Protection to Fault Tolerant Memory (ADDDC)".</td><td>From the System Utilities, select "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options to set Advanced Memory Protection to Fault Tolerant Memory (ADDDC)".</td></tr>
<tr><td>Chapter 2 Preparations
1.25.1 Notes on Building RAID System</td><td>If the optional RAID Controller N8103-189/192/195 is used, the RAID System cannot be built in RAID5/RAID6/RAID50/RAID60.

<table><tr><th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr><tr><th>N8103-189/192/195</th><th>N8103-190/191/193/194/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td></td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>3</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>6</td></tr></table></td><td>If the optional RAID Controller N8103-189/192/195 is used, the RAID System cannot be built in RAID6/RAID50/RAID60.

<table><tr><th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr><tr><th>N8103-189/192/195</th><th>N8103-190/191/193/194/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td>3</td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>4</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>8</td></tr></table></td></tr>
<tr><td>Chapter 3 Setup
2.4 Cases that Require Configuration
>Memory
>Use memory RAS feature</td><td>Set System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Oprations - Advanced Memory Protection</td><td>Set System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options - Advanced Memory Protection</td></tr>
<tr><td>OS supported</td><td>VMware ESXi™ 6.7 Update1 or later</td><td>VMware ESXi™ 6.7 Update2 or later</td></tr>
<tr><td>On-board CPU</td><td>Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td><td>Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td></tr>
</table>

■ Errata Information for Express5800/R120h-2M User's Guide

The following table covers corrections for User's Guide.
Please read the following information and use it as reference.

<table>
<tr><th></th><th>Error</th><th>Correct</th></tr>
<tr><td>Chapter 2 Preparations
1.11.6 Memory Function
(1) Memory Mirroring Function</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Advanced Memory Protection" to "Mirrored Memory with Advanced ECC Support".</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection" to "Mirrored Memory with Advanced ECC Support".</td></tr>
<tr><td>Chapter 2 Preparations
1.11.6 Memory Function
(2) Memory Sparing Function</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) >System Options > Memory Oprations > Advanced Memory Protection" to "Online Spare with Advanced ECC Support".</td><td>From System Utility, set "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection" to "Online Spare with Advanced ECC Support".</td></tr>
<tr><td>Chapter 2 Preparations
1.11.6 Memory Function
(3) Fault tolerant memory function (ADDDC)</td><td>From the System Utilities, select "System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations to set Advanced Memory Protection to Fault Tolerant Memory (ADDDC)".</td><td>From the System Utilities, select "System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options to set Advanced Memory Protection to Fault Tolerant Memory (ADDDC)".</td></tr>
<tr><td>Chapter 2 Preparations
1.33.1 Notes on Building RAID System</td><td>● If the optional RAID Controller (N8103-189/195) is used, the RAID System cannot be built in RAID5/RAID6/RAID50/RAID60.

<table><tr><th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr><tr><th>N8103-189/195</th><th>N8103-190/191/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td></td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>3</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>6</td></tr></table></td><td>● If the optional RAID Controller (N8103-189/195) is used, the RAID System cannot be built in RAID6/RAID50/RAID60.

<table><tr><th rowspan="2">RAID level</th><th colspan="2">The minimum number of hard disk drives required to set up a RAID System</th></tr><tr><th>N8103-189/195</th><th>N8103-190/191/201</th></tr><tr><td>RAID 0</td><td>1</td><td>1</td></tr><tr><td>RAID 1</td><td>2</td><td>2</td></tr><tr><td>RAID 5</td><td>3</td><td>3</td></tr><tr><td>RAID 6</td><td></td><td>4</td></tr><tr><td>RAID 10</td><td>4</td><td>4</td></tr><tr><td>RAID 50</td><td></td><td>6</td></tr><tr><td>RAID 60</td><td></td><td>8</td></tr></table></td></tr>
<tr><td>Chapter 3 Setup
2.4 Cases that Require Configuration
>Memory
>Use memory RAS feature</td><td>Set System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Oprations - Advanced Memory Protection</td><td>Set System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options - Advanced Memory Protection</td></tr>
<tr><td>OS supported</td><td>VMware ESXi™ 6.7 Update1 or later</td><td>VMware ESXi™ 6.7 Update2 or later</td></tr>
<tr><td>On-board CPU</td><td>Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td><td>Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)</td></tr>
</table>

■ Errata Information for Express5800/R120h-1M, R120h-2M Maintenance Guide

The following table covers correction for Maintenance Guide.
Please read the following information and use it as reference.

	Error	Correct
Chapter 2 Useful Features 1.2.2 BIOS/Platform Configuration (RBSU) (3) Memory Options Menu	When you select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Options from the System Utilities, the Memory Options menu appears	When you select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options from the System Utilities, the Memory Options menu appears
Chapter 2 Useful Features 1.2.2 BIOS/Platform Configuration (RBSU) (a)Persistent Memory Options Menu	When you select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Memory Operations > Persistent Memory Options from the System Utilities, the Persistent Memory Options menu appears.	When you select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Persistent Memory Options from the System Utilities, the Persistent Memory Options menu appears.

■ Correction of DIMM installation order

There are misdescription about DIMM installation order in user's guides.
The following is the correction.

Correction point

- Express5800/R120h-1M User's Guide

  Chapter 2 Preparations 1.10 DIMM 1.10.2 DIMM installation order

- Express5800/R120h-2M User's Guide

  Chapter 2 Preparations 1.11 DIMM 1.11.2 DIMM installation order

DIMM installation order

The order of installation may be different on x1CPU configuration, x2CPU configuration, and mounted number of the DIMM.

- When only CPU1 is mounted

DIMM slot number		1	2	3	4	5	6	7	8	9	10	11	12
DIMM Mounted number and installation order	1 DIMM								1				
	2 DIMM								1		2		
	3 DIMM								1		2		3
	4 DIMM			4		3			1		2		
	5 DIMM			5		4			1		2		3
	6 DIMM	6		5		4			1		2		3
	7 DIMM	6		5		4		7	1		2		3
	8 DIMM			4	8	3	7	5	1	6	2		
	9 DIMM	6		5		4		7	1	8	2	9	3
	10 DIMM	6		5	10	4	9	7	1	8	2		3
	11 DIMM	6		5	11	4	10	7	1	8	2	9	3
	12 DIMM	6	12	5	11	4	10	7	1	8	2	9	3

(Continue to the next page)

- When CPU1 and CPU2 are mounted

DIMM slot number		CPU2												CPU1											
		1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
DIMM Mounted number and installation order	2 DIMM								2												1				
	3 DIMM								2												1		3		
	4 DIMM								2		4										1		3		
	5 DIMM								2		4										1		3		5
	6 DIMM								2		4		6								1		3		5
	7 DIMM								2		4		6			7		5			1		3		
	8 DIMM			8		6			2		4					7		5			1		3		
	9 DIMM			8		6			2		4					9		7			1		3		5
	10 DIMM			10		8			2		4		6			9		7			1		3		5
	11 DIMM			10		8			2		4		6	11		9		7			1		3		5
	12 DIMM	12		10		8			2		4		6	11		9		7			1		3		5
	13 DIMM	12		10		8			2		4		6	11		9		7		13	1		3		5
	14 DIMM	12		10		8		14	2		4		6	11		9		7		13	1		3		5
	15 DIMM	12		10		8		14	2		4		6			7	15	5	13	9	1	11	3		
	16 DIMM			8	16	6	14	10	2	12	4					7	15	5	13	9	1	11	3		
	17 DIMM			8	16	6	14	10	2	12	4			11		9		7		13	1	15	3	17	5
	18 DIMM	12		10		8		14	2	16	4	18	6	11		9		7		13	1	15	3	17	5
	19 DIMM	12		10		8		14	2	16	4	18	6	11		9	19	7	17	13	1	15	3		5
	20 DIMM	12		10	20	8	18	14	2	16	4		6	11		9	19	7	17	13	1	15	3		5
	21 DIMM	12		10	20	8	18	14	2	16	4		6	11		9	21	7	19	13	1	15	3	17	5
	22 DIMM	12		10	22	8	20	14	2	16	4	18	6	11		9	21	7	19	13	1	15	3	17	5
	23 DIMM	12		10	22	8	20	14	2	16	4	18	6	11	23	9	21	7	19	13	1	15	3	17	5
	24 DIMM	12	24	10	22	8	20	14	2	16	4	18	6	11	23	9	21	7	19	13	1	15	3	17	5

- Notice for the combination of DIMM

When more than one kinds of DIMM is combined, install them in the order from the following list to the installation order on the above table.

(High priority) N8102-711 > N8102-710 > N8102-714 > N8102-709 > N8102-708 (Low priority)

■ 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

March 2026 25th Edition