

Express5800/R110j-1 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。誠にとおそれ入りますが、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。

◇ Index

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

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 サイトに掲載の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」で、「3170102220」を入力して検索してください。

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確認し、利用してください。

● 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 サイトに掲載の内容を確認し、バージョン S8.10-005.01 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、「S8.10-005」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 サイトに掲載の内容を確認し、適切なバージョンを適用してください。

- ・ 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 6.5/6.7 または ESXi 7.0 を利用している場合は、【旧版】と表示される、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))

- ・ 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 6.5 版, 6.7 版, 7.0 版, 8.0 版) を適用してください)

- ・ 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一覧」を選択)

● 本製品の保守作業時間に関して

本製品は、障害発生時などの保守作業において、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3.40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。

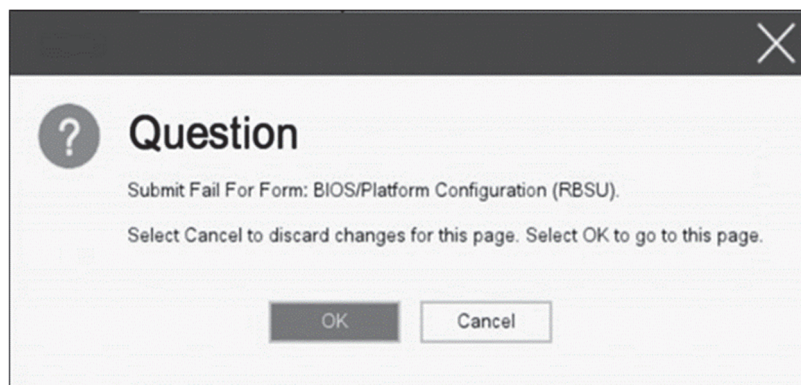
(*1) BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control

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

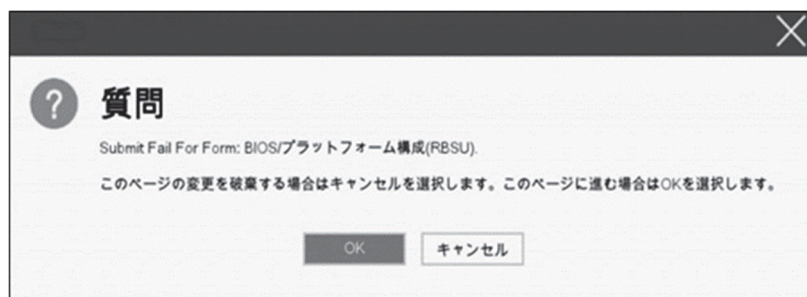
● Submit Fail For FormのQuestion(質問)ポップアップ表示についての注意事項

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

● 「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)」の項を参照してください。

● 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オフ、オンによって回復します。

赤文字画面 (RSoD) が表示された場合は、装置電源のオフ、オンを実施してください。

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

RCX-0000000000001E0 BX-0000000000001E0 RB-000000000000000 R9-000000000000010
RSP-0000000059C711E0 BP-0000000059C7123B AX-0000000000000000 BX-000000000000000
R10-0000000037FB0790 I1-0000000059C711AB I2-0000000059C712BC I3-0000000059C71240
R14-0000000059C16724 I5-0000000059C1E0C9 SI-0000000048E69018 DI-0000000059C711EB
CR2-0000000059C712BC CR3-0000000059BD1000 CR0-00010013 CR4-00000668 CR8-00000000
CS-00000038 DS-00000038 SS-00000038 ES-00000038 RFLAGS-00210206
MSR: 0x1D9 = 00004B01, 0x345=0000F4C5, 0x1C9=0000000E

LBRs From To From To
01h 0000000059C712BC->0000000053BD31AE 0000000037FAF807->0000000059C712BC
03h 0000000037FAF76F->0000000037FAF77F 0000000059C16737->0000000037FAF76C
05h 00000000520EB4DA->0000000059C16733 00000000520EB4B7->00000000520EB4C3
07h 0000000059C7E0AB->00000000520EB41B 0000000059C7E094->0000000059C7E098
09h 0000000059C7E06B->0000000059C7E07D 0000000059C7E04D->0000000059C7E059
0Bh 0000000059C7F6E3->0000000059C7E034 0000000059C7F52C->0000000059C7F6CF
0Dh 0000000053BD029A->0000000059C7F528 0000000053BD0611->0000000053BD029D
0Fh 0000000059C72BF0->0000000059C7E3D1 0000000053BD31B9->0000000053BE0A00

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

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。

● システムROMバージョン2.32、かつiLO5ファームウェアバージョン2.40以降の場合、iLO Webインターフェイス上のPCI Slot 1の情報が正しく表示されない

システムROMバージョン2.32、かつiLO5ファームウェアバージョン2.40以降の場合、iLO Webインターフェイス上で、PCI Slot 1はUnknown、またはEmpty Slot 1と表示されます。

また、PCI Slot 1でエラーを検出しても、IMLに正しく記録されません。

例: クラス: 0x8、コード: 0x2 Uncorrectable PCI Express Error Detected. ...

クラス: 0x11 コード: 0xA <ネットワークカード名> - NIC Connectivity status changed to Link Failure for adapter ...

...

など。

PCI Slot 1の情報については、システムユーティリティのPCI Device Informationメニューを参照してください。

システムROMバージョン2.52では、この問題が修正されています。

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

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

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

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

システム ROM バージョン 1.22 以降、2.14 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。

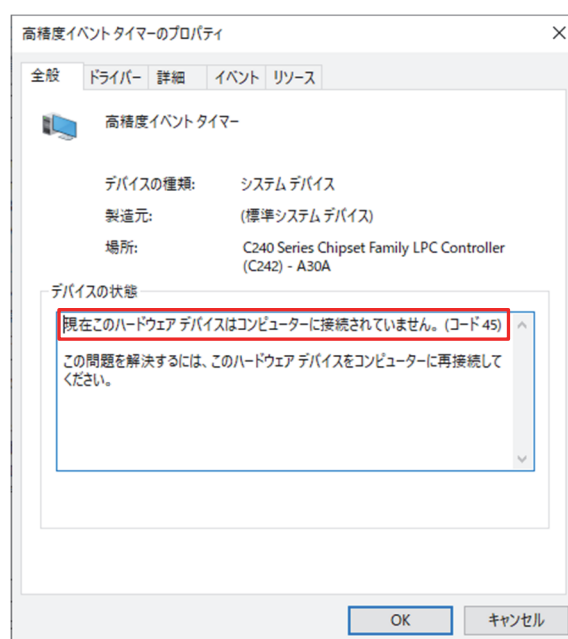
(*1) 「System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration」

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

● Windows (R) デバイスマネージャーに高精度イベントタイマーが表示されず、使用できない

システム ROM バージョン 2.52 未満の場合、Windows (R) デバイスマネージャーに高精度イベントタイマーが表示されず、使用できません。

本問題が発生した場合、高精度イベントタイマーのプロパティに以下のメッセージが表示されます。



高精度イベントタイマーのプロパティ画面

● システムユーティリティおよびワнтаイムブートメニューの表示について

・ 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 1.20 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。

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

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

【発生条件】

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

以下 2 つの条件をすべて満たす場合、発生します。

1. RAID コントローラファームウェアバージョン 4.11 以降、または 3.01.04.072 以降
2. システム ROM バージョン 2.60 未満

● システムROMバージョン 2.00である場合の注意事項

システム ROM バージョン 2.00 である場合は、以下の Web サイトよりシステム ROM のアップデートモジュールをダウンロードし、システム ROM バージョン 1.22 を適用してください。

<https://www.support.nec.co.jp/View.aspx?id=9010108425>

● システムROMバージョン2.32の場合、搭載していないNVMeの情報がiLO Webインターフェイスに表示される

システム ROM バージョン 2.32 の場合、iLO Web インターフェイス上に搭載していない NVMe の情報が以下のように表示されますが、使用できません。

- ファームウェア & OS ソフトウェア - ファームウェア: NVMe Drive
- システム情報 - ストレージ: NVMe SSD
- システム情報 - デバイスインベントリ: PCI-E Slot 1 (製品名は Empty Slot 1 と表示されます)

システム ROM バージョン 2.52 では、上記の誤表示問題が修正されています。

● PCIe Device DisableにてHPE Ethernet 1Gb 2-port 361i Adapterを無効にできない

HPE Ethernet 1Gb 2-port 361i Adapter の LAN ファームウェアバージョンが以下の場合、RBSU の PCIe Device Disable(*) を Disabled に設定しても無効にできません。

- ・ 対象 LAN ファームウェアバージョン
 - 1.2529.0
 - 1.2688.0
 - 1.2836.0

(*) System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration
> (Embedded LOM 名) メニュー > PCIe Device Disable

● 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では、この問題が修正されています。

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などの設定情報を消失することがあります。また、POST実行中にiLOの再起動を行うと、iLO Webインターフェイス : [Information] > [Overview] ページにおけるUUID、UUID (論理) が不正な表示になる場合があります。

不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

＜対象となるiLOの再起動の方法＞

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

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

● iLOのダウングレードポリシー機能の注意事項

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

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

また、本設定は一度設定を行うと永続的に保持されるため、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戻しても、その他の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を行っても、『Permanently disallow downgrades』設定は維持されたままになります。

● iLO WebインターフェイスのUUID不正値表示について

POST実行中にiLOの再起動を行うと、iLO Webインターフェイスの[Information] > [Overview] ページのUUID、UUID (論理) の値がまれに不正な表示となることがあります。

不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

● iLO Webインターフェイスの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、以下を確認してください。

- ・ iLO5ファームウェアバージョン2.14以降、2.18未満をご使用の場合、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。

- ・ iLO5ファームウェアバージョン1.40以降、1.47未満、もしくは、2.31以降をご使用の場合、デフォルト値は『無効(Disabled)』です。

● 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

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場合、[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、読み替えて利用してください。

● 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、確認してください。

iLO5ファームウェア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利用できません。

- ・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

● 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未満をご使用の場合、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ことがあります。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確認してください。

● ネットワークブリッジ構成時のiLO Webインターフェ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以降をご使用の場合、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確認してください。

● 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できなくなります。その場合、ブラウザのリロードボタンをクリックするか、もしくはいったんiLO Webインターフェイスのログアウトを実行して再度ログインしてください。

情報 - セキュリティダッシュボード

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

Active Health System ログ 診断

全体セキュリティステータス: OK

セキュリティ状態 本番環境
サーバー構成ロック: Disabled

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

日本語表示の場合

Information - Security Dashboard

Overview Security Dashboard Session List iLO Event Log Integrated Management Log

Active Health System Log Diagnostics

Overall Security Status : OK

Security State Production
Server Configuration Lock: Disabled

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

英語表示の場合

● 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

iLO5ファームウェアバージョン3.00以降の適用装置:

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の再起動を行ってください。

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

物理ドライブのステータス変更時のSNMP Trap通知において、ロケーション情報が欠損する場合があります。

ロケーション情報に関しては、iLO Webインターフェイスの[情報] > [インテグレートドマネジメントログ]で同じイベントのロケーション情報を確認してください。

例:

Abnormal, physical drive status change detection, iLO SNMP Trap, mgr_WIN-U6H1HPNIH1Q, 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の再起動を行ってください。また、その後10分程度経過してから、以下の対象OSごとの再起動方法を参考に、Agentless Management Service (AMS)を再起動してください。

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

・ Windowsの場合

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

・ Red Hat Enterprise Linux 7.x/8.xの場合

以下のコマンドを実行します。

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

・ ESXi 6.5/6.7の場合

以下のコマンドを実行します。

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

※ お使いのAMSバージョンによりコマンドが異なります。

・ ESXi 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
```

(※) 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、一部の情報が取得できず、iLO Webインターフェイスの「Host > Hardware > Storage > Storage Controllers」や「Host > Hardware > Network」の情報が正しく表示されません。また、この影響によりESMPRO/ServerManagerによるIML監視やエクスプレス通報などが正しく行えない可能性もあります。

● 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。

● 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 WebインターフェイスにてSNTPの設定を行い、使用することを推奨します。

iLOのSNTPの設定方法については、iLO5ユーザズガイドを参照してください。

● 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

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

iLO5ファームウェアバージョン2.71または2.72の適用装置:

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

iLO5ファームウェアバージョン2.90以降の適用装置:

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以降の適用装置:

ESMPRO/ServerManagerを利用している場合、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次のニ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)バージョン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バージョン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バージョン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。

a) 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。

b) 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。

● 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
バージョン 2.10 以降	バージョン 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
	バージョン 6.47 未満	アラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに表示されない、もしくは「不明タイプ」のアラートとして表示される

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

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

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

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

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

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

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

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

- ② ESMPRO Platform Management Kit の ESMPRO インストールツールを起動します。
- ③ インストールツール画面の説明書をクリックし、Software Manuals から ESMPRO/ServerManager をクリックします。
- ④ 「ESMPRO/ServerManager Ver. 7 インストールガイド (Windows 編)」をクリックします。
- ⑤ 「ESMPRO/ServerManager Ver. 7 インストールガイド (Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager を Ver. 6 から Ver. 7 へアップデートします。

・ iLO 管理機能向けの受信情報設定ファイル に関する発生現象

※エクスプレス通報サービス (MG) を利用し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
バージョン 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 MGMTB.zip 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>
- ・ iLO ファームウェアのバージョン確認方法
 - ・ Server Health Summary で確認する方法
 サーバー本体の UID ボタンを押下して、サーバーに接続されたコンソールに表示される iLO ファームウェアのバージョンを確認します (Server Health Summary の詳細は iLO5 ユーザーズガイド参照)。
 - ・ ネットワーク経由で確認する方法
 iLO にネットワーク接続可能な場合、ブラウザから iLO にログインして、メニュー「ファームウェア & OS ソフトウェア」から iLO バージョンを確認します。
- ・ ESMPRO/ServerManager (Windows 版) のバージョン確認方法
 - ① ESMPRO/ServerManager の Web サイトにログインします。
 - ② 画面右上の「ESMPRO/ServerManager について」のリンクを選択します。
 - ③ 表示される ESMPRO/ServerManager のバージョン情報を確認します。
- ・ iLO 管理機能向けの受信情報設定ファイルのバージョン確認方法
 「エクスプレス通報サービス (MG) インストレーションガイド (Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で「詳細情報」の「iLO SNMP Trap」のバージョンを確認します。

● VMware ESXi ご使用時の注意事項

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。

- ・ 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 の適用装置>
 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 以降の適用装置>
 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。
- ・ システム ROM バージョン 2.16 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
- ・ 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

● Linux OSご使用時の注意事項

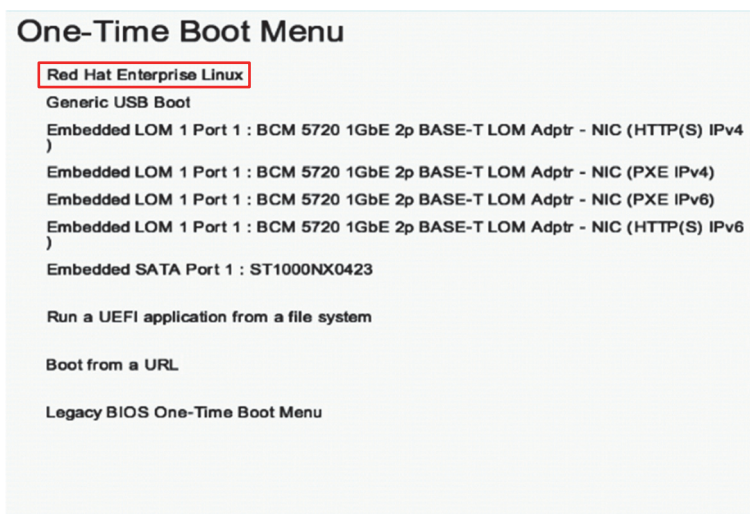
OSが自動的に認識するLOMやオプションNICのデバイス名を使用してください。独自udevルールを追加する際、PCIアドレスを基準にNICデバイス名を変更したり、固定したりする設定は行わないでください。
また、PCIアドレスを含む/dev/disk/by-path/配下のストレージデバイス名は使用しないでください。

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

● Red Hat Enterprise Linux 8.5 以前を使用する場合の注意事項

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

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



ワンタイムブートメニュー画面

5) 全般の機能に関する注意事項

● 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。

すで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場合があります。

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



【重要】Product IDとは、『N8100-xxxxY』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。

● 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。

● Intel (R) Software Guard Extensions (SGX) オプションについて

本機能をサポートするCPUは下記2タイプのCPUのみとなります。それ以外のCPUにおいて、Intel (R) Software Guard Extensions (SGX) オプションが表示される場合でも、Disabled(デフォルト値)の設定から変更しないでください。下記2タイプのCPU以外では本機能をサポートしておりません。

- ・ N8101-1507 (4C/E-2174G)
- ・ N8101-1518 (6C/E-2186G)

● N8104-173 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。
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、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

● 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。

● 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。
- ・ N8103-184 SAS コントローラを使用する場合、下記制限事項をお守りください。
搭載枚数 : 1 枚まで搭載可能です (ほかのカードとの混載は可能です)。
搭載 PCI スロット : スロット 1 に搭載してください。

● N8117-12 管理 LAN/シリアルポート搭載時の設定について

N8117-12 管理 LAN/シリアルポートオプションを搭載し、管理 LAN ポートを使用する場合は、以下の設定を変更してください。

設定手順

System Configuration > BMC Configuration Utility > Network Options > Network Interface Adapter を「ON」に設定してください。

● 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 サイトを確認してください。

- ・ 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>

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 2.32 以降にて利用できるオプションです。

(2) Server Security メニュー

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

追加のオプションについて、次の表を参照してください。

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

[]: 出荷時の設定

(注 1) システム ROM バージョン 2.32 以降にて利用できるオプションです。

(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
Minimum Processor Idle Power Core C-State	[C6 State] C3 State C6 Without C1E State (注1) C1E State No C-states	このオプションは、「Workload Profile」が「Custom」に設定されている場合のみ設定できます。システムが使用するプロセッサの最小アイドル電力状態 (C-ステート) を選択するには、このオプションを使用します。C-ステートが高いほど、そのアイドル状態の消費電力が低くなります。(プロセッサがサポートする最小電力アイドル状態は C6 です)。

[]: 出荷時の設定

(注1) システムROMバージョン3.10以降にて利用できるパラメーターです。

(4) Trusted Platform Module Optionsメニュー

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

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Omit Boot Device Event (注1)	[Disabled] Enabled	ブートデバイスイベント省略の記録を設定します。「Enabled」に設定すると、PCRブート試行の測定が無効になり、PCR[4]での測定が記録されなくなります。

[]: 出荷時の設定

(注1) システムROMバージョン2.80以降にて利用できるオプションです。

B) 誤記訂正

■ Express5800/ R110j-1 メンテナンスガイドについて

メンテナンスガイドの記述に不足がありましたので、以下に訂正いたします。

	誤	正
P. 44 トラブルシューティング	[?] Serial Number、Product IDが正しくない、あるいは消失してしまった → Serial Number、Product IDが消失してしまった場合、以下の手順にて対処します。	[?] Serial Number、Product IDが正しくない、あるいは消失してしまった → Serial Number、Product IDが消失してしまった場合、以下の手順にて対処します。 (※Product IDとは、『N8100-2766Y』のような型番のことです。)

■ メモリ搭載順序の訂正

ユーザーズガイドにおいて、メモリの搭載順序に誤記がありました。
については、下記のとおり訂正いたします。

修正箇所

- Express5800/R110j-1 ユーザーズガイド
2章 準備 1.8 DIMM 1.8.2 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、搭載順序は以下の表となります。容量の大きいDIMMから順に増設してください。

DIMMスロット番号		1	2	3	4
メモリ搭載枚数と 搭載順序	DIMM 1枚			1	
	DIMM 2枚	2		1	
	DIMM 3枚	2		1	3
	DIMM 4枚	2	4	1	3

・ 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) N8102-719 → N8102-718 (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わせについて

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

お問い合わせ先：ファーストコンタクトセンター

T E L : 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。



2026年 3月 第18版

Precautions for Using Express5800/R110j-1

Thank you for purchasing our products.

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

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

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

1) Introduction

● About the manual of this product.

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

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

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

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

● About Starter pack

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

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

● About service and driver modules for VMware ESXi

Please see the following web site to check the latest modules.

1. Agentless Management Service and iLO Channel Interface Driver

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

2. WBEM Provider and CLI tool

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

● Notice about service operation time of this product

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

2) Notice about the function of the System ROM

● Note for UEFI Boot Order Control

If the System ROM version is 3.40, you cannot enable or disable new boot devices or save these settings in the UEFI Boot Order Control menu (*1). To change the priority of the device to boot from, please adjust the priority in the UEFI Boot Order menu (*2).

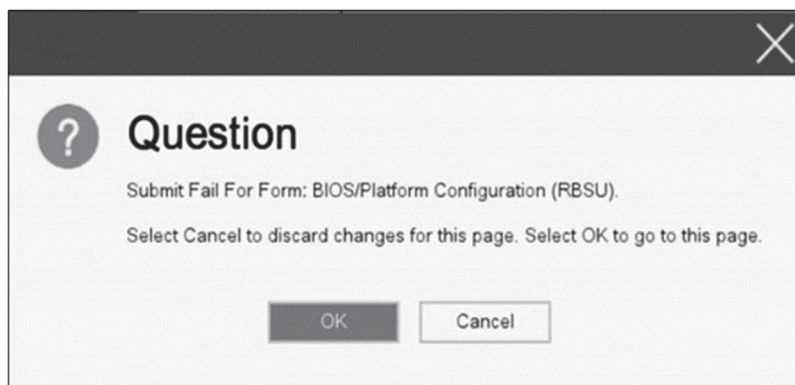
Additionally, each time you navigate to the UEFI Boot Order menu or the UEFI Boot Order Control menu, a red circle (◎) will appear in front of the "Changes Pending" string at the bottom of the screen. Press the F10 key as needed to save the settings.

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

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

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

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



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

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

To recover from this condition, power off and then on the server again.

If the problem persists, contact your sales representative for maintenance.

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

RCX-0000000000001E0 BX-0000000000001E0 RB-000000000000000 R9-000000000000010
RSP-000000059C711E0 BP-000000059C7123B AX-000000000000000 BX-000000000000000
R10-0000000037FB0790 I1-00000000059C711AB I2-00000000059C7120C I3-000000059C71240
R14-000000050C16724 I5-000000050C1E0C9 SI-000000048E69018 DI-000000059C711E0
CR2-000000059C7120C CR3-000000059BD1000 CR0-80010013 CR4-00000668 CR8-00000000
CS-0000003B DS-0000003B SS-0000003B ES-0000003B RFLAGS-00210206
MSR: 0x1D9 = 00004001, 0x345=0000F4C5, 0x1C9=0000000E

LBRs From To From To
01h 000000059C7120C->0000000538D31AE 0000000037FAF007->000000059C7120C
03h 0000000037FAF76F->0000000037FAF77F 0000000050C16737->0000000037FAF76C
05h 00000000520EB4DA->000000050C16733 00000000520EB4B7->00000000520EB4C3
07h 000000059C7E04B->0000000520EB41B 000000059C7E094->000000059C7E09B
09h 000000059C7E06B->000000059C7E07D 000000059C7E04D->000000059C7E059
0Bh 000000059C7F6E3->000000059C7E034 000000059C7F52C->000000059C7F6CF
0Dh 0000000538D029A->000000059C7F520 0000000538DC0A1->0000000538D029D
0Fh 000000059C72BF0->000000059C7E3D1 0000000538D31B9->0000000538E0000

CALL ImageBase ImageName+Offset
00h 000000059B71000( h)
```

- **If Secure Boot fails, a red screen (RSoD: Red Screen of Death) may be displayed**

If Attempt Secure Boot (*) in RBSU is set to Enabled, and Secure Boot (signature verification) fails during boot, a 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 a Red Screen of Death (RSoD) appears, power the device OFF and then ON. After that, resolve the cause of the Secure Boot failure (e.g., the boot loader/OS components are outdated and fail verification under the current Secure Boot policy), and then boot from the boot device.

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

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

- **Server may become unresponsive during Network PXE Boot**

When System ROM version is below 3.10, the server may occasionally become unresponsive when booting via Network PXE Boot with an OS. If this issue occurs, please follow one of the procedures below to restart the server:

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

This issue has been fixed in System ROM version 3.10.

- **In the case of System ROM version 2.32 and iLO5 firmware version 2.40 or later, the information of PCI Slot 1 on the iLO Web Interface is not indicated correctly**

The name of PCI option card attached on PCI Slot 1 is indicated as "Unknown" or "Empty Slot 1" on the iLO Web Interface.

When an error was detected in PCI Slot 1, the error will not be recorded correctly in IML. This issue has been fixed in System ROM version 2.54

Ex. Class: 0x8, Code: 0x2 Uncorrectable PCI Express Error Detected. ...

Class: 0x11, Code: 0xA <Network Card Name> - NIC Connectivity status changed to Link Failure for adapter ...

...

etc.

- **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 - 7.3.3 Restore the Default Settings of System Configuration" of the maintenance guide.

- **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).)

- **When "PCIe Device Disable" is set to "Disabled", "HPE Ethernet 1Gb 2-port 361i Adapter" cannot be disabled**

When LAN firmware is included in the following list, setting "PCIe Device Disable" to "Disabled" will not disable HPE Ethernet 1Gb 2-port 361i Adapter.

LAN firmware list

- 1.2529.0
- 1.2688.0
- 1.2836.0

System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration
> (Embedded LOM Name) menu > PCIe Device Disable

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

When System ROM version 1.22 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」

● Caution when the System ROM version is 2.00

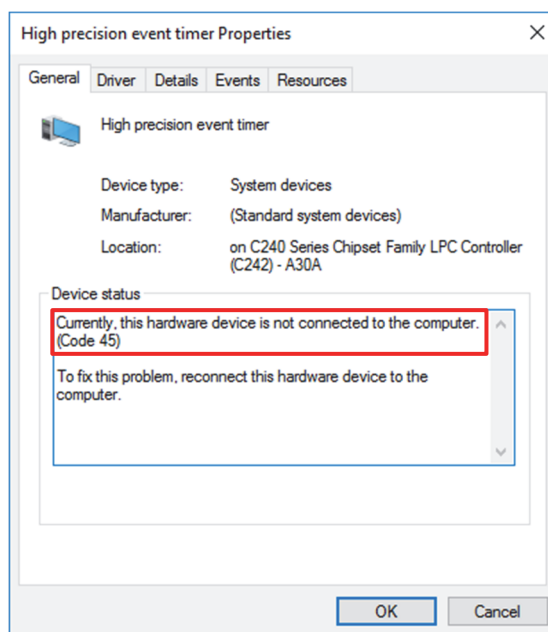
Download update module System ROM version 1.22 from the following web site and update, if System ROM version is 2.00.

<https://www.58support.nec.co.jp/global/download/055042-G02/index.html>

● High Precision Event Timer (HPET) is not displayed in the Windows(R) Device Manager and cannot be used

When System ROM version is earlier than 2.52, the High Precision Event Timer (HPET) is not displayed in the Windows(R) Device Manager and cannot be used.

When this issue occurs, the following message will be displayed in the properties of the High Precision Event Timer.



● About System Utilities and One-Time Boot Menu display

(1) 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 1.20 or later, it is indicated by converting 1 MB to 1048576 bytes.

(2) 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 4.11 or higher, or 3.01.04.072 or higher.
2. The version of System ROM is lower than 2.60.

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.

● When System ROM version 2.32, NVMe which was not installed will be displayed on iLO Web Interface

When updated to System ROM version 2.32, NVMe which was not installed will be displayed as the following, but cannot be used. This issue has been fixed in System ROM version 2.52.

- Firmware & OS Software - Firmware: NVMe Drive
- System Information - Storage: NVMe SSD
- System Information - Device Inventory: PCI-E Slot 1 (Product Name is displayed as Empty Slot 1)

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 version 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 version 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 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.

Don't 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

- **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.

- **About Storage Information of iLO Web Interface**

If you are using the iLO5 firmware version 3.00 or later

iLO5 may not retrieve Storage Information after server reboot.

In this case in the iLO Web Interface, under “System Information,” clicking on the “Storage” tab displays the following:
“Failed to retrieve complete storage device information. Refresh the page in a few minutes.”

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

● Caution about iLO time function

This caution is for iLO 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.

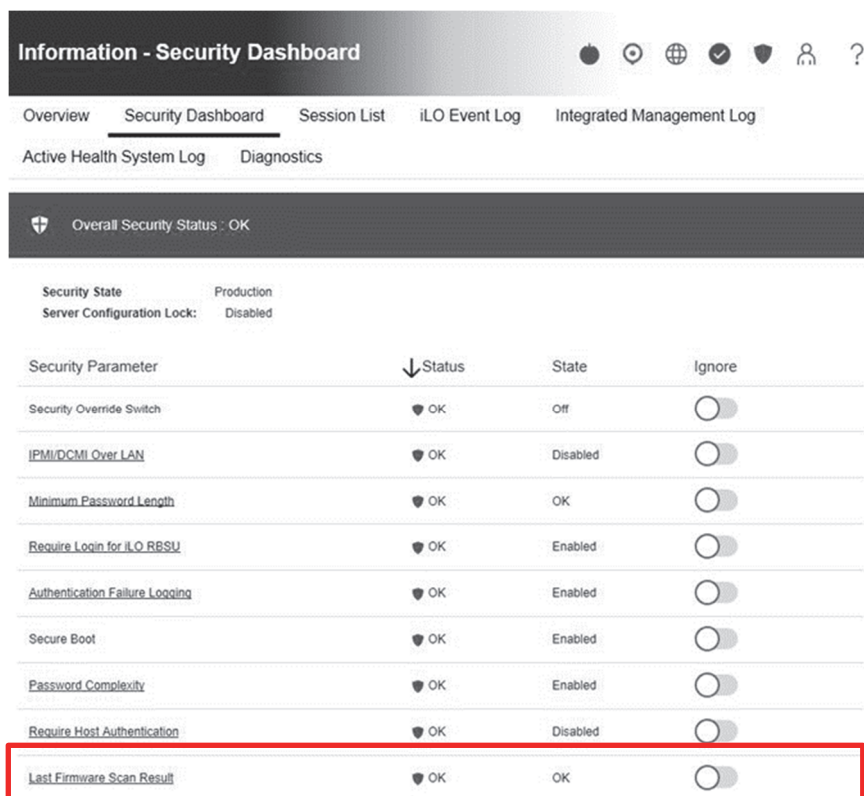
● Caution for the Security Dashboard of iLO Web Interface

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.



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

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

e.g.:

Abnormal, physical drive status change detection,iLO SNMP Trap,mgr_WIN-U6HHPNIH1Q,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)',

● Note About Rapid Setup

If you are using the iLO5 firmware version 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 version 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.

● 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."

● SNMP Alert

If you are using the iLO5 firmware version 3.00 or later

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

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

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

A: Controller location (slot number)

B: The port number of the physical drive

C: box number of the physical drive

D: The bay number of the physical drive

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

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

Error in open session response message: no matching cipher suite

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

4) Notice about the OS

● About EXPRESSBUILDER Manual Installation

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

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

● Notice of Windows Server

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

< Event Log >

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

● 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".

• 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]".

- Updating NEC ESMPRO Manager Ver 7 (Windows)

(1) Download the NEC ESMPRO Platform Management Kit from the following website.

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

- ESMPRO tab
- NEC ESMPRO Manager

(2) Launch the ESMPRO installation tool included in the ESMPRO Platform Management Kit.

(3) On the "Installation Tools screen" click on "Instructions", then from Software Manuals click on "ESMPRO/ServerManager".

(4) Click on "ESMPRO/ServerManager Ver.7 Installation Guide (Windows)".

(5) For more details on "Update NEC ESMPRO Manager from Ver 6 to Ver 7", refer to Chapter 2 Installation in "NEC ESMPRO Manager Ver. 7 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 Lower than 1.4.0	It is impossible to detect a failure of the hardware added along with the update of hardware and to issue an alert of this failure. * If iLO Receiving Information has been updated and NEC ESMPRO Manager has not been updated, it is impossible to detect the failure of the added hardware and issue the alert of the failure, as with the above.
	iml_en.mtb Lower than 1.5.0	
	* There are 2 kinds of iLO Receiving Information.	

- Updating iLO Receiving Information
 - (1) Download the latest version of iLO Receiving Information (ilo_en.mtb, iml_en.mtb) from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows) Receiving Information
 - iLO.zip
 - (2) Delete current Receiving Information from Express Report Service (MG) (Windows).
 For details refer to “3.1.5 Setting for Receiving Information” or “3.2.4 Setting for Receiving Information” in “Express Report Service (MG) Installation Guide (Windows)”.
 - (3) Set the latest version of Receiving Information downloaded in step (1) to Express Report Service (MG)
- * Download “Express Report Service (MG) Installation Guide (Windows)” from the following website.
<https://www.58support.nec.co.jp/global/download/index.html>
 - ESMPRO tab
 - Express Report Service (MG) (Windows)
- The steps of confirmation for iLO5 firmware version
 - Server Health Summary
 Push the UID button on the server and check the version of the iLO firmware on the console connected to the server.
 (For the detail, refer to Server Health Summary in iLO5 user guide.)
 - Remote
 Check the version of the iLO firmware on “Firmware & OS Software - Installed Firmware” by iLO Web Interface.
- The steps of confirming version for NEC ESMPRO Manager (Windows)
 - (1) Log in NEC ESMPRO Manager.
 - (2) Click the “About NEC ESMPRO Manager” link at the top right of the screen.
 - (3) Confirm the version information of NEC ESMPRO Manager.
- The steps of confirming version for iLO Receiving Information (ilo_en.mtb, iml_en.mtb)

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

• Note on using VMware ESXi

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 version 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 version : 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) 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

● Cautions on using Linux OS

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

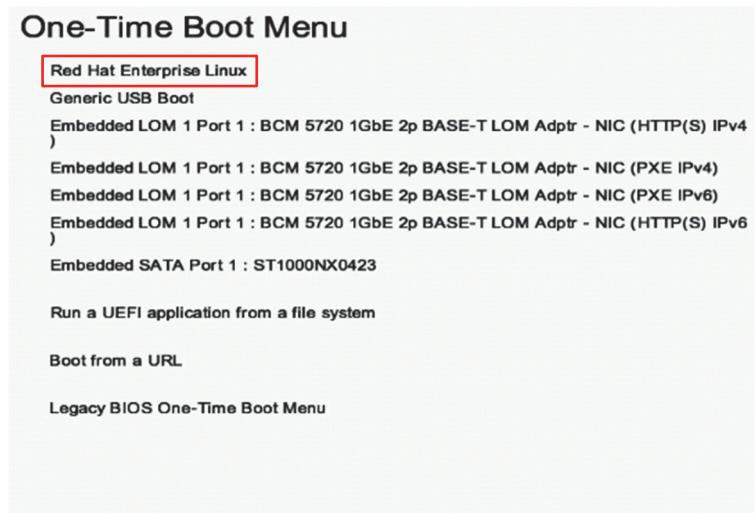
In addition, do not use the storage device name under /dev/disk/by-path/ that includes the PCI address.

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

● Cautions on using Red Hat Enterprise Linux 8.5 or earlier

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

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



One-Time Boot Screen

5) Notice of the function in general

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



【Important】 Product ID is the model number like "N8100-xxxxF". 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]

● 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.

● Changing the cooling setting

This topic pertains to the following HDDs:

N8150-551 300GB 15K Hot Plug 2.5-inch SAS HDD
N8150-552 600GB 15K Hot Plug 2.5-inch SAS HDD
N8150-553 900GB 15K Hot Plug 2.5-inch SAS HDD
N8150-602 900GB 15K Hot Plug 2.5-inch SAS HDD

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

Procedure for changing the setting

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

Note:

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

● Notes of using SAS controller (N8103-184)

(1) When using N8103-184, "Status" of iLO Web Interface [System Information] > [Storage] > [Storage Controller] is might display to "Unknown", but it does not affect server operation and SAS Controller operation.

(2) Please keep the following restrictions when using N8103-184.

- Number : Up to 1pc can be installed. Mixing with other cards is still possible.
- Installed PCI slot : slot 1.

● About FCoE function in N8104-173

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

The FCoE function is enabled in spite of the LOM firmware version.

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

● 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.

● About the Intel(R) Software Guard Extensions (SGX) option

The CPUs that support this function are only the following two types of CPUs.

Even if Intel(R) Software Guard Extensions (SGX) option is displayed on the other CPUs, please do not change from Disabled (default value) setting.

This function is not supported except for the following 2 types of CPU.

- N8101-1507 (4C/E-2174G)
- N8101-1518 (6C/E-2186G)

● About the setting when the N8117-12 Management Lan with Serial kit are installed

When the option of the N8117-12 (Management Lan with Serial kit) are installed and the management LAN is used, change the setting as follows.

Procedure to change settings

In the System Utilities, select System Configuration > BMC Configuration Utility > Network Options > Network Interface Adapter > [ON]

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 2.32 or later.

(2) 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 2.32 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
Minimum Processor Idle Power Core C-State	[C6 State] C3 State C6 Without C1E State (*1) C1E State No C-states	You can only configure this option if Workload Profile is set to Custom. Use this option to select the lowest idle power state (C-state) of the processor that the operating system uses. The higher the C-state, the lower the power usage of that idle state. (C6 is the lowest power idle state supported by the processor).

[]: Default setting

*1: the parameter usable with System ROM version 3.10 or later.

(4) Trusted Platform Module Options Menu

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

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

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

[]: Default setting

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

B) Errata Information

■ Errata Information for Express5800/ R110j-1 Maintenance Guide

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

	Error	Correct
P.39 Troubleshooting	[?] Lost Serial Number and Product ID → If the server loses Serial Number and Product ID, recover them as follows:	[?] Lost Serial Number and Product ID → If the server loses Serial Number and Product ID (*), recover them as follows: (*) Product ID is the model number like "N8100-2602F". Product ID is not PID

■ Correction of DIMM installation order

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

Correction point

- Express5800/R110j-1 User's Guide
Chapter 2 Preparations 1.8 DIMM 1.8.2 DIMM installation order

DIMM installation order

The following table describes the DIMM population order.
You should install in turn from large capacity DIMM.

DIMM slot number	1	2	3	4
DIMM Mounted number and installation order	1 DIMM		1	
	2 DIMM	2	1	
	3 DIMM	2	1	3
	4 DIMM	2	4	3

- 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) N8102-719 > N8102-718 (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 18th Edition

CBZ-022445-006-11