

Express5800/T120h (2nd-Gen) ご使用時の注意事項

このたびは弊社製品をお買い上げいただき、誠にありがとうございます。
本製品のご使用において、ご注意いただくことがあります。誠にそれ入りますが、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
- 2) システム ROM の機能に関する注意事項
- 3) iL05 の機能に関する注意事項
- 4) OS に関する注意事項
- 5) 全般の機能に関する注意事項
- A) ファームウェア変更に伴う変更点

1) はじめに

● 本製品のマニュアルについて

本製品に関する詳細は、以下の Web サイトに掲載しているマニュアルに記載しています。

<https://www.support.nec.co.jp/>

「NEC サポートポータル内検索」で、「3170102319」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 S8.10-006.04 以降を適用してください。

<https://www.support.nec.co.jp/>

(「NEC サポートポータル内検索」より、「S8.10-006」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=5 または 7), 7.0 版, 8.0 版)」を適用してください)

(3) VMware ESXi デバイスドライバ

<https://www.support.nec.co.jp/View.aspx?id=3140105866>

(「PC サーバ/ブレードサーバ (Express5800 シリーズ)」から対象 OS の「デバイスドライバー一覧」を選択)

● 本製品の保守作業時間に関して

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

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。

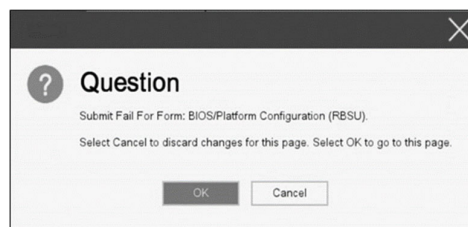
(*1) BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Order Control

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

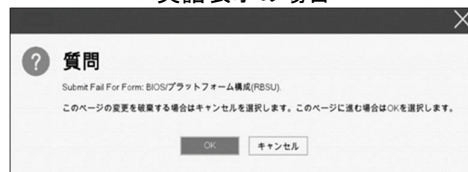
● Submit Fail For Form の Question(質問)ポップアップ表示についての注意事項

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 などの設定情報を消失することがあります。



英語表示の場合

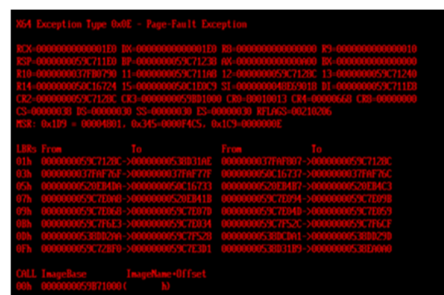


日本語表示の場合

● 赤文字画面 (RSoD : Red Screen of Death) が表示された場合の対処について

装置の構成変更や設定変更などシステムの状態を変更した場合や、接続デバイスへのアクセスタイミングにより、OS 起動前にまれに赤文字画面 (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のオフ、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、装置の電源オフ、オンを実施してください。
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。



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 (7.4.3 システム設定をデフォルト値に戻す)」の項をご参照ください。

● **シリアルコンソールに POST デバッグ情報が出力される件について**

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

システム ROM バージョン 2.34 (04/09/2020) では、この問題が修正されています。

● Server Configuration Lock (SCL)についての注意事項

- (1) システム運用中は SCL 機能を無効にし、使用しないでください。
- (2) SCL 機能有効時に設定するパスワードは大切に保管してください。SCL のパスワードを紛失した状態で、SCL 機能によりロック (OS ブート前に停止) されると、ロック解除できず、二度とブートできなくなります。
ブート可能状態への復旧/回復は有償にて承ることになります。
なお、SCL のパスワードを紛失した場合、SCL のパスワードをクリアする方法はありません。
- (3) 保守を依頼する際は、SCL 機能を無効化していただく必要があります。
SCL 機能を無効にできない場合、**保守は有償にて承ることになります。**
- (4) RBSU の「Halt on Server Configuration Lock failure detection.」機能は有効化しないでください。もし有効に設定した場合、SCL 機能が回復不能条件の該当を検出し、ロック (OS ブート前に停止) されてしまうと、システムユーティリティも起動できず、二度とサーバー構成ロックを無効にすることができません。
ブート可能状態への復旧/回復は有償にて承ることになります。

SCL 機能の回復不能条件

- RBSU の設定変更によりロックされた場合
- ファームウェア更新によりロックされ、元のファームウェア バージョンに戻すことができない場合
- DIMM、または PCI オプションカードの故障によりロックされた場合

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

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

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

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

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

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

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

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

● 工場出荷時の設定について

以下の項目については、工場出荷時に以下のように設定しています。

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

● iLO イベントログ (IEL) に IPMI Watchdog Timer Timeout のログが登録される。

システム ROM バージョン 2.62 (03/08/2022) が適用されている場合、かつ IPMI Watchdog Timer オプションを「Disabled (出荷時の設定)」に設定している場合、iLO イベントログに下記の IPMI Watchdog Timer Timeout が登録されることがあります。

以下の手順を実施することで本問題が解消します。

iLO IPMI Watchdog Timer Timeout: Action: None, TimerUse: 0x44, TimerActions: 0x00

イベントクラス: 0x23

イベントコード: 0xB3

復旧手順:

以下の復旧手順 1、または 2 のどちらかを実施していただくことで、本問題が解消できます。

復旧手順 1

(1) 装置の電源をオフにした後、電源コードをコンセントから外す。

(2) 30 秒以上経過したのち、電源コードをコンセントに接続する。

復旧手順 2

システムユーティリティより、IPMI Watchdog Timer オプションの設定を 2 回変更します。

(1) POST 中に<F9>キーを押下し、システムユーティリティを起動する。

(2) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timer オプション を「Enabled」に設定する。

(3) <F12>キーを押下し、設定を保存してシステムを再起動する。

(4) POST 中に<F9>キーを押下し、システムユーティリティを起動する。

(5) System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timer オプションを「Disabled」に設定する。

(6) <F12>キーを押下し、設定を保存してシステムを再起動する。

● システムユーティリティおよびワнтаイムブートメニューの表示について

- (1) BMC Configuration Utility 配下のメニューの変更権限については、BMC Configuration Utility > Setting Option > Require user login and configuration privilege for BMC Configuration を有効にすることで保護してください。
BIOS/Platform Configuration (RBSU) > Server Security > Set Admin Password の設定では保護されません。
- (2) System Information > Processor Information で表示される L2 Cache、L3 Cache の Maximum Size、Installed Size は 1MB を 1048576 バイトに換算した数値で表示されます。
- (3) 以下の発生条件を満たす場合、ワнтаイムブートメニューと RBSU の PCIe Device Configuration メニュー(*) に、RAID コントローラ名が正しく表示されないことがあります。RAID コントローラ名表示のみの問題であり、RAID コントローラに搭載されている HDD/SSD からのブートには影響しません。

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

【発生条件】

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

以下 2 つの条件をすべて満たす場合、発生します。

1. RAID コントローラファームウェアが v4.11 以降、または v3.01.04.072 以降
2. システム ROM 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)
- ・ 2.32 (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、本体装置の電源オフ、オンを実施してください。

＜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ません。

なお、本設定は Set to factory defaults オプションから iLO を出荷時のデフォルト設定にリセットを行った場合においても、リセットされず『Permanently disallow downgrades』を維持します。

● iLO のセキュリティ機能の注意事項

iLO Web インターフェイスの [Information] > [Security Dashboard] および iLO Web インターフェイス画面の右上部に  リスクが表示される場合があります。

RBSU の設定や iLO の設定の内容によって、iLO セキュリティの状態がリスク状態 (赤色) で表示されますので、お客様のセキュリティポリシーに応じてセキュリティの対処を行ってください。

推奨値などの詳細については、iLO5 ユーザーズガイドを参照してください。

ただし、『Require Host Authentication』設定については、本書内の「iLO Web インターフェイスから、[ホスト認証が必要] 設定を有効(※)に設定した場合の注意事項」に記載がありますので、ご確認ください。

iLO の負荷の状態により [Information] > [Security Dashboard] の”全体セキュリティステータス”が『リスク』であっても、iLO Web インターフェイス画面の右上部の”iLO セキュリティ”アイコンが無色になる場合があります。[Information] > [Security Dashboard] の”全体セキュリティステータス”が現在のセキュリティ状態を示します。

● iLO Web インターフェイスから、[ホスト認証が必要]設定を有効(※)に設定した場合の注意事項

(※) iLO5 ファームウェアバージョン : 1.40 以降を適用した環境の場合が対象となります。

[Security] > [Access Settings] > [iLO]にある[ホスト認証が必要/Require Host Authentication]を『有効』に設定しないでください。

設定を行った場合、次に示す状況が発生します。

- ・アラートビューアに、“Remote Insight/Integrated Lights-Out 認証されないログイン試行検出”のメッセージが多数表示されます。
- ・Starter Pack (Standard Program Package)を適用するとエラーが発生します。

また、次のサービスや機能をご利用いただけません。

- ・エクスペ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 (N8116-83) 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.”

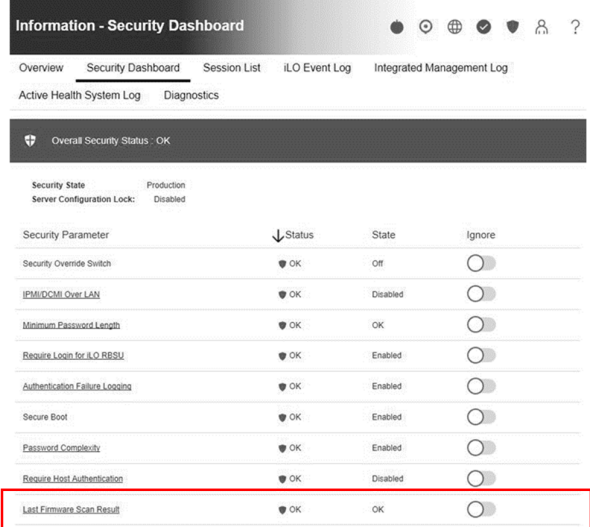
上記メッセージがストレージ情報ページに表示された場合、iLO リセットを行ってください。

● 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。



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]-[インテグレートドマネジメントログ]で同じイベントのロケーション情報をご確認ください。

例 : Abnormal, physical drive status change detection, iLO SNMP Trap, mgr_WIN-U6HIHPNIH1Q, uru-rhel83, 192.168.0.57, 2021/10/01 15:22:57, iLO, 0xc0000be6, "A physical drive status change has been detected. Current status is 3. (Location: port 12 Controller: Slot 12)", "If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

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

iLO Web インターフェイスの[System Information] > [Summary] > [Subsystem and Devices]の Agentless Management Service (AMS)のステータスにおいて、不明(または利用不可能)※と表示された場合、iLO リセットを行ってください。また、その後、10 分程度経過した後、以下の Agentless Management Service (AMS)の再起動方法の対象 OS を参考に、Agentless Management Service (AMS)を再起動してください。

※ Agentless Management Service (AMS)のステータスが不明(または利用不可能)の状態の場合、iLO Web インターフェイスの[System Information] > [Storage]や[Network]の一部の情報が取得できず、正しく表示されません。

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

・ Windows の場合

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

・ Red Hat Enterprise Linux 7.x/8.x の場合

以下のコマンドを実行します。

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

・ ESXi 6.5/6.7 の場合

以下のコマンドを実行します。

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

※ お使いの AMS バージョンによりコマンドが異なります。

・ ESXi 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

iL05 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 Array 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

iL05 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

iL05 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

iL05 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

● 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

iLO5 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
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(ilo_jp.mtb、iml_jp.mtb)をダウンロードします。

<https://www.support.nec.co.jp/View.aspx?id=9010100096>

ilo_jp.mtb、iml_jp.mtb は MGMTB.zip に包含しています。

- (2) 「エクスプレス通報サービス (MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で登録済みの受信情報を削除します。
- (3) (1) でダウンロードした最新版の受信情報設定ファイルを登録します。
「エクスプレス通報サービス (MG) インストレーションガイド(Windows 編)」は以下の Web サイトからダウンロードしてください。

<https://www.support.nec.co.jp/View.aspx?id=9010102124>

◆ iLO5 ファームウェアのバージョン確認方法

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

◆ ESMPRO/ServerManager (Windows 版) のバージョン確認方法

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

◆ iLO 管理機能向けの受信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) インストールガイド (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 を使用する場合の注意事項

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

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

- Cooling Unit 1 Fans

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

- System Chassis 1 UID

● VMware ESXi で TPM キットを使用する場合の注意事項

システム ROM 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、赤文字画面(RSoD)が発生することがあります。

One-Time Boot Menu

```
Red Hat Enterprise Linux
Generic USB Boot
Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (HTTP(S) IPv4
)
Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (PXE IPv4)
Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (PXE IPv6)
Embedded LOM 1 Port 1 : BCM 5720 1GbE 2p BASE-T LOM Adptr - NIC (HTTP(S) IPv6
)
Embedded SATA Port 1 : ST1000NX0423

Run a UEFI application from a file system

Boot from a URL

Legacy BIOS One-Time Boot Menu
```

ワンタイムブートメニュー画面

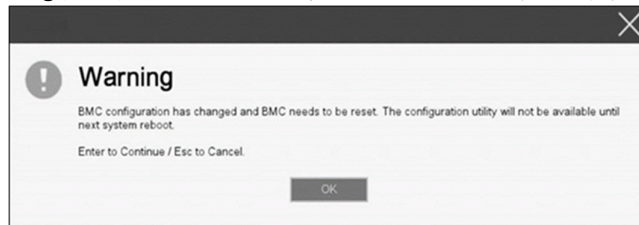
5) 全般の機能に関する注意事項

● 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

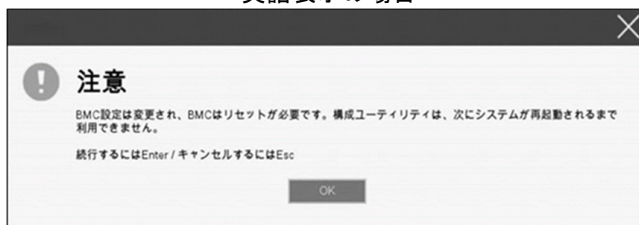
システムユーティリティの「BMC Configuration Utility」での操作において、以下の(1)のポップアップが表示された場合は(2)以降の手順を厳守してください。

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。



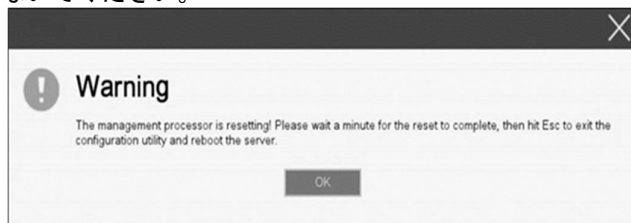
英語表示の場合



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



【重要】Product ID とは、『N8100-2783Y』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。

● N8116-83 SAS エクスパンダカード ご使用時の注意事項

Starter Pack Version S8.10-009.01 に含まれている、N8116-83 SAS エク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。

● 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>

A) ファームウェア変更に伴う変更点

■ BIOS/Platform Configuration (RBSU) メニューの変更について

本製品の搭載ファームウェアの更新に伴い、メニューの一部に変更があります。
下記、変更点を記載します。

(1) Server Availability メニュー

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

追加のオプションについて、次の表を参照してください。

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

[]: 出荷時の設定

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

(2) Power and Performance Options メニュー

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

追加のオプションについて、次の表を参照してください。

オプション	パラメーター	説明
Energy Performance Preference (注 1)	[Disabled] Enabled	このオプションを使用して、エネルギーパフォーマンス優先を有効または無効にします。ご使用の環境でベンチマークを実施し、パフォーマンスの向上を確認した上で、本オプションを有効にしてください。

[]: 出荷時の設定

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

(3) Server Security メニュー

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

追加のオプションについて、次の表を参照してください。

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

[]: 出荷時の設定

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

(a) 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 以降にて追加されるオプションです。

■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 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。
