

iStorage NS300Ri ご使用時の注意事項

このたびは弊社製品をお買い上げいただき、誠にありがとうございます。

本製品のご使用において、ご注意いただくことがあります。誠におそれ入りますが、ご使用前に下記内容を必ずご一読ください。

なお、本書は必要なときにすぐに参照できるよう大切に保管してください。

- 1) はじめに
- 2) システムROMの機能に関する注意事項
- 3) iLO 5の機能に関する注意事項
- 4) OSに関する注意事項
- 5) 全般の機能に関わる注意事項
- 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、「3170102338」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. 10-007. 01 以上を適用してください。

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

(「NEC サポートポータル内検索」より、「S8. 10-007」を検索)

● 本製品の保守作業時間に関して

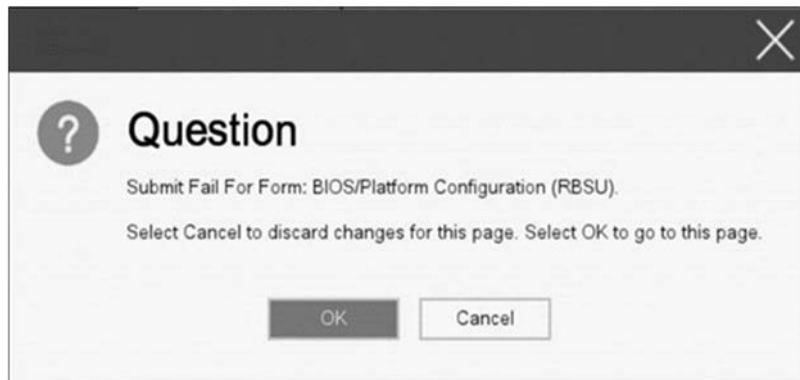
本製品は、障害発生時等に伴う保守作業に際し、保守部材と搭載ファームウェア、ドライバの組み合わせによっては、保守作業に時間を要することがあります。

2) システムROMの機能に関する注意事項

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

システムユーティリティにおいて設定の変更中に、次のSubmit Fail For FormのQuestion(質問)ポップアップが表示された場合は、「キャンセル」を選択して変更を破棄してください。

さらに、サーバーの再起動を行ってシステムユーティリティに入りなおしてから設定の変更を再度行ってください。もし「OK」を押してそのまま設定変更を進めると、装置に記録されているSerial Number、Product IDなどの設定情報を消失することがあります。



英語表示の場合



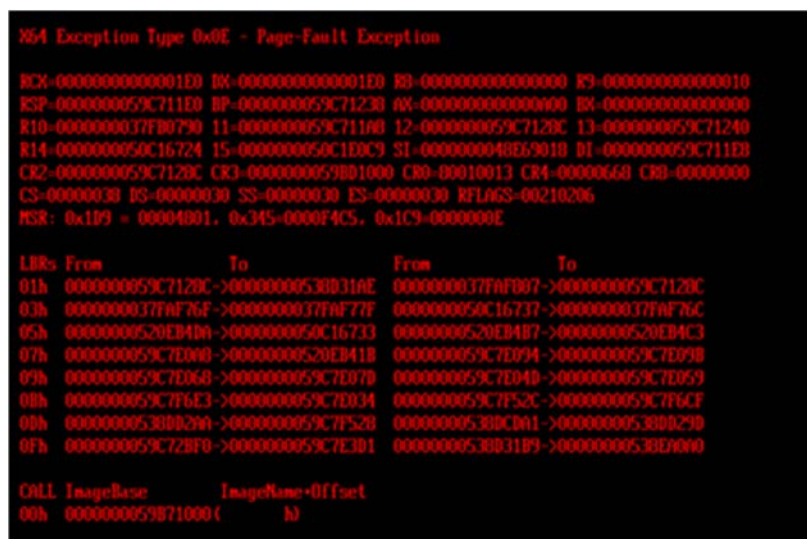
日本語表示の場合

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

装置の構成変更や設定変更などシステムの状態を変更した場合や、接続デバイスへのアクセスタイミングにより、OS起動前に稀に赤文字画面 (RSOD) が表示され、本製品の操作が出来なくなることがあります。構成変更や設定変更に伴う一過性の事象の場合があり電源OFF/ONによって回復します。

赤文字画面 (RSOD) が表示された場合、装置の電源OFF/ONをお願いします。

問題が解決しないときは、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

● 「Memory Initialization Start」のメッセージでPOST停止した場合の対処について

「Memory Initialization Start」のメッセージでPOST停止した場合、システムメンテナンススイッチのSW6によりシステム設定をデフォルト値に戻すことで復旧することができます。

詳細な手順は、メンテナンスガイド「1章(7.4.3 システム設定をデフォルト値に戻す)」の項をご参照ください。

● シリアルコンソールにPOSTデバッグ情報が出力される件について

システム ROM v2.32 (03/09/2020)において、POST 実行時、まれに POST デバッグ情報がシリアルポートに出力され、POST 実行時間がおおよそ2分長くなることがあります。

システム ROM v2.34 (04/09/2020)では、この問題が修正されています。

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

- (1) システム運用中は SCL 機能を無効にし、使用しないでください。
- (2) SCL 機能有効時に設定するパスワードは大切に保管してください。SCL のパスワードを紛失した状態で、SCL 機能によりロック (OS ブート前に停止) されると、ロック解除できず、二度とブートできなくなります。

ブート可能状態への復旧/回復は有償にて承ることになります。

なお、SCL のパスワードを紛失した場合、SCL のパスワードをクリアする方法はありません。

- (3) 保守を依頼する際は、SCL 機能を無効化していただく必要があります。
SCL 機能を無効にできない場合、**保守は有償にて承ることになります。**
- (4) RBSU の「Halt on Server Configuration Lock failure detection.」機能は有効化しないでください。もし有効に設定した場合、SCL 機能が回復不能条件の該当を検出し、ロック (OS ブート前に停止) されてしまうと、システムユーティリティも起動できず、二度とサーバー構成ロックを無効にすることができません。

ブート可能状態への復旧/回復は有償にて承ることになります。

SCL 機能の回復不能条件

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

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

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

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

● フォールトトレラントメモリ機能(ADDDC) の仕様変更について

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

- CPUあたりDIMM 8枚、もしくはDIMM 12枚以外の構成であっても、フォールトトレラントメモリ機能(ADDDC)が使用できる構成であれば、本機は自動的に設定変更し、同機能の使用を始めます。
- 各チャネルあたりのRANK数の合計が2以上になるようにメモリを搭載しなくても、フォールトトレラントメモリ機能(ADDDC)は利用できます。

● Extended Memory Testオプションの設定値について

システム ROM のバージョンが v2.36 (07/16/2020) の場合、Extended Memory Test オプションは、自動的に Disabled となります。

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

● 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 バージョンが v2.32 (03/09/2020) 未満の場合、Embedded SATA Configuration 設定(*1)を[Smart Array SW RAID Support]設定時、運用環境により Disk Utilities メニュー(*2)に内蔵 DVD ドライブ情報が2個表示されます。

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

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

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

● 工場出荷時の設定について

以下の項目については、工場出荷時に以下のように設定しています。

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

● 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 バージョンが v2.10 (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。

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

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

*2 :



*3 :



3) iLO 5の機能に関する注意事項

● iLOの再起動を行う場合の注意事項

サーバー起動からOSの起動完了までの間(POST (Power On Self Test)実行中も含みます)は、iLOの再起動を行わないでください。

また、システムユーティリティの操作途中も、iLOの再起動を行わないでください。

該当タイミングでiLOの再起動を行うと、期待しない動作となる場合があります。

たとえばシステムユーティリティの設定変更途中にiLOの再起動(※)を行うと、直後のシステム再起動処理(Reboot)が正常に動作しない場合や、装置に記録されているSerial Number、Product IDなどの設定情報を消失することがあります。また、POST (Power On Self Test)実行中にiLOの再起動を行うと、iLO Webインターフェース: [Information] - [Overview]ページにおけるUUID、UUID(論理)が不正な表示になる場合があります。不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

＜対象となるiLOの再起動の方法＞

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

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

● iLOのダウングレードポリシー機能の注意事項

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

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

なお、本設定はSet to factory defaultsオプションからiLOを出荷時のデフォルト設定に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インターフェースの[Information] - [Security Dashboard]およびiLO Webインターフェース画面の右上部に  リスクが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、お客様のセキュアポリシーに応じてセキュリティの対処を行ってください。

推奨値などの詳細については、iLO 5ユーザーズガイドを参照してください。

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

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

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

(※) [Security] - [Access Setting] - [iLO]にある[ホスト認証が必要/Require Host Authentication]を『有効』に設定する。

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。

(次ページへ続く)

また、次のサービスや機能をご利用頂けません。

- ・ エクスプレス通報サービスにおいてハードウェア障害に関する通報
- ・ RAID 通報
- ・ サー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

iLO 5ファームウェア1.45以下で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インターフェースにてSNTPの設定を行い、ご使用いただくことを推奨します。

iLOのSNTPの設定方法については、iLO 5ユーザーズガイドを参照してください。

● iLO WebインターフェースのUUID不正値表示について

POST (Power On Self Test) 実行中にiLOの再起動を行うと、iLO Webインターフェースの[Information] - [Overview] ページのUUID、UUID(論理)の値が稀に不正な表示となることがあります。

不正な表示となった場合は、本体装置の電源をオフ、オンしてください。

● iLO Webインターフェースの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インターフェー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、読み替えてご利用ください。

● iLO WebインターフェースのVirtual NIC設定の注意事項

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

- (1) iLO 5ファームウェア : 2.10以上 2.18以下をご使用の場合、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上のデバイスマネージャーで「Virtual NIC」が警告表示される場合があります。
[Security] - [iLO]の“Virtual NIC”の設定を『無効(Disabled)』に変更してください。
- (2) iLO 5ファームウェア : 1.40以上 1.47以下、もしくは、2.31以上をご使用の場合、デフォルト値は『無効(Disabled)』です。

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

iLO 5ファームウェア : 2.10以上 2.18以下をご使用の場合、Windows OS上でvEthernet (Hyper-V Virtual Ethernet Adapter)が構成されている場合、iLO Webインターフェースの[Information] - [Network] - [Physical Network Adapters]において、構成されている各[Adapter]の[Network Ports]の“IPv6 Address”において正しいIPv6アドレスが表示されない場合があります。vEthernet構成時のIPv6アドレスに関しては、OS上のネットワークアダプタのプロパティにてご確認ください。

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

ネットワークをブリッジ設定で構成し、iLO 5ファームウェア : 2.31以上をご使用の場合、iLO Webインターフェースの[Information] - [Network] - [Physical Network Adapters]に表示される内容がOS上の内容と一致しない場合があります。ブリッジ情報の詳細は、OS上のネットワークアダプタのプロパティにてご確認ください。

● iLO WebインターフェースのDevice Inventory情報の表示について

〈LOMカード (N8104-193/194/195) 構成時〉

システムROMのバージョン2.34 (04/08/2020) 以下をご使用の場合、iLO Webインターフェースの[Information] - [Device Inventory]において、LOM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、サーバの運用およびLOMカードの動作に影響はありません。

- Location : Unspecified
- Firmware Version : N/A
- Status : Unknown

〈SASエクスパンダカード (N8116-84) 構成時〉

iLO 5ファームウェア: 2.31以上をご使用の場合、iLO Webインターフェースの[Information] - [Device Inventory]において、SASエク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、サーバの運用およびSASエク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インターフェースのセキュリティダッシュボードの注意事項

iLO 5ファームウェア1.45以上、2.10未満をご使用の場合、[Information] - [Security Dashboard]に[Last Firmware Scan Result]が表示されますが、本ハイパーリンクをクリックしないでください。

誤ってクリックした場合、Webサイト内のメニュー間移動が出来なくなります。その場合、ブラウザのリロードボタンをクリックするか、もしくはいったんiLO Webインターフェースのログアウトを実行して再度ログインしてください。

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	<input type="checkbox"/>
IPMI/DCMI over LAN	♥ OK	無効	<input type="checkbox"/>
最小パスワード長	♥ OK	OK	<input type="checkbox"/>
iLO RBSUへのログイン要求	♥ OK	有効	<input type="checkbox"/>
認証失敗ログ	♥ OK	有効	<input type="checkbox"/>
セキュアブート	♥ OK	有効	<input type="checkbox"/>
パスワードの複雑さ	♥ OK	有効	<input type="checkbox"/>
ホスト認証が必要	♥ OK	無効	<input type="checkbox"/>
最新のファームウェアスキャン結果	♥ OK	OK	<input type="checkbox"/>

日本語表示の場合

(次ページへ続く)

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	<input type="checkbox"/>
IPMI/DCMI Over LAN	♥ OK	Disabled	<input type="checkbox"/>
Minimum Password Length	♥ OK	OK	<input type="checkbox"/>
Require Login for iLO RBSU	♥ OK	Enabled	<input type="checkbox"/>
Authentication Failure Logging	♥ OK	Enabled	<input type="checkbox"/>
Secure Boot	♥ OK	Enabled	<input type="checkbox"/>
Password Complexity	♥ OK	Enabled	<input type="checkbox"/>
Require Host Authentication	♥ OK	Disabled	<input type="checkbox"/>
Last Firmware Scan Result	♥ OK	OK	<input type="checkbox"/>

英語表示の場合

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

物理ドライブのステータス変更時のSNMPトラップ通知において、ロケーション情報が欠損する場合があります。ロケーション情報に関しては、iLO5 webインターフェースの[情報]-[インテグレー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-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: ot 12 Controller: Slot 12)", "If the physical drive status is 'failed(3)', 'predictiveFailure(4)',

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

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

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

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

○ Windowsの場合

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

○ Red Hat Enterprise Linux 7.x/8.xの場合

以下のコマンドを実行します。

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

(次ページへ続く)

○ ESXi6.5/6.7の場合

以下のコマンドを実行します。

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

※ お使いのAMSバージョンによりコマンドが異なります。

○ ESXi7.0の場合

以下のコマンドを実行します。

```
# /etc/init.d/amsd restart
```

4) OSに関する注意事項

● 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iLOファームウェアバージョンと、ESMPRO/ServerManager (Windows版) およびエクスプレス通報サービス (MG) のバージョンの組み合わせによってはESMPRO/ServerManager (Windows版) およびiLO管理機能向けの受信情報設定ファイルのアップデートが必要になる場合があります。

以下をご参照のうえ、アップデートが必要な場合は、最新バージョンにアップデートしてください。

各バージョンの確認方法については、本注意事項の末尾に記載します。

◆ESMPRO/ServerManager (Windows版) に関する発生現象

iLO ファームウェア	ESMPRO/ ServerManager (Windows版)	発生現象
Version 2.10 以上	Version 6.25 未満	<ul style="list-style-type: none">構成タブ - サーバー状態 “SNMP 通報設定” が “取得に失敗しました” と表示されるリモート制御タブ - iLO 情報 - IML の表示、IML の保存 IML 情報の取得に失敗し、表示および保存ができないアラートビューア ファームウェアアップデートにともない追加されたハードウェアの障害がアラートビューアに “不明タイプ” のアラートとして表示される
	Version 6.47 未満	<ul style="list-style-type: none">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>

(次ページへ続く)

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

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

- (1) 以下の Web サイトより ESMPRO Platform Management Kit をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010109532>
ESMPRO/ServerManager Ver. 7 は ESMPRO Platform Management Kit に含まれています。
- (2) ESMPRO Platform Management Kit の ESMPRO インストールツールを起動します。
- (3) インストールツール画面の説明書をクリックし、Software Manuals から ESMPRO/ServerManager をクリックします。
- (4) 「ESMPRO/ServerManager Ver. 7.00 インストレーションガイド(Windows 編)」をクリックします。
- (5) 「ESMPRO/ServerManager Ver. 7 インストレーションガイド(Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager を Ver. 6 から Ver. 7 へアップデートします。

◆iLO 管理機能向けの受信情報設定ファイルに関する発生現象

※エクスプレス通報サービス (MG) をご利用されている方が対象です。

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

◆iLO 管理機能向けの受信情報設定ファイルのアップデート方法

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

◆iLO ファームウェアのバージョン確認方法

- ・Server Health Summary で確認する方法
サーバー本体の UID ボタンを押下して、サーバーに接続されたコンソールに表示される iLO Firmware のバージョンを確認します (Server Health Summary の詳細は iLO 5 ユーザーズガイド参照)。
- ・ネットワーク経由で確認する方法
iLO にネットワーク接続可能な場合、ブラウザから iLO にログインして、メニュー「ファームウェア & OS ソフトウェア」から iLO のバージョンを確認します。

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

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

◆iLO 管理機能向けの受信情報設定ファイルのバージョン確認方法

「エクスプレス通報サービス (MG) インストレーションガイド(Windows 編)」の「3.1.5 受信情報の設定」または「3.2.4 受信情報の設定」を参照して受信情報の設定画面で「詳細情報」が「iLO SNMP Trap」のバージョンを確認します。

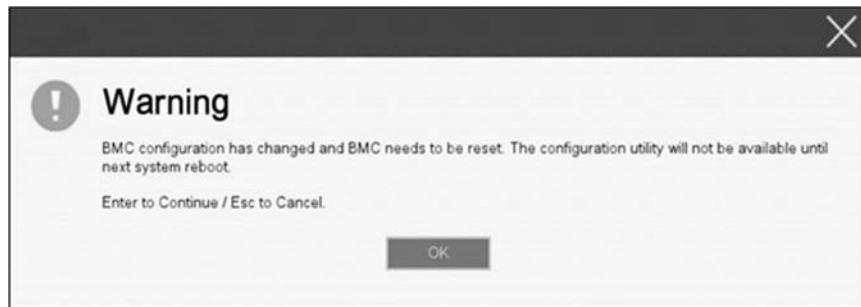
5) 全般の機能に関わる注意事項

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

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

注意事項に従った操作を実施されない場合、「Memory Initialization Start」のメッセージでPOST停止、あるいは、装置に記録されているSerial Number、Product IDの消失が発生する場合があります。

- (1) システムユーティリティの「BMC Configuration Utility」において設定の変更を行うと、iLOの再起動を行うために、次のWarning（注意）ポップアップが表示されることがあります。

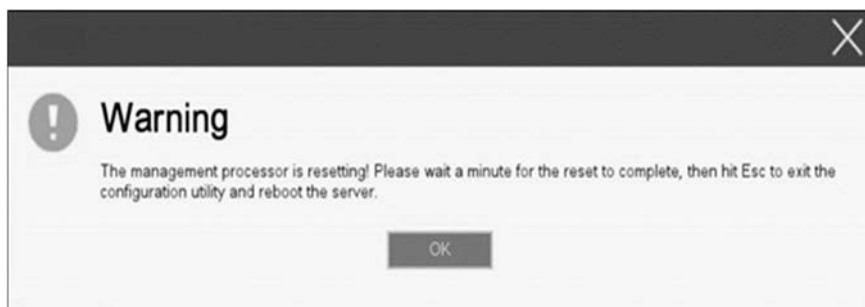


英語表示の場合



日本語表示の場合

- (2) 「OK」を押して進めます。
(3) 次のWarning（注意）ポップアップが表示されます。
このWarning（注意）ポップアップが表示されている状態にて、**必ず1分以上お待ちください。**
その間、何も操作しないでください。



英語表示の場合



日本語表示の場合

(次ページへ続く)

- (4) 1分以上経過後、装置前面のステータスランプが緑色で点灯していることを確認してください。
 ※ iLOが再起動中 : ステータスランプが緑色で点滅 (毎秒1回)
 iLOの再起動が完了し正常動作 : ステータスランプが緑色で点灯
- (5) 再起動の完了が確認できたら、「OK」を押してください。
- (6) <ESC>キーを複数回押してシステムユーティリティの画面に戻ります。
- (7) システムユーティリティの「Reboot the System」を選択して再起動します。

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

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

- (1) 装置の電源を切り、電源コードをコンセントから外します。
- (2) 30秒以上経過したのち、電源コードをコンセントに接続します。
- (3) POWERスイッチで装置の電源をONにします。
- (4) サーバーが起動し、POST画面が表示されます。
- (5) <F9>キーを押してシステムユーティリティを起動します。もし、システムユーティリティが起動できない状態になっている場合は、「1章(7.4.3 システム設定をデフォルト値に戻す)」を参照し、システムメンテナンススイッチを操作して、RBSU設定の初期化をします。
- (6) システムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、Serial NumberとProduct IDの値を確認します。
- (7) Serial NumberとProduct IDの値が期待する値の場合は、手順14)に進みます。
- (8) Serial NumberとProduct IDの値が期待する値ではない(消失している)場合は、システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options」を選択します。
- (9) 「Restore Default Manufacturing Settings」を選択します。
- (10) 「Yes, restore the default settings.」を選択します。
- (11) 自動的に装置が再起動し、POST画面が表示されます。
- (12) <F9>キーを押してシステムユーティリティを起動します。
- (13) 装置のスライドタグに記載されているSerial NumberとProduct IDをシステムユーティリティの「System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options」メニューより、設定します。



【重要】Product IDとは、『N8100-255Y』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。

● N8104-195 10GBASE-T 接続 LOM カード ご使用時の注意事項

本製品と、N8104-195 10GBASE-T 接続 LOM カードを使用する場合は、以下の設定を変更してください。

◆設定手順

System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Configuration を「Increased Cooling」に設定してください。

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

● EXPRESSBUILDER ヘルプについて

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

● サーバ診断カルテについて

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

● サーバ診断カルテの制限事項

- ・ Windows Server 2019/Windows Server 2016 でサーバ診断カルテを使用する場合は、下記の Web サイトよりモジュールをダウンロードし、インストールしてください。

NEC サポートポータル

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

A) ファームウェア変更に伴う変更点

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

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

(1) Server Availability メニュー

システムユーティリティから、「System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability」を選択すると、「Server Availability」メニューが表示されます。
追加のオプションについて、次の表を参照してください。

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

[]: 出荷時の設定

注 1: システム ROM Version 2.54 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。

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

[]: 出荷時の設定

注 1: システム ROM Version 2.54 以降にて利用できるオプションです。

B) 誤記訂正

● iStorage NS300Ri メンテナンスガイドについて

メンテナンスガイドに誤記がありましたので、以下に訂正いたします。

■誤記修正

誤)

Windows Storage Server 2016 「システムログ」			
225	Microsoft-Windows-Kernel-PnP	警告	プロセス ID XXX のアプリケーション YYY がデバイス ZZZ の取り外しまたは取り出しを停止しました。 * ZZZ は対象のデバイス インスタンス名 YYY はデバイスを使用していたプロセス名 XXX はデバイスを使用していたプロセス ID が入ります。
	OS 初回起動時、RAID カード追加後の OS 初回起動時		OS 初回起動時のみに記録される場合は、システム運用上問題ありません。

正)

Windows Storage Server 2016 「システムログ」			
225	Microsoft-Windows-Kernel-PnP	警告	プロセス ID XXX のアプリケーション YYY がデバイス ZZZ の取り外しまたは取り出しを停止しました。 * ZZZ は対象のデバイス インスタンス名 YYY はデバイスを使用していたプロセス名 XXX はデバイスを使用していたプロセス ID が入ります。
	OS 初回起動時、RAID カード追加後の OS 初回起動時、Standard Program Package 適用時		システム運用上問題ありません。

■記述追加

Windows Storage Server 2016 「システムログ」			
7031	Service Control Manager	エラー	Agentless Management Service サービスは予期せぬ原因により終了しました。 このサービスの終了は 1 回目です。次の修正操作が 60000 ミリ秒以内に実行されます：サービスの再開。
	Standard Program Package 適用時		本イベントに続けて「ソース：Service Control Manager、ID：7045」（Agentless Management Service サービスの自動的な開始）のログが記録され、その後本ログが記録されていなければ、システム運用上問題ありません。

Windows Storage Server 2016 「アプリケーションログ」			
1000	Application Error	エラー	障害が発生しているアプリケーション名：ams.exe、バージョン：x.x.x.x、タイムスタンプ：0xXXXXXXX
	Standard Program Package 適用時		同時刻にシステムイベントログに「ソース：Service Control Manager、ID：7031」が記録されており、該当イベントが問題ないと判断できる場合は、システム運用上問題ありません。

■ 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。

NEC

* CBZ-030969-301-08 *

2021年 12月 10版