

Express5800/R120h-1M (2nd-Gen), R120h-2M (2nd-Gen)

ご使用時の注意事項

この度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。誠に恐れ入りますが、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。

■ 注意事項

● 本製品のマニュアルについて

本製品に関する詳細は、下記サイトに掲載しているマニュアルに記載しています。

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

「NEC サポートポータル内検索」より、以下の ID で検索してください。

R120h-1M (2nd-Gen) : 3170102287

R120h-2M (2nd-Gen) : 3170102288

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<<http://jpn.nec.com/esmsm/>>

NEC サポートポータル<<http://www.support.nec.co.jp/View.aspx?isIntra=0&id=9010102124>>

の最新の情報およびバージョンをご確認の上、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 Web サイトに最新版が掲載されています。

Web に掲載されている内容を確認し、バージョン S8.10-006.02 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)

なお、Starter Pack バージョン S8.10-004.xx, S8.10-003.xx, S8.10-002.xx, S8.10-001.xx (xx は任意の数字) は使用できません。

● 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 Web サイトに最新版が掲載されています。Web 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】と表示された【Agentless Management Service および iLO Channel Interface Driver

(VMware ESXi 6.x 版 (x=5 または 7)) を適用してください)

2. WBEM プロバイダおよび CLI ツール

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

(「NEC サポートポータル内検索」より、「WBEM プロバイダ」を検索

「【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) 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。

● Product IDについて

Product ID は、スライドタグに記載されています。




● 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、本装置は自動的に設定が変更し、同機能の使用を始めます。
- System ROMのバージョンが v2.10以降、各チャネルあたりのRANK数の合計が 2 以上になるようにメモリを搭載しなくても、フォールトトレラントメモリ機能(ADDDC)は利用できます。

● iLOのセキュリティ機能の注意事項

iLO5 ファームウェア 1.40 以上をご使用の場合、[Information] - [Security Dashboard] 及び iLO Web インターフェイス画面の右上部に  リスクが常に表示されます。

RBSU の設定や iLO の設定の内容次第で、iLO セキュリティの状態がリスク状態(赤色)で表示されますので、お客様のセキュ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、iLO5 ユーザーズガイドを参照してください。

但し、『Require Host Authentication』設定については、「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」に注意事項がありますので、ご確認ください。

iLO5 ファームウェアのバージョンによって該当する条件が異なります。

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

● 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。

例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インターフェイス: [情報] - [概要] 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。

<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、ユーザーズガイド 3章の「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 WebインターフェースのUUIDの不正值表示について**

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 iLO5 ファームウェア 1.40 が適用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の時刻についての注意事項**

iLO5 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、iLO5 ユーザーズガイドを参照してください。

● **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インターフェースから [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) iLO ファームウェアバージョン : 1.40 以上を適用した環境の場合が対象となります。
[セキュリティ]-[アクセス設定]-[iLO]にある[ホスト認証が必要]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。

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、及びイベントログ採取機能

● iLO 1.43以上へのアップデート後の注意事項

iLO5 ファームウェア 1.43 以上をご使用の場合、[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 ページ内のメニュー間移動が出来なくなります。その場合、ブラウザーのリロードボタンをクリックするか、もしくは一旦 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なおしてください。

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

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"/>

英語語表示の場合

● 内蔵DVD-ROM (N8151-137/138) 表示について

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 つ表示されます。

どちらのドライブを選択した場合でも同じ内蔵 DVD 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 Server 環境での Agentless Management Service (AMS) の注意事項

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

◆ 本事象は Agentless Management Service (AMS) 1.43.0.0 で修正されています。

AMS は Starter Pack に含まれています。Starter Pack Version S8.10-006.03 以降を適用してください。すでに AMS 1.40.0.0 がインストールされている環境で Starter Pack Version S8.10-006.03 を使用する場合は、個別に AMS をアップデートする必要があります。Starter Pack が掲載されている Web 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" フォルダをエクスプローラで開きます。

3. "storelib.dll" のファイル名を "storelib.dll.bak" に変更します。

4. 以下のコマンドをコマンドプロンプトで実行して AMS を開始します。

```
>net start ams
```

(※1) AMS 停止時に以下のメッセージが表示されることがありますが問題ありません。

Agentless Management Service サービスを停止中です..

システム エラーが発生しました。

システム エラー 1067 が発生しました。

プロセスを途中で強制終了しました。

Agentless Management Service サービスは正常に停止されました。

(※2) AMS 起動時に以下のメッセージが表示されることがありますが問題ありません。

要求したサービスは既に開始されています。

◆ Agentless Management Service (AMS) のバージョンの確認方法には以下の 2 つの方法があります。

・ 対象装置の OS 上で確認する方法

(1) Windows PowerShell を起動して以下のコマンドを実行します。

```
> Get-WmiObject Win32_Product | Select-Object Name, Version | Select-String "Agentless Management Service"
```

(2) コマンド実行結果からバージョンを確認します。

・ iLO Web インターフェースを利用して、リモートから確認する方法

(1) リモート環境において、Web ブラウザーから iLO Web インターフェー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。

● VMware ESXi環境でのAgentless Management Service (AMS) の注意事項

VMware ESXi 6.5, または VMware ESXi 6.7 の環境に Agentless Management Service (AMS) version 11.4.0 がインストールされている場合、VMware Update Manager による VMware システムの更新が、/tmp ディレクトリへスレーシングするための空きがないことを示すエラーで失敗することがあります。/tmp ディレクトリの使用可能なディスク容量に依存する他のアプリケーションでも同様に失敗することがあります。VMware ESXi ホストの/tmp ディレクトリにある“ams-bbUsg.txt”ファイルのサイズが時間の経過とともに増加するためです。空き容量を確保するために“ams-bbUsg.txt”ファイルを定期的に削除してください。

※ファイルを削除した場合は再度ファイルが作成されます。また、VMware ESXi ホストを再起動した場合も当該ファイルは削除されますが、再起動後に再度作成されます。

/tmp ディレクトリの容量が 256MB である場合、2 か月程度で上限に達することがあります。1 か月に一度を目安に削除してください。

※ご使用の環境の/tmp ディレクトリの容量に比例してファイル削除の実施頻度を変更していただけます。

例) /tmp ディレクトリの容量が 512MB である場合、4 か月程度で上限に達することがありますので、3 か月に一度を目安に削除します。

本事象は Agentless Management Service (AMS) 11.4.5 で修正されています。VMware のバージョンによって AMS のダウンロードサイトが異なりますので下記のサイトをご確認いただき、AMS のアップデートを行ってください。

■ ご使用の OS が ESXi 6.0 の場合

<https://www.support.nec.co.jp/View.aspx?NoClear=on&id=9010108698>

■ ご使用の OS が ESXi 6.5 の場合

<https://www.support.nec.co.jp/View.aspx?NoClear=on&id=9010108699>

■ ご使用の OS が ESXi 6.7 の場合

<https://www.support.nec.co.jp/View.aspx?NoClear=on&id=9010108700>

◆ /tmp ディレクトリの容量は以下のコマンドを実行することで確認することができます。“tmp”の行を確認してください。

```
# vdf -h
:
Randisk          Size      Used Available Use% Mounted on
root             32M        2M      29M    7%  —
etc              28M      172K      27M    0%  —
opt              32M      564K      31M    1%  —
var              48M      448K      47M    0%  —
tmp             256M      276K     255M    0%  —
:
```

◆ Agentless Management Service (AMS) のバージョンの確認方法には以下の 2 つの方法があります。

・対象装置の OS 上で確認する方法

(1) コンソール端末から以下のコマンドを実行します。

```
# esxcli software vib get -n amsd | grep Version
```

(2) コマンド実行結果から「600. xx. x. x-…」、「650. xx. x. x-…」などの xx. x. x の箇所を確認します。

・iLO Web インターフェースを利用して、リモートから確認する方法

(1) リモート環境において、Web ブラウザーから iLO Web インターフェー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「amsd」のバージョンを確認します。

※「600. xx. x. x-…」、「650. xx. x. x-…」など、xx. x. x の箇所を確認します。

● 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 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
バージョン 1.40 以上	バージョン 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
	バージョン 6.41 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 (Windows 版) のアップデート方法

- (1) 以下より最新版の ESMPRO/ServerManager をダウンロードします。
<https://www.support.nec.co.jp/View.aspx?id=9010103524>
- (2) 「ESMPRO/ServerManager Ver.6 インストレーションガイド (Windows 編)」の「2 章 インストール」を参照して ESMPRO/ServerManager をアップデートします。

◆iLO 管理機能向けの受信情報設定ファイル に関する発生現象

※エクスプレス通報サービス (MG) をご利用されている方が対象です。

iLO ファームウェア	iLO 管理機能向けの 受信情報設定 ファイル	発生現象
バージョン 1.40 以上	ilo_jp.mtb バージョン 1.1.0 未満	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。
	iml_jp.mtb バージョン 1.3.0 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。	

◆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」は以下の URL 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 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。

● 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方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、月毎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。

● ドキュメントの型番読み替えについて

末尾が HnY (n は数字) で終わる型番の装置に添付されているドキュメント (ユーザーズガイド、メンテナンスガイド) では、記載されている型番に Hn を付加して読み替えて下さい。

例 : N8100-2773Y → N8100-2773H1Y

● Express5800/R120h-1M、Express5800/R120h-2M ユーザーズガイドについて

ユーザーズガイドに誤記がありましたので、以下に訂正いたします。

	誤	正
サポートOS	VMware ESXi™ 6.7 Update1 以降	VMware ESXi™ 6.7 Update2 以降
搭載CPU	Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)	Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)

■ ファームウェア更新に伴う変更点

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) Advanced Performance Tuning Options メニュー

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

追加のオプションの追加について、次の表を参照してください。

項目	パラメーター	説明
IODC Configuration	[Auto] Enable for Remote InvItOM Hybrid Push InvItOM AllocFlow InvItOM Hybrid AllocFlow Enable for Remote InvItOM and Remote WViLF	IODC(IO Direct Cache)の有効/無効:リモートInvItOM (IIO) および/または WViLF (cores)のために、代わりにメモリ検索のスヌープを生成します。

[]: 出荷時の設定

(2) Advanced PCIe Configuration メニュー

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

追加のメニューについて、次の表を参照してください。

項目	パラメーター	説明
PCIe MCTP Options	-	-

(a) PCIe MCTP Options メニュー

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

追加のオプションについて、次の表を参照してください。

項目	パラメーター	説明
PCIe Slot XX MCTP Broadcast Support	[Enabled] Disabled	指定されたスロットのPCIe管理コンポーネント転送プロトコル (MCTP) を制御します。このオプションは、PCIeエンドポイントに対するMCTPサポートを無効にするために使用します。このオプションはシステムの全機能に対して有効に設定することを推奨します。 XX: 1/2/3... (CPU数やライザーカード種類に応じて表示が変わります。)

[]: 出荷時の設定

■ 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

2019年 12月 6版

Precautions for Using Express5800/R120h-1M (2nd-Gen), R120h-2M (2nd-Gen)

Thank you for purchasing our product.

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.

■ Precautions

● 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.

< <http://www.nec.com/express> >

- Related Links : Download
- Documents & 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).

<<http://www.58support.nec.co.jp/global/download/>>

Windows OS :

- ESMPRO

Linux OS :

- Documents & Software
- Rack : (Select your server model)

● About Starter pack

Please see the following web site to check the latest Starter Pack.

<<https://www.nec.com/en/global/prod/express/>>

- Related Links : Download
- Documents & Software
- (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

< <http://www.nec.com/express> >

- Related Links : Download
- Documents & Software
- Rack or Tower: (Select your server model)

2. WBEM Provider and CLI tool

< <http://www.nec.com/express> >

- Related Links : Download
- Utility

● About Product ID

Product ID is listed in the slide tag.



● 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.

● Caution about iLO security function

In case that iLO5 firmware 1.40 or latest is used,  is always displayed in [Information] - [Security Dashboard] and in iLO Web interface screen.

Depending on the setting of RBSU or iLO, the status of security may be displayed in red showing security is at Risk. Please set security settings appropriately in order to follow customer's security policy.

For the recommended settings, please review the iLO5 User's Guide.

For the settings of "Require Host Authentication", please refer to the other descriptions of **Caution for the case where Admin Password is set from System Utilities(*1), or the case where the setting "Require Host Authentication" is enabled from iLO Web interface(*2).**

The matching condition is different by iLO5 Firmware version.

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

● 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 iLO time function

This caution is for iLO firmware version lower than 1.47.

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 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 iLO 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 iLO firmware version 1.40 and higher.

Set "Require Host Authentication" Enabled in "Security > Access setting > iLO"

When the setting described above is executed, the following symptoms are expected

- Many messages "Remote Insight/ Integrated Lights-Out Unauthorized Login Attempts" are displayed in alert viewer.
- Error occurs, when Starter Pack(Standard Program package) is applied.

The following services and functions are not supported

- Report services for hardware faults in Express Report Service
- Report services in RAID Report Service
- Server diagnosis function in Server Diagnostic Karte
- Function to display Device information and configuration collected by iLO
- Function to collect event logs collected by iLO

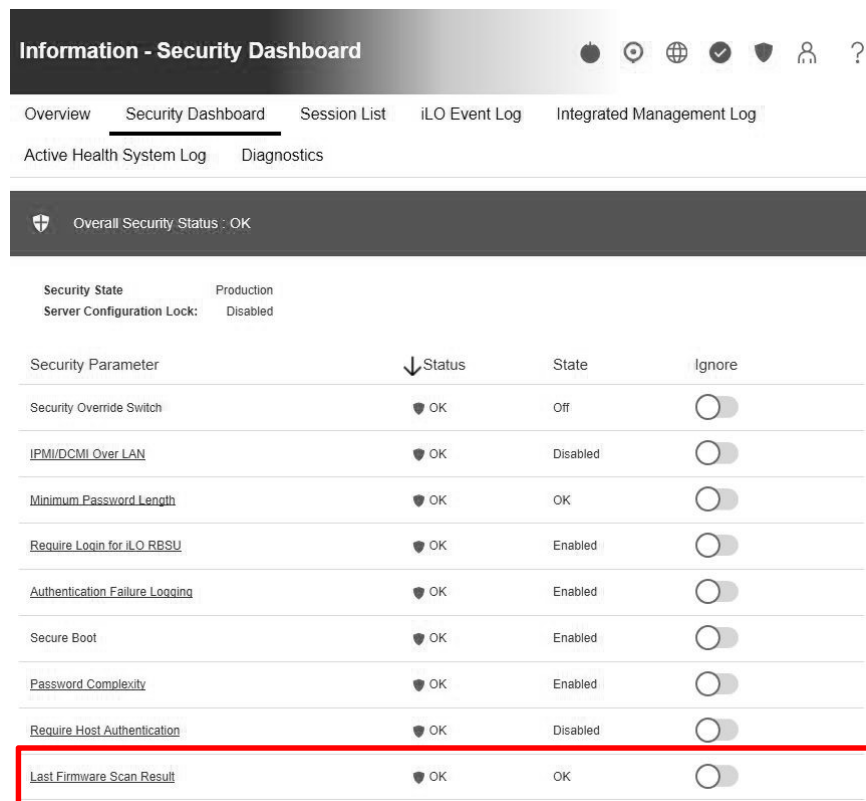
• Caution for iLO firmware 1.43 or later

If you update to iLO5 firmware 1.43 or later, "Last Firmware Scan Result" is displayed in "Information > Security Dashboard". Do not click this Hyper link.

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.



• 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 I/F.

(1) Login to iLO Web I/F 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".

● **Notice of Agentless Management Service(AMS) on the server running VMware ESXi**

On any of the servers running VMware ESXi 6.5 or VMware ESXi 6.7 with Agentless Management Service (AMS) version 11.4.0, updating a VMware system via VMware Update Manager may fail with an error indicating there is no room on /tmp to stage updates. Other applications that depend on available disk space in /tmp will also fail. This happens because the size of the "ams-bbUsg.txt" file in the /tmp directory of the VMware ESXi host is increasing as the time goes. As a workaround, periodically manually delete the "ams-bbUsg.txt" file in the /tmp directory of the VMware host to free up space.

※ When the "ams-bbUsg.txt" is deleted, it will be created again automatically. And when the VMware host is rebooted, the file will be deleted and then created automatically after the reboot.

If the /tmp directory size is 256MB, the available space may be full about 2 months. So delete the file for about once in a month.

※ The frequency of deleting the file can be adjusted depending on the size of /tmp directory.

Ex.) If the /tmp directory size is 512MB, it may be full about 4 months, so delete the file for about once in 3 months.

This symptom will not occur in the release of Agentless Management Service 11.4.5.

◆ The size of the /tmp directory can be checked using the following command. (see the "tmp" row)

```
# vdf -h
:
Randisk          Size      Used Available Use% Mounted on
root             32M        2M      29M    7%  —
etc              28M      172K      27M    0%  —
opt              32M      564K      31M    1%  —
var              48M      448K      47M    0%  —
tmp             256M      276K      255M    0%  —
:
```

◆ You can check the AMS version by using two ways below.

- The way to confirm on the VMware ESXi host OS of the target system.

(1) Run the following command on ESXi shell.

esxcli software vib get -n amsd | grep Version

(2) Check the version from the command result.

- Using iLO Web I/F:

(1) Login to iLO Web I/F with web browser on the remote system.

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

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

* Check the location of "xx.x.x" such as "600.xx.x.x-...", "650.xx.x.x-...".

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

When 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」

● Notice of NEC ESMPRO Manager (Windows) and Express Report Service (MG) (Windows)

Even in the case of adding this product into NEC ESMPRO Manager (Windows) and Express Report Service (MG) (Windows) which have already been managing same model product as this product, updating of NEC ESMPRO Manager (Windows) and iLO Receiving Information (ilo_en.mtb, iml_en.mtb) may be required because this product which is newly shipped from a factory may have newer version of iLO firmware. Referring to information below, update the software if it is required.

Regarding the steps of confirmation version of iLO firmware, NEC ESMPRO Manager (Windows), and iLO receiving information, please refer to the end of this chapter.

◆Restrictions without updating the NEC ESMPRO Manager

iLO firmware version	NEC ESMPRO Manager (Windows) Version	Restrictions
1.40 or higher	Lower than 6.25	<ul style="list-style-type: none"> Constitution Tab - Server Status screen "SNMP Alert setting" will show error message "Failed to get SNMP Alert setting". Remote Control Tab - iLO Information - Show IML or Save IML NEC ESMPRO Manager will fail to get IML information and Show IML or Save IML feature will not work. AlertViewer New Alerts of hardware failure added with firmware update will be displayed as "Unknown" alert on AlertViewer.
	Lower than 6.41	<ul style="list-style-type: none"> 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.

◆Update steps of NEC ESMPRO Manager (Windows)

(1) Download latest version of NEC ESMPRO Manager from the following website.

<http://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]".

◆Restriction without updating the iLO Receiving Information

iLO firmware version	iLO Receiving Information Version	Restriction
1.40 or higher	ilo_en.mtb Lower than 1.1.0	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 1.3.0	
	* There are 2 kinds of iLO Receiving Information.	

◆Update steps of iLO Receiving Information

- (1) Download latest version of iLO Receiving Information(ilo_en.mtb, iml_en.mtb) from the following website.

<http://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 Receiving Information downloaded in step (1) to Express Report Service (MG)

* Download "Express Report Service (MG) Installation Guide (Windows)" from the following website.

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

- ESMPRO tab
- Express Report Service (MG) (Windows)

◆The steps of confirmation for iLO FW version

- Server Health Summary
Push the UID button on the server and check the version of the iLO firmware on the screen.
(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 confirmation version for NEC ESMPRO Manager

- (1) Log in NEC ESMPRO Manager.
- (2) Click the "About NEC ESMPRO Manager" link at the top right of the screen.
- (3) Confirm "Setup Value" field on the screen.

◆The steps of confirmation 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)".

● About EXPRESSBUILDER Help

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

● Errata Information for Express5800/R120h-1M, Express5800/R120h-2M User's Guide

The following table covers correction for User's Guide.

Please read the following information and use it as reference.

	Error	Correct
OS supported	VMware ESXi™ 6.7 Update1 or later	VMware ESXi™ 6.7 Update2 or later
On-board CPU	Xeon Gold 6234 Processor (3.40 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)	Xeon Gold 6234 Processor (3.30 GHz, 8C/16T, TDP 130W, DDR4 2933 1TB)

● The additional options by firmware update

Some options are added or changed by firmware update of this product.

The additional options are listed below.

(1) Advanced Performance Tuning Options Menu

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

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

Option	Parameter	Description
IODC Configuration	[Auto] Enable for Remote Invltom Hybrid Push Invltom AllocFlow Invltom Hybrid AllocFlow Enable for Remote Invltom and Remote Wvlf	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote Invltom (IIO) and/or Wvlf (cores)

[]: Default setting

(2) Advanced PCIe Configuration Menu

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

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

Option	Parameter	Description
PCIe MCTP Options	-	-

ii. PCIe MCTP Options

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

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

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

[]: Default setting

■ 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



* CBZ-031404-001-04 *

Dec 2019 6th Edition