

NX7700x/A5010E-2 v2

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。

ご購入頂いた型番で、製品マニュアルをご検索ください。

<https://jpn.nec.com/nx7700x/>

また、ESMPRO/ServerManager、ESMPRO/ServerAgentService、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?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。

● 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://jpn.nec.com/nx7700x/>

([技術サポート情報・ダウンロード] – [ドライバー、ユーティリティ関連の物件] のページの
ユーティリティの項を参照)

2. WBEM プロバイダおよび CLI ツール

<https://jpn.nec.com/nx7700x/>

([技術サポート情報・ダウンロード] – [ドライバー、ユーティリティ関連の物件] のページの
ユーティリティの項を参照)

3. VMware ESXi デバイスドライバ

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

(「エンタープライズサーバ(NX7700x シリーズ)」から対象 OS の「デバイスドライバー一覧」を選択)

● 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。

● Product IDについて

Product ID は、スライドタグに記載されています。



● iLOのセキュリティ機能の注意事項

- [Information] - [Security Dashboard]及びiLO Webインターフェース画面の右上部に  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、「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」に注意事項がありますので、ご確認ください。

● システムユーティリティより、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

「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。

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”的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の再起動を行う場合の注意事項

サーバ起動から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：[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、次項の「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 1.43での注意事項

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

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

英語表示の場合

● iLOの時刻についての注意事項

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。

● 内蔵DVD-ROM(NE3351-137)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 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」

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

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ディレクトリへステージ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ヶ月程度で上限に達することがあります。1ヶ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ヶ月程度で上限に達することがありますので、3ヶ月に一度を目安に削除します。

本事象はAgentless Management Serviceの今後のリリースで改善される予定です。

◆/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”的行を確認してください。

```
# vdf -h
:
  Ramdisk          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 フームウェア	ESMPRO/ServerManager (Windows 版)	発生現象
Version 1.43 以上	Version 6.25 未満	<ul style="list-style-type: none"> 構成タブ - サーバ状態 “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 フームウェア	iLO 管理機能向け受信情報設定ファイル	発生現象
バージョン 1.43 以上	iLo_jp.mtb バージョン 1.1.0 未満 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。	フ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) 以下より最新版の受信情報設定ファイル(iLo_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 は MGMTB.zip に含まれています。

- (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

サーバ本体の UID ボタンを押下して、サーバ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。

NEC



CBZ-035220-001-007

2019年 9月