

iStorage M シリーズ  
NAS オプション ソフトウェア(Virtual File Platform)  
Ver.3.4.2 (FOS6.4.3-08)  
リリースノート

2020 年 7 月  
日本電気株式会社

日頃より弊社製品をご愛顧いただきありがとうございます。iStorage M シリーズ NAS オプション ソフトウェアでご提供する機能の強化ならびに変更いたしました点につきましてご説明させていただきます。

1.	本資料の範囲.....	3
1.1.	リリース SW バージョン .....	3
1.2.	対象製品名 .....	3
1.2.1.	組み込みソフトウェア(FOS)対象製品 .....	3
1.2.2.	オプションソフトウェア製品 .....	3
1.2.3.	管理ソフトウェア製品 .....	3
1.3.	更新インストール対象バージョン .....	3
2.	提供する更新物件とその適用方法.....	5
2.1.	ファイル名とサイズ .....	5
2.2.	File Services Manager がインストールされたマシンに必要な空き容量.....	5
2.3.	適用時間 .....	5
2.4.	更新インストール手順 .....	5
3.	提供物件の追加機能ならびに変更内容 .....	6
3.1.	追加機能内容 .....	6
3.2.	変更内容 .....	6
4.	提供物件の修正内容.....	7
4.1.	標準機能 .....	7
4.1.1.	CIFS.....	7
4.1.2.	その他 .....	7
4.2.	File Services Manager .....	8
4.3.	オプションソフトウェア .....	8
4.3.1.	File Remote Replicator.....	8
4.3.2.	File System Importer .....	8
4.3.3.	File Retention Utility .....	8
5.	注意事項.....	9

6.	制限事項.....	11
7.	マニュアル .....	13
8.	お問い合わせ先.....	13
9.	商標類 .....	13

## 1. 本資料の範囲

本資料は、iStorage M シリーズの NAS オプション部で動作する組み込みソフトウェア (FOS)、オプションソフトウェア、および NAS オプション部を管理するための外部サーバで動作するソフトウェア (File Services Manager、以下 FSM) について説明しております。

### 1.1. リリース SW バージョン

- Ver.3.4.2(FOS6.4.3-08)

### 1.2. 対象製品名

#### 1.2.1. 組み込みソフトウェア(FOS)対象製品

- NAS オプション Nh4b/8b
- NAS オプション Nh4c/8c
- M110 NAS セット ※Nh4b のみ

#### 1.2.2. オプションソフトウェア製品

- File Remote Replicator (FRR)
- File Retention Utility (FRU)
- File System Importer (FSI)

#### 1.2.3. 管理ソフトウェア製品

- File Services Manager

### 1.3. 更新インストール対象バージョン

本ソフトウェアは、下記のバージョンから更新インストールすることができます。

- Ver.2.2.0(FOS5.7.1-00)
- Ver.3.0.0(FOS6.0.2-02)
- Ver.3.1.0(FOS6.1.1-02)
- Ver.3.2.0(FOS6.2.0-04)
- Ver.3.3.0(FOS6.3.1-00)
- Ver.3.4.0(FOS6.4.3-00)
- Ver.3.4.1(FOS6.4.3-05)

なお、それぞれのバージョンの機能追加・変更・修正内容については、各バージョンのリリースノートをご確認ください。

ご利用の OS バージョンは、下記のとおりコマンドまたは File Services Manager を用いてご確認いただけます。

## ■コマンドにて OS バージョンを確認する場合

1. ノードまたは Virtual Server SSH 用アカウントとして **nasroot** を使用し、ログインしてください。あるいはリモートホストから、アカウント **nasroot** を使用し、下記のコマンドを実行してください。
2. コマンド **versionlist** を実行しバージョンを表示してください。

表示例:

```
nasroot@node0:~$ sudo versionlist
```

Products Version:

Hitachi Virtual File Platform : 5.7.1-00

※上記の場合、node0 の FOS バージョンは 5.7.1-00 であることを示しています。

SSH 用アカウント **nasroot** の使用についての詳細は、マニュアル「コマンドリファレンス」(IF311)の「1.4 コマンドの実行方法」を参照ください。コマンドを実行する場合は、ノードの固有 IP アドレスを指定してください。

## ■File Services Manager にてバージョンを確認する場合

1. File Services Manager を Open してください。

例:

<http://localhost:23015/FileServicesManager/Title.jsp>

※上記 URL を開きます。ここでは、“localhost”にアプリケーションをインストールしている場合の例です。

2. 左側のエクスプローラ欄から[リソース]—[Processing Node]を開いてください。
3. 右側のファイルサーバ欄内の対象 Processing Node 名のシステムバージョン欄を確認してください。

※上記欄にたとえば 5.7.1-00 と表示されている場合は、FOS バージョンは 5.7.1-00 であることを示しています。

## 2. 提供する更新物件とその適用方法

### 2.1. ファイル名とサイズ

FOS : install\_files\_3.4.2.tar.gz(約 1GB)

FSM : nec\_fsm20200422\_342\_32.iso (約 630MB)

### 2.2. File Services Manager がインストールされたマシンに必要な空き容量

FOS の更新インストールの適用時には、一時的に 2GB 以上の容量が必要となります。

### 2.3. 適用時間

180 分(Virtual Server 未使用時)

本時間はお客様環境によって異なりますので、あくまで目安として提示しております。

適用時間見積もりの詳細についてはマニュアル「ユーザーズガイド」(IF305)の「15.2 ノードのソフトウェアを更新する」をご参照ください。

### 2.4. 更新インストール手順

File Services Manager のアップデートを実施したのち、FOS の更新インストールを実施してください。本ソフトウェアの更新インストール手順・適用状況確認につきましては、下記のマニュアルをご覧ください。

- ・「ユーザーズガイド」(IF305)

- 「15.更新インストールする」

また、本資料の「5.注意事項」も事前にご確認ください。

### 3. 提供物件の追加機能ならびに変更内容

#### 3.1. 追加機能内容

- 1) CIFS サービスを制御するコマンド(**svctl** コマンド)において、相手ノードのリソースグループがフェールオーバーしてきている状態で、自ノードと相手ノードの両リソースグループを再起動するオプション(**--restart-all** オプション)を追加しました。

#### 3.2. 変更内容

特に変更はありません。

## 4. 提供物件の修正内容

以下の内容を修正しました。

### 4.1. 標準機能

#### 4.1.1. CIFS

- 1) 以下の条件がすべて重なった状態でフェールバックした際に、CIFS サービスの構成定義が不正になる場合がありますので、これを修正しました。

- ① CIFS サービスでユーザーマッピングを使用する。
- ② クラスタ内の各ノードで CIFS サービスのユーザーマッピング設定が異なる。
- ③ フェールオーバーしていたリソースグループを元のノードにフェールバックする。

- 2) 以下の条件がすべて重なった状況で、CIFS サービスの停止や再起動を実施した際に、CIFS サービス停止の遅延や CIFS サービスの再起動が失敗することがありましたので、これを修正しました。

- ① システムの負荷が高騰している。
- ② CIFS クライアントから CIFS 共有へアクセスしている。

- 3) 以下の条件がすべて重なった場合に、ドメインコントローラーとの通信量が増加する場合がありますので、これを修正しました。

- ① CIFS ユーザーの認証方式として「Active Directory 認証」を選択している。
- ② ユーザーマッピングを使用している。
- ③ ドメインコントローラーとの LDAP 通信を署名付き (client\_ldap\_sasl\_wrapping = sign) にしている。

#### 4.1.2. その他

- 1) 以下の共通脆弱性識別子(CVE)により報告された脆弱性の影響を受け、sftp クライアントからローカルユーザを使用して接続した際に CPU 負荷が高騰する場合があります問題を修正しました。

CVE-2016-651

- 2) 以下の共通脆弱性識別子(CVE)により報告された脆弱性の影響を受け、ノードの OS 再起動やサービス提供の妨害を受ける可能性がある問題を修正しました。

CVE-2019-11477、CVE-2019-11478、CVE-2019-11479

- 3) 以下に示すメッセージ ID のメッセージに Virtual Server の記載がない不具合を修正しました。

- ・ KAQG52018-W
- ・ KAQG52019-E
- ・ KAQG52053-I

- 4) エンドユーザが利用する GUI に不正にアクセスできる問題がありましたが、これを修正しました。
- 5) ノードと NTP サーバの時刻差が 1000 秒を超過している際に、`ntpq` コマンドでの時刻差情報が正しく表示されない場合がありましたが、これを修正しました。  
また、ノードと NTP サーバで 5 分以上の時刻差が発生しても、通報 (KAQG53017-W) が発生しない場合がありましたが、これを修正しました。
- 6) 以下の条件がすべて重なった場合に、システム設定情報ファイルが定時保存されない問題がありましたが、これを修正しました。
  - ① システム設定情報ファイルの定時保存の保存先に、ファイルシステム上のディレクトリを指定している。
  - ② 指定したファイルシステム上のディレクトリのパスにシェルが解釈する特殊文字(スペースなど)が含まれている。

## 4.2. File Services Manager

特に修正はありません。

## 4.3. オプションソフトウェア

### 4.3.1. File Remote Replicator

特に修正はありません。

### 4.3.2. File System Importer

特に修正はありません。

### 4.3.3. File Retention Utility

特に修正はありません。

## 5. 注意事項

本バージョンを利用する上での注意事項は、以下のとおりです。

- 1) システム全体でファイルシステム(スナップショットを含む)を 6000 個以上作成することはできません。
- 2) CIFS の全通知処理(notify)について、監視範囲の設定機能を無効から有効に変更したとき、複数の CIFS クライアントから接続すると CPU 使用率が高負荷状態になる場合があります。
- 3) 本バージョンの File Services Manager では、V2.2.0 より過去のバージョンの FOS を管理することはできません。
- 4) Windows Server 2008 から SMB2 を使用して CIFS 共有にアクセスする場合、Microsoft 社の Knowledge Base:KB978625 にある対処が必要です。Knowledge Base:KB978625 の内容を確認し、Microsoft 社のサポートに問い合わせてください。対処しないで SMB2 を使用してアクセスした場合、Windows クライアントが STOP エラーになり、画面上にエラーメッセージ「STOP: 0x00000027(parameter1,parameter2, parameter3, parameter4)」または「mrxsmb20.sys - Address parameter1 base at parameter2, Datestamp parameter3」が表示されることがあります。
- 5) 障害等が発生してログファイルへの出力中にノードダウンが発生したとき、出力中のログが文字化けする場合があります。
- 6) FOS では未サポートの監査 ACL を有効として robocopy 等のデータ移行を行うと、実際には監査 ACL は付与されていないため、以前のバージョンでは監査 ACL の設定・参照をするとエラーとなりましたが、本バージョンではエラーとはなりません。
- 7) V3.0.0 から CVE-2008-5161 の脆弱性の改修により低強度の暗号化アルゴリズム (CBC モード・一部の MAC アルゴリズム) のサポートを停止しました。これにより低強度の暗号化アルゴリズムを使用していた ssh クライアントで接続できなくなります。下記の暗号化方式に対応した ssh クライアントをご使用ください。  
暗号アルゴリズム: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128  
MAC アルゴリズム:  
hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com  
なお、CD に同梱した putty にて接続確認を行っております。
- 8) 管理サーバの時刻が大幅に変更されると、File Services Manager にログインできなくなる可能性があります。そのような場合には、File Services Manager をアンインストールした後、再インストールしてください。

- 9) Virtual Server への CPU 割り当てによる性能チューニングの設定を行う場合、設定を行う前に「8. お問い合わせ先」までご連絡ください。運用環境に合わせた設定手順をご案内させていただきます。
- 10) FSM を新規インストールまたはアップデートするとき、OS ドライブ※直下に下記ファイルが作成されているとインストールまたはアップデートに失敗する場合があります。事前に下記ファイルが作成されていないことを確認してください。
- ・ OS ドライブ:¥Program
  - ・ OS ドライブ:¥Program.exe
  - ・ OS ドライブ:¥Program Files (64 ビット版 OS の場合)
  - ・ OS ドライブ:¥Program Files.exe (64 ビット版 OS の場合)
  - ・ OS ドライブ:¥Program Files¥Common
  - ・ OS ドライブ:¥Program Files¥Common.exe
  - ・ OS ドライブ:¥Program Files (x86)¥Common (64 ビット版 OS の場合)
  - ・ OS ドライブ:¥Program Files (x86)¥Common.exe (64 ビット版 OS の場合)
- ※OS ドライブ Windows OS をインストールしたドライブ(通常は C ドライブ)
- 11) FSM を新規インストールまたはアップデートするとき、インストールメディアの内容をコピーして使用する場合は、必ず管理サーバのローカルディスクにコピーしてください。ネットワークドライブ上のデータを使用してインストールすることはできません。
- 12) FSM を新規インストールまたはアップデートするとき、管理サーバのキーストアファイル(jssecacerts)のパスワードが設定されている場合は、[インストールの完了]ダイアログが表示される前にエラーダイアログが表示されます。ダイアログの内容を確認して[OK]をクリックし、インストールが完了した後に、管理サーバに SSL の証明書をインポートしてください。管理サーバに SSL の証明書をインポートする方法については、「システム構成ガイド」(IF302)を参照してください。
- 13) V3.1.0 において、CIFS を使用している場合、セキュリティ強化のために、ドメインコントローラーとの通信の LDAP 署名有無の初期値を「LDAP 署名あり」に変更しました。

本修正により、cifsopstset コマンド client\_ldap\_sasl\_wrapping オプションで LDAP 署名有無を設定していない場合、ドメインコントローラーとの通信で LDAP 署名が付与されます。(セキュリティ強化を優先し、本動作に変更しています)

署名付き LDAP 通信が必要でない場合は、署名付き LDAP 通信の設定を「なし (client\_ldap\_sasl\_wrapping を plain)」としてください。

## 6. 制限事項

本バージョンを利用する上での制限事項は、以下のとおりです。

- 1) CIFS クライアントがアクセスしたファイルパスに特殊文字が含まれる場合、リアルタイムスキャン処理が正常に完了しません。ファイルパスに特殊文字が含まれないように変更してください。
- 2) 以下のいずれかの条件を満たしたとき、**File Services Manager** のインストールに失敗する場合があります。条件に該当しない別領域でインストールしてください。
  - ・ Windows8、Windows Server 2012 でサポートされたシン・プロビジョニングで作成したディスクを使用している。
  - ・ Windows8、および Windows Server 2012 でサポートされた物理・論理セクタサイズが 4096 バイト (4K native) のディスクを使用している。
- 3) SMB3.0 の暗号化を有効にした CIFS 共有では、CIFS サービスおよび CIFS 共有の設定に関わらず、クライアントキャッシュは無効となります。
- 4) 外部サーバに所属するユーザーを FTP ユーザーとして使用したとき、セカンダリグループのアクセス権でデータにアクセスすることはできません。セカンダリグループのアクセス権が有効になるのはローカルユーザだけです。
- 5) 差分格納デバイスの警告閾値に 0 を設定したファイルシステムが存在するとき、バックアップしたシステム設定ファイルを使用してシステム設定情報を回復すると、警告閾値の 0 が引き継がれずに 80 が設定されます。この場合、警告閾値を 0 に変更してください。
- 6) Firefox を使用して FSM からノードの更新インストールを実施するとき、更新インストールの途中で画面が止まる場合があります。画面が止まった場合、[ツリー更新] ボタンで画面情報を更新し、両ノードの[システムバージョン]がインストールしたソフトウェアのバージョンになっていることを確認してください。
- 7) Virtual Server が存在する Processing Node で管理ポートの固有 IP アドレスを変更した後、[ノード編集] ダイアログで管理サーバに Processing Node を再認識させようとするとき KAQM23302-E エラーとなります。一度[ノード削除]で Processing Node を削除して、[Processing Node 追加]で再登録してください。
- 8) FSM を新規インストールするとき、インストール先のパス名が括弧を含むかつ空白文字を含まないと KAQM30012-E エラーが発生してインストールが失敗します。この条件に合致しないフォルダにインストールしてください。
- 9) 管理サーバとノードの HTTPS 通信は TLS1.0 のため、TLS1.0 の設定を無効にしないでください。
- 10) Windows Server 2016 を Active Directory のドメインコントローラーとして利用している環境において MMC 連携機能のセッションの一覧表示/切断を利用する場合、MMC 連携機能を起動するクライアントの hosts ファイルに、FOS に接

続している Windows クライアントのホスト名から IP アドレスへの変換ルールを記述することで利用することができます。

- 11) ディレクトリの属性を表示するコマンド(**dirlist** コマンド)に指定するディレクトリパスの途中にマルチバイト文字のみのディレクトリが存在する場合、コマンドの実行結果がエラー(**KAQM08053-E**)となります。コマンドがエラーとなる場合は、**CIFS** または **NFS** クライアントからディレクトリの属性を確認してください。
- 12) **NFS/CIFS/FTP** アクセス混在環境において、**NFS** または **FTP** クライアントで **UTF-8** 以外の文字コードのファイル名を付与したファイルを作成した場合、当該ファイルを **CIFS** でアクセスすると、アクセスに失敗し **core** ファイルが出力される場合があります。

**NFS/CIFS/FTP** アクセス混在環境では、**NFS** または **FTP** クライアントからは **UTF-8** の文字コードを使用してファイルを作成してください。

- 13) 以下の条件がすべて重なった場合、**NFS** アクセスが不可となる事象が発生します。
  - ① **NFS** サービスに固定のポート番号を割り当てる設定である。
  - ② **NFS** サービスの設定で、**NFSv3** が使用不可の設定である。
  - ③ ノードの再起動、または、リソースグループ、**Virtual Server** の再起動、フェールオーバー、フェールバックを行う。

本事象を回避するため、以下のいずれかの設定変更を実施してください。

- ・ **NFS** サービスのポート番号を動的に割り当てる設定にする。
- ・ **NFS** サービスの設定で、**NFSv3** を使用可能な設定にする。

- 14) 以下の条件がすべて重なった場合、**NFS** で応答遅延が発生していないにもかかわらず、**NFS** サービスの性能統計情報の応答時間に非常に大きな値が記録される場合があります。当該値を無視して統計情報をご参照ください。
  - ① **Virtual Server** を使用している。
  - ② **Virtual Server** に 2 個以上の **CPU** を割り当てている。

- 15) 本装置の LAN ポート(データポート)とネットワークスイッチ間の通信経路が障害となり、不正パケットを受信した場合においても、リンクは **Down** 状態にならず、通報も行いません。

**HW** 障害通報はないが、経路障害が疑われる場合は、下記マニュアルを参照の上、データポートの状態確認、ならびに経路の確認を実施してください。

- ・ 「トラブルシューティングガイド」(IF308)

「4.15 データポートのエラー情報を確認して障害を回復する」

## 7. マニュアル

本ソフトウェアの詳細な使用方法につきましては、下記のマニュアルをご覧ください。  
本ソフトウェアを新規に導入する場合は、最初にマニュアル「ファーストステップガイド」(IF301)を参照ください。最新版のマニュアルは NEC サポートポータルで公開しておりますので、ダウンロードしてご確認ください。

- [Nhxb/Nhxc]NAS オプション取扱説明書(第3版)
- ファーストステップガイド(IF301-3)
- システム構成ガイド(IF302-11)
- セットアップガイド(IF303-1)
- 仮想サーバ環境セットアップガイド(IF304-3)
- ユーザーズガイド(IF305-11)
- ファイルアクセス(CIFS/NFS)ユーザーズガイド(IF306-8)
- ファイルアクセス(Quota)ユーザーズガイド(IF307-1)
- トラブルシューティングガイド(IF308-10)
- トラブルシューティングガイド別紙(IF309-1)
- インストールガイド(IF310-2)
- コマンドリファレンス(IF311-9)
- API リファレンス(IF312-6)
- メッセージリファレンス(IF313-10)
- メッセージリファレンス別紙(IF314-3)
- ESMPRO 通報設定(IF315-4)
- BackupRestore 機能補足資料(NetBackup) (IF316-1)
- システム動作情報のグラフ化手順書(IF317-2)
- 仮想サーバ環境セットアップガイド別紙(IF318-1)

## 8. お問い合わせ先

ご不明な点につきましては、弊社「NEC カスタマーサポートセンターiStorage グループ」までお問い合わせください。

## 9. 商標類

記載の会社名および商品名は、各社の登録商標または商標です。

Copyright (C) NEC Corporation 2013-2020

以上