

FUJITSU Storage ETERNUS BE50

バックアップアプライアンス

アップデートについて

平成 26 年 5 月
富士通株式会社

ETERNUS BE50 にインストールされているソフトウェアのアップデートについてお知らせいたします。

1. 性能が向上する修正プログラムについて

・ETERNUS BE50 にインストールされている Backup Exec 2012 は、LiveUpdate の Web サービスで自動配布される最新の修正プログラムを適用してください。

2013 年 2 月末に Backup Exec 2012 の性能が向上する修正プログラムが、Web サービスで自動配布されています。

以下の性能改善修正プログラム(Hotfix)が、適用済みかをご確認願います。

Symantec Backup Exec (Hotfix 201596)

上記の修正プログラムと合わせて、下記の修正プログラムも適用済みかをご確認願います。

Symantec Backup Exec (Hotfix 180964)

Symantec Backup Exec (Hotfix 189571)

Symantec Backup Exec (Hotfix 194470)

Symantec Backup Exec (Hotfix 199866)

Symantec Backup Exec (Hotfix 200433)

適用済みの修正プログラム(Hotfix)の確認方法

- (1) Backup Exec 管理コンソール画面左上の[Backup Exec]ボタンをクリックします。
- (2) 表示されたメニューから[インストールとライセンス]を選択し、[インストール済みの更新]をクリックします。
- (3) 「インストール済みの更新」画面で適用されている Service Pack と Hotfix を確認します。

なお、上記修正プログラムは Backup Exec 2012 の最新の Service Pack (以下 SP)に含まれるため、Backup Exec 2012 の最新の SP を適用した場合、これらの修正プログラムを適用する必要はありません。

最新の SP は以下のサイトにて入手可能です。

「FUJITSU Storage ETERNUS BE50 バックアップアプライアンス」>「ダウンロード」

<http://storage-system.fujitsu.com/jp/products/dedupe/be/tool/>

また、SP 適用については、留意事項がありますので、以下のドキュメントをご確認願います。

「FUJITSU Storage ETERNUS BE50 バックアップアプライアンス」>「製品のご使用にあたって」

<http://storage-system.fujitsu.com/jp/notice/be/>

「ETERNUS BE50 バックアップアプライアンス 注意事項」

2. Java Runtime Environment (JRE) のバージョンについて

- ・ETERNUS BE50 には JRE 6 がインストールされています。Java SE 6 の公式アップデートが終了となったため Java Update を使用して Java SE 7 へのアップデートを実施願います。
- ・Java 7 Update 10 (7u10)以降のバージョンには、使用している Java のバージョンが最新ではないか、または既知のセキュリティ脆弱性がある場合に、「Java Update が必要」というメッセージ(「Java のバージョンが最新ではありません。」または「お使いの Java バージョンは安全ではありません。」)といったメッセージが表示されます。
インターネットに接続された環境でお使いの場合は「更新(推奨)」を選択してアップデートを実施してください。インターネットに接続されていない環境でお使いの場合は、「後で」を選択してください。
- ・Java 7 U25(7u25)以降のバージョンをお使いの場合、Java Applet(ServerView RAID Manager)の画面が正しく表示されないことがあります。以下の対処を行うことで Java Applet を実行することができます。

インターネットに接続された環境でお使いの場合:

以下のいずれかの対処を行ってください。

対処 1)

最新の Java 7 にアップデートしてください。

対処 2)

1. Windows のコントロール・パネルを開きます。

表示されたアイコンの中から Java をダブルクリックします。

2. セキュリティタブのセキュリティ・レベルを「中」にし、「適用」をクリックします。

インターネットに接続されていない環境でお使いの場合:

1. Windows のコントロール・パネルを開きます。

表示されたアイコンの中から Java をダブルクリックします。

2. 詳細タブの”証明書失効チェックを実行”で「チェックしない(非推奨)」を選択し、「OK」をクリックします。

2.1 Java 7 Update 51の適用について

オラクル・コーポレーション社が米国時間の 2014 年 1 月 14 日より提供された Java 7 Update 51 により、Java Applet および Java Web Start の Java プログラムが正常に動作しなくなる事象が生じる場合があります。

つきましては、ETERNUS BE50 の Java プログラムを実行するウェブブラウザ環境に対し、後述する回避策を実施いただけますようお願いいたします。

・概要

オラクル・コーポレーション社の公開情報によると、Java 7 Update 51 より、セキュリティ要件が変更され、"公的機関の署名付 JAR" 及び "Permissions"アトリビュートが、Java Applet および Java Web Start の Java プログラムの必須要件に変更されます。

その結果、当該要件を満たしていない Java プログラムは、ウェブブラウザ上で実行できなくなります。

詳細は、オラクル・コーポレーション社の公開情報を参照ください。

- [「Java Platform Group Product Management」ブログ\(英文\)](https://blogs.oracle.com/java-platform-group/entry/new_security_requirements_for_rias)
https://blogs.oracle.com/java-platform-group/entry/new_security_requirements_for_rias
- [ブラウザの Java コンテンツ - セキュリティの変更\(和文\)](http://www.java.com/ja/download/faq/signed_code.xml)
http://www.java.com/ja/download/faq/signed_code.xml

・影響を受ける可能性のある ETERNUS BE50 対象プログラム

ウェブブラウザ上で動作する Java Applet および Java Web Start の Java プログラムについて、プログラムが起動できない等の不具合が発生する可能性があります。

- [ServerView RAID Manager v5.6.4](#)

・お願いとお知らせ

Java 7 Update 51 により影響を受ける可能性のある Java プログラムを実行するウェブブラウザ環境 (ETERNUS BE50 本体やクライアント PC) への当版数の適用を実施する際は、ETERNUS BE50 にインストールされている ServerView RAID Manager を Java 7 Update51 対応版 (ServerView RAID Manager v5.8.5) にあらかじめアップデートいただくか、下記の回避策を実施いただきますようお願いいたします。Java 7 Update51 対応版 (ServerView RAID Manager V5.8.5) は、以下の URL の掲載内容に従って入手してください。

「FUJITSU Storage ETERNUS BE50」>「ダウンロード」

<http://storage-system.fujitsu.com/jp/products/dedupe/be/tool/>

プログラム「ServerView RAID Manager」

<回避策>

Java 7 Update 51 以降にて実装された、「例外サイト・リスト」に、ServerView RAID Manager の URL を指定してください。「例外サイト・リスト」は、Java コントロール・パネルの「セキュリティ」タブ から設定することができます。

- ServerView RAID Manager の URL : <https://<ホスト名、もしくは IP アドレス>:3173/>

詳細は、オラクル・コーポレーション社の公開情報を参照ください。

- 「[どうすれば例外サイト・リストを構成できますか。](https://www.java.com/ja/download/faq/exception_sitelist.xml)」(和文)
https://www.java.com/ja/download/faq/exception_sitelist.xml
- 「[Java Platform Group Product Management](https://blogs.oracle.com/java-platform-group/entry/upcoming_exception_site_list_in)」ブログ(英文)
https://blogs.oracle.com/java-platform-group/entry/upcoming_exception_site_list_in

3. ServerViewのアップデートについて

- ・ETERNUS BE50 のダウンロードから下記 URL の掲載内容に従って ServerView RAID Manager V5.8.5、ServerView エージェント V6.30.08 へアップデートをお願いします。

アップデートすることで JRE 7 の対応(「[2. Java Runtime Environment \(JRE\) のバージョンについて](#)」をご参照願います。)および、OpenSSL の脆弱性の対策(「[3.1 OpenSSL 'Heartbleed' 脆弱性問題の影響について](#)」をご参照願います。)になります。

「FUJITSU Storage ETERNUS BE50 バックアップアプライアンス」>「ダウンロード」

<http://storage-system.fujitsu.com/jp/products/dedupe/be/tool/>

ServerView をアップデートする際には、留意事項がありますので、以下のドキュメントをご確認願います。

「FUJITSU Storage ETERNUS BE50 バックアップアプライアンス」>「製品のご使用にあたって」

<http://storage-system.fujitsu.com/jp/notice/be/>

「ETERNUS BE50 ServerView アップデートにおける留意事項」

3.1 OpenSSL 'Heartbleed' 脆弱性問題の影響について

OpenSSL Project が提供する OpenSSL にリモートからメモリ情報を参照可能な脆弱性 (CVE-2014-0160) の存在が報告されております。

本脆弱性による ETERNUS BE50 への影響について、お知らせいたします。

1. 概要

OpenSSL の脆弱性に関する注意喚起が、JPCERT より公開されております。

<https://www.jpCERT.or.jp/at/2014/at140013.html>

OpenSSL Project が提供する OpenSSL の heartbeat 拡張には情報漏えいの脆弱性があります。結果として、悪意を持った第三者が、細工したパケットを送付することでシステムのメモリ内の情報を閲覧し、秘密鍵などの重要な情報を取得する可能性があります。

以下の版数の OpenSSL が、本脆弱性の影響を受けます。

- OpenSSL 1.0.1 から 1.0.1f
- OpenSSL 1.0.2-beta から 1.0.2-beta1

2. 影響を受ける可能性のある ETERNUS BE50 対象プログラム

ServerView RAID Manager V5.5.2 および V5.6.4

3. お願いとお知らせ

本脆弱性による影響を受けないように修正された対策版 (ServerView RAID Manager V5.8.5) を以下の URL の掲載内容に従って入手し、アップデートの実施をお願いします。

「FUJITSU Storage ETERNUS BE50」>「ダウンロード」

<http://storage-system.fujitsu.com/jp/products/dedupe/be/tool/>

プログラム「ServerView RAID Manager」

対策版にアップデートされるまでの間は、回避策を実施していただけますようお願いいたします。

<回避策>

影響を受けるバージョンの ServerView RAID Manager に対する外部接続からの攻撃に対しては、ネットワークポート 3173 番をブロックすることで受けつけなくなります。

この場合、BE50 本体のブラウザからのみ ServerView RAID Manager を利用することが出来ます。

また、以下を行うことでも外部から ServerView RAID Manager へのアクセスが出来なくなるため、外部接続からの脆弱性を突いた攻撃を受けつけなくなります。

1) amDPatch.ini ファイルを編集します。

ファイルの配置場所

C:\Program Files(x86)\Fujitsu\ServerView Suite\RAID Manager\bin\amDPatch.ini

2) ファイル中の " LocalConnections =" を "1" に編集します (デフォルト:0)

LocalConnections = 1 ; From which servers are connections allowed to our port

3) ServerView RAID Manager サービスを再起動します。

「スタートメニュー」の「管理ツール」から「サービス」を起動してください。

表示されたサービスの一覧から、「ServerView RAID Manager」サービスを 選択し、「サービスの再起動」を実施してください。

- 4) ServerView RAID Manager にアクセスする場合は、ETERNUS BE50 のスタートメニューから ServerView RAID Manager を起動せずに、ETERNUS BE50 自身のブラウザから <https://127.0.0.1:3173/> または <https://localhost:3173/> に接続します。

上記回避策を実施後、OpenSSL 脆弱性の対策版にアップデートインストールを行った場合、外部（ローカルホスト以外）からの ServerView RAID Manager へのアクセス不可の設定は引き継がれます。外部からのアクセスを許可する場合は、アップデートインストール後に以下の手順を実施願います。

- 1) amDPatch.ini ファイルを編集します。

ファイルの配置場所

C:¥Program Files¥Fujitsu¥ServerView Suite¥RAID Manager¥bin¥amDPatch.ini

- 2) ファイル中の " LocalConnections ="を"0"に編集します(修正前:1)

LocalConnections = 0 ; From which servers are connections allowed to our port

- 3) ServerView RAID Manager サービスを再起動します。

「スタートメニュー」の「管理ツール」から「サービス」を起動してください。

表示されたサービスの一覧から、「ServerView RAID Manager」サービスを 選択し、「サービスの再起動」を実施してください。