

Enterprise Linux with Dependable Support 「SJISサポート」オプション

Enterprise Linux with Dependable Supportのオプション製品として、「SJISサポート」を提供。UNIXからのマイグレーションやメインフレームとのデータ連携を力強くサポートします。

通常、Red Hat Enterprise Linux でサポートされる文字コードは、「UTF-8」のみ*です。「SJIS」を使用していたシステムからのマイグレーションなどでは、お客様のアプリケーション修正が必要となり、SIコスト増大の原因となることがあります。

NECでは、「SJISサポート」をオプション製品として提供し、お客様のSIコスト削減を強力に支援します。
(日本語文字コードとして「SJIS(Shift-JIS, Shift-JISX0213-200, Windows-31J準拠)」のサポートを提供します。)

*RHEL4以降、標準でサポートされる文字コードは「UTF8」のみです。

●Red Hat社の提供ポリシーに基づき、下記のRPMパッケージで、SJISを扱うことに起因する問題が発生した場合、修正アップデートモジュールが提供されます。

bash	coreutils	cpp	diffutils	dos2unix	ed	findutils	fontconfig
gawk	gcc	gcc-c++	gcc4	gcc4-c++	gdb	gettext	glib2
glibc	glibc-common	glibc-devel	grep	gtk2	less	libstdc++	libtermcap
m4	ncurses	pdksh	sed	tclsh	unix2dos	util-linux	vim-common
vim-enhanced	vim-minimal	xorg-X11-libs					

*上記の対象パッケージとPPサポートサービス(レスポンスサービス)におけるサポート対象は、異なる場合があります。

価格

下記表に掲載した製品以外にも、導入する環境に適した製品を用意しています。

型名	製品名	希望小売価格(税別) (月額保守料)	CPU数
UL4666-H015	Enterprise Linux with Dependable Support / RHEL6 / Class2/G1用	¥400,000 (¥33,400)	1
UL4666-H016	Enterprise Linux with Dependable Support / RHEL6 / Class2/G2用	¥600,000 (¥50,000)	2
UL4666-H017	Enterprise Linux with Dependable Support / RHEL6 / Class2/G3用	¥1,000,000 (¥83,400)	3~4
UL4666-H018	Enterprise Linux with Dependable Support / RHEL6 / Class2/G4用	¥1,800,000 (¥150,000)	5~8
UL4667-H002	Enterprise Linux with Dependable Support / MC SCOPEリソース管理基盤オプション / 1CPUライセンス / 1年間保守付き	¥100,000 (¥1,700)	-
UL4667-H009	Enterprise Linux with Dependable Support (SJISオプション/G1/G2用)	¥400,000 (¥33,400)	1~2
UL4667-H003	Enterprise Linux with Dependable Support (AUSオプション/G1/G2用)	¥600,000 (¥50,000)	1~2
—	Advanced Mission Critical Support (AMCオプション)	詳細はお問い合わせください	

- Enterprise Linux with Dependable Supportでは、搭載する物理CPU数に応じて4つの「Grade」を定義しています。上記に掲げた製品以外のGradeの製品、24時間受付対応製品もございます。詳しくは価格表またはWebサイト (<http://jpn.nec.com/linux/linux-os/ds/>)に掲載の情報をご確認ください。
- 上記製品には1年分のサポートを添付しております。2年目以降は自動更新のための契約(月払い、価格は表に月額保守料として掲載)をお願いいたします。
- SJISオプション製品
Red Hat Enterprise Linux利用時に、日本語文字コードとしてSJIS環境に対するサポートを提供するオプション製品です。
一部のRPMパッケージについて、SJISコードを扱う上での問題を修正したものを入手することができます。
- AUS(Advanced Mission Critical Update Support)オプション製品
Red Hat Enterprise Linux の安定重視・長期使用を実現するオプション製品です。
一部のマイナーリリースについて修正を長期間提供
- Advanced Mission Critical Support (AMCオプション)
ミッションクリティカル用途におけるLinuxの問題点を解決し、お客様のSI・評価コストや運用コストの増大を抑えることができます。
一部のマイナーリリースについて、修正を長期間提供・緊急性の高いバグに対する修正物件を迅速に提供

Linux全般の詳細については
<http://jpn.nec.com/linux/>

CLUSTERPROの詳細については
<http://jpn.nec.com/clusterpro/>

NX7700xシリーズの詳細については
<http://jpn.nec.com/nx7700x/>

NX7700xシリーズ、Enterprise Linux with Dependable Supportに関するお問い合わせは、下記へ

NEC プラットフォームビジネス本部

TEL: 03(3798)9771

E-mail: contact@pfcc.jp.nec.com

●Linux®は、Linux Torvalds氏の日本およびその他の国における登録商標または商標です。●Red Hat®およびShadowman logoは、米国およびその他の国におけるRed Hat, Inc.の商標または登録商標です。●本カタログに掲載する製品名、会社名は、一般に各社の商標または登録商標です。●Linux (カーネル)を含むオープンソースソフトウェアは、NECがその動作を保証するものではありません。Linuxシステムの導入や運用につきましては、あくまでもお客様の自己責任のもとをお願いいたします。●内容に関しては予告なく変更する場合がありますのでご了承ください。●本製品の輸出(非居住者への役員提供等を含む)に際しては、外国為替及び外国貿易法等、関連する輸出管理法令等をご確認の上、必要な手続きをお取りください。ご不明な場合、または輸出許可等申請手続きに当たり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。●本カタログに掲載しております価格には、消費税は含まれておりません。ご購入の際に、消費税が附加されますのでご承知願います。

Red Hat Enterprise Linux対応

Enterprise Linux with Dependable Support



Linuxシステムの高可用性と高信頼性を支える、
強力かつ緻密な技術サポートサービスを提供。

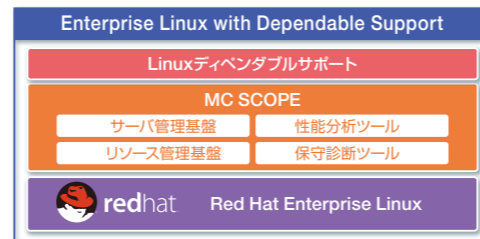
メインフレームやUNIX並みの信頼性が求められるシステムに、ハイレベルの信頼性を備えたLinuxプラットフォームを実現します。

Enterprise Linux with Dependable Supportの特長

Enterprise Linux with Dependable Supportは、Red Hat Enterprise LinuxをベースにLinux専門の開発エンジニアによる高レベルなOSサポートと、システムの障害検出/原因究明を支援する基盤ミドルウェアセットMC SCOPEの組み合わせにより、これまでにない高い信頼性を実現します。

Linuxディペンダブルサポート

Linuxディペンダブルサポートは、メインフレームやUNIXサーバで行っていた業務を、高信頼XeonサーバとLinuxで構築するシステムにおいて、高度かつ緻密な技術サポートをおとどける強力なLinuxサポートサービスです。基幹業務など高可用性が求められるシステム環境において、ハイレベルの技術サポートを期待されるお客様には最適なLinuxサポートサービスを提供します。



MC SCOPE

Enterprise Linux with Dependable Supportは、基盤ミドルウェアセットMC SCOPEを同梱しています。システム障害を確実に検出し、原因究明の支援を通じて安全なシステム構築と運用をサポート。4種類の基盤ミドルウェアとRAS強化モジュールで、Linuxシステムの安定した運用をバックアップします。

● 性能分析ツール

OSの性能情報を収集し、稼動状態の可視化や性能ボトルネックの解明に有効です。

● 保守診断ツール

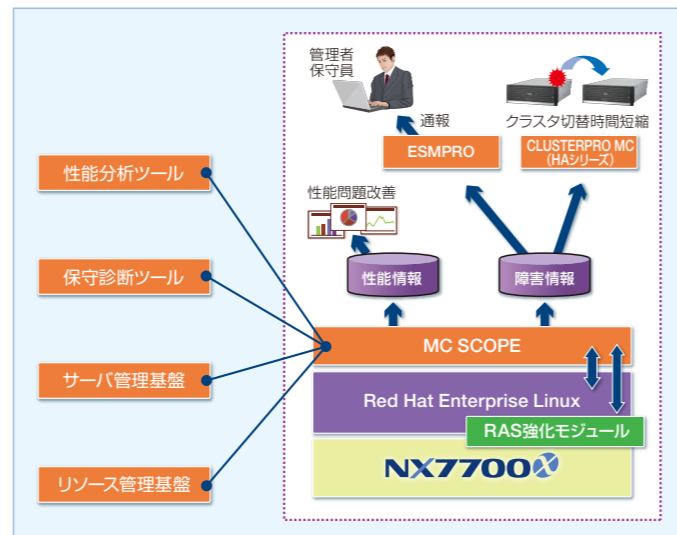
ハードウェア構成や装置状態を確認し、確実に迅速な構成の把握を実現して運用保守をサポートします。

● サーバ管理基盤

障害検出、および障害時のログ収集機能を強化します。重障害を確実に迅速に検出することで、ハードウェア障害が発生した際のクラスタ切替時間を短縮します。

● リソース管理基盤*

システムリソース(CPUやメモリ等)の割り当て制御を行います。それぞれの業務に必要なリソースを割り当てることにより、業務間の干渉を抑え、大規模サーバにおける安定稼働を実現します。 *オプション製品です。



導入効果

高信頼Xeonサーバ

エンタープライズサーバ NX7700xに対応。HWの保守性とシステムの可用性が向上します。

高レベルなOSサポート

Red Hat Enterprise Linuxの採用と、LinuxOSの開発エンジニアによる迅速で高レベルな技術サポート(Linuxディペンダブルサポート)により、高い信頼性を必要とするシステムをサポートします。

高可用基盤ミドルウェア「CLUSTERPROシリーズ」との連携

HP-UXで実績のあるHAシリーズ製品群を移植。サーバ、ストレージ、OS、アプリケーション、データベースなどの障害監視を強化し、クラスタ切り替えなどの障害対応を確実に迅速に行います。NX7700x、MC SCOPEのサーバ管理基盤、CLUSTERPRO X / CLUSTERPRO MC (HAシリーズ)が連携して高可用性を実現します。



更なる安定稼働・長期運用を可能にする AUS/AMCオプション

長期間の安定稼働を実現するRed Hat Enterprise Linux「AUSオプション」

AUS: Advanced Mission Critical Update Support
AMC: Advanced Mission Critical

「AUS」では、重要性・緊急性の高いセキュリティ問題やバグに範囲を絞って、修正アップデートモジュールが提供されます。

● システム安定性重視の長期サポート

安定稼働・セキュリティ面で、安心・安全にLinuxを長期運用することが可能となります。

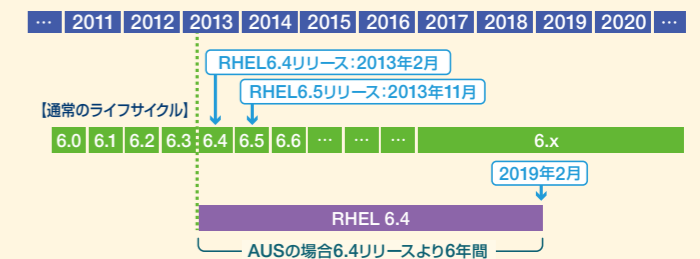
● Linux運用時のコストを大幅に削減

修正アップデートの修正内容・範囲が限定されることで、アップデート時のシステム評価範囲を局所化でき、工数を大幅に削減することが可能となります。

例) RHEL6(6.4)の問題を修正するには、6.5、6.6……とマイナーリリース*1の更新が必要となる。

課題1 RHEL6(6.4)を継続して長期間使用したい。
(修正アップデートは最新のマイナーリリースに対してのみの提供となり、問題を修正するにはマイナーリリースの更新が必須となるケースが多い)

➡ AUSの導入により、ご使用中のマイナーリリース(RHEL6.4)に対して、バグ修正を加えた物件が2019年2月まで提供されます。これにより、マイナーリリースの更新をせずにセキュリティ対策はもちろんのこと、システムの安定性を保ちながら、長期間安心してLinuxをご使用いただけます。



課題2 修正適用のためマイナーリリースの更新をした場合、お客様アプリケーションの評価検証の範囲が拡大し、SIコストが膨大となる可能

➡ AUSの導入により、特定マイナーリリース*2に対する修正アップデートを継続して入手できるようになります。これにより、マイナーリリースの更新をせずにOSの不具合やセキュリティ問題の修正だけを適用可能になりますので、Linux運用時のSIコストの大幅な削減を図ることができます。

*1 マイナーリリース: メジャーバージョン(「RHEL6」等)内でのアップデートリリース。「RHEL6.x」のようにメジャーバージョンに小数をつけて表現される。 *2: AUSの対象マイナーリリース、提供期間についてはお問い合わせください。

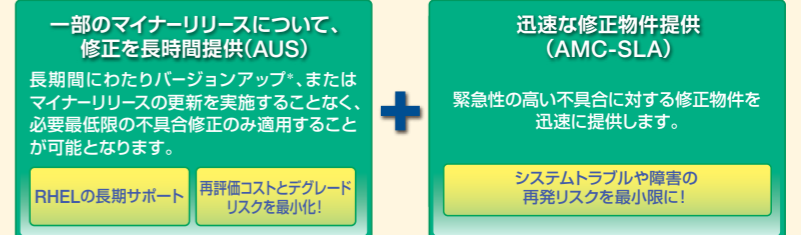
AUSに加え、緊急対応も可能なRed Hat Enterprise Linux「AMCオプション」

AMC(Advanced Mission Critical)オプションは、AUSに加え、緊急性の高いバグを迅速に修正する「AMC-SLA」を提供します。

AMC-SLAは、緊急性の高い問題が発生した場合に、問題を修正する「errata」を迅速に提供し、問題再発のリスク、Linuxシステムの運用リスクを大幅に軽減することができます。

* バージョンアップ: 「RHEL5」→「RHEL6」のように、新しいメジャーバージョンへの更新を示す。

AMCオプションにより提供される2つのサービス



AUSオプション対応例 一般ユーザが権限昇格できてしまう重大な脆弱性問題においても、「AUS」で確実な対応が実施されました。

Kernel security update [CVE-2014-9322] における対応

