LinuxOSサポート／
CentOS7延長サポートサービスご紹介

V8.0

Linux各種メニューと延長サポートについて

2023年5月22日：AlmaLinux参加 / CloudLinux社協業

サイバートラスト、「AlmaLinux OS」の開発に参画へ　米CloudLinuxとの協業も発表

EnterpriseZine編集部[著]　2023/05/23 17:35

サイバートラスト、「AlmaLinux OS」の開発に参画へ 米CloudLinuxとの協業も発表

AlmaLinxへの参加

- AlmaLinxのスポンサー増加
- Linux開発者の増強
- セキュリティ機能の強化
- **MIRACLE LINUX 8, 9はEOLまでサポート**

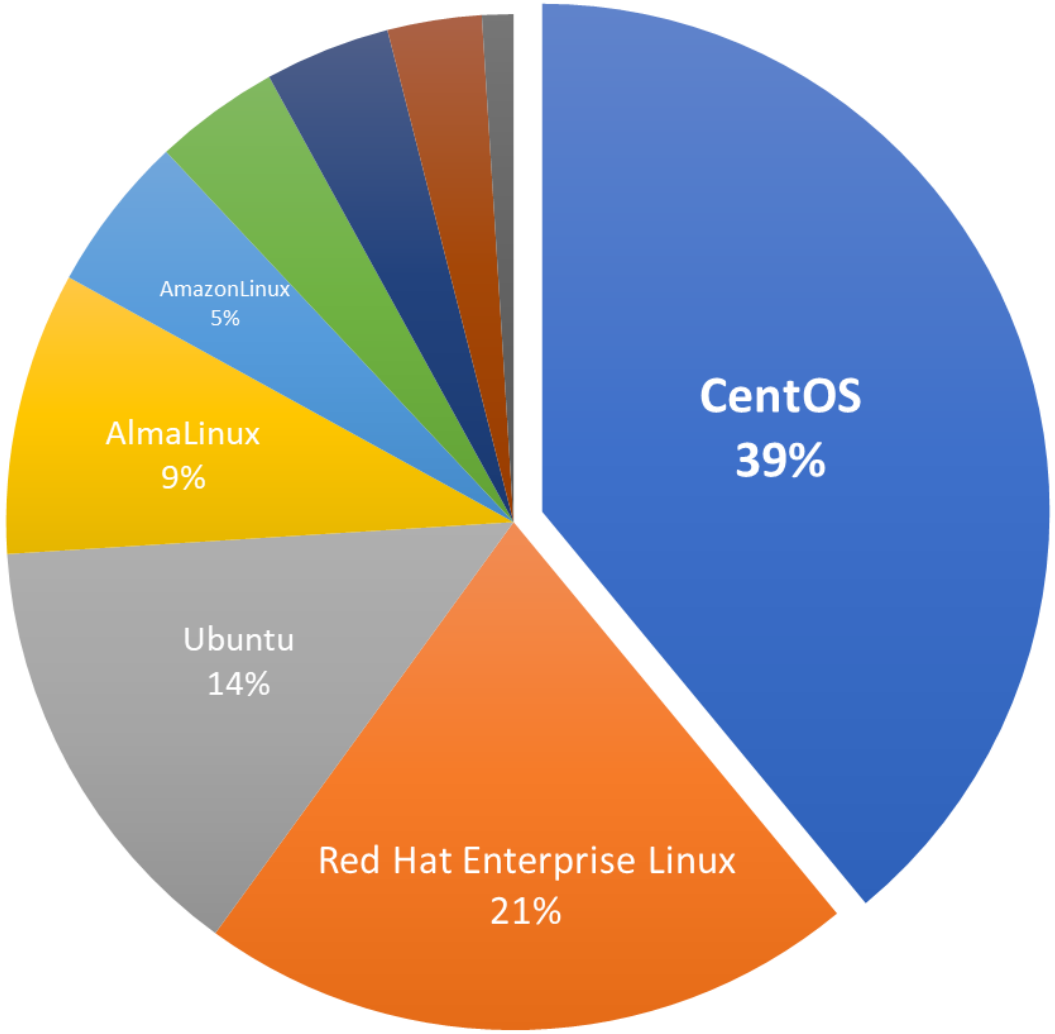
CloudLinuxとの協業

- AlmaLinxux向けサポートサービス
- Enterprise Linux向け新サービス

国内でAlmaLinuxを
”安心安全/長期/迅速”に利用可能に

CentOS終了

[国内] 現在使用しているLinux OS



国内シェアの高いCentOS Linuxの開発終了

CentOS 7のサポート期間(EOL)は
2024年 6月 30日まで


RED HAT ブログ

CentOS Stream: Building an innovative future for enterprise Linux

2020年 12月 8日 | Chris Wright

CentOS 8の提供は2021年で終了、今後はCentOS Stream開発に注力

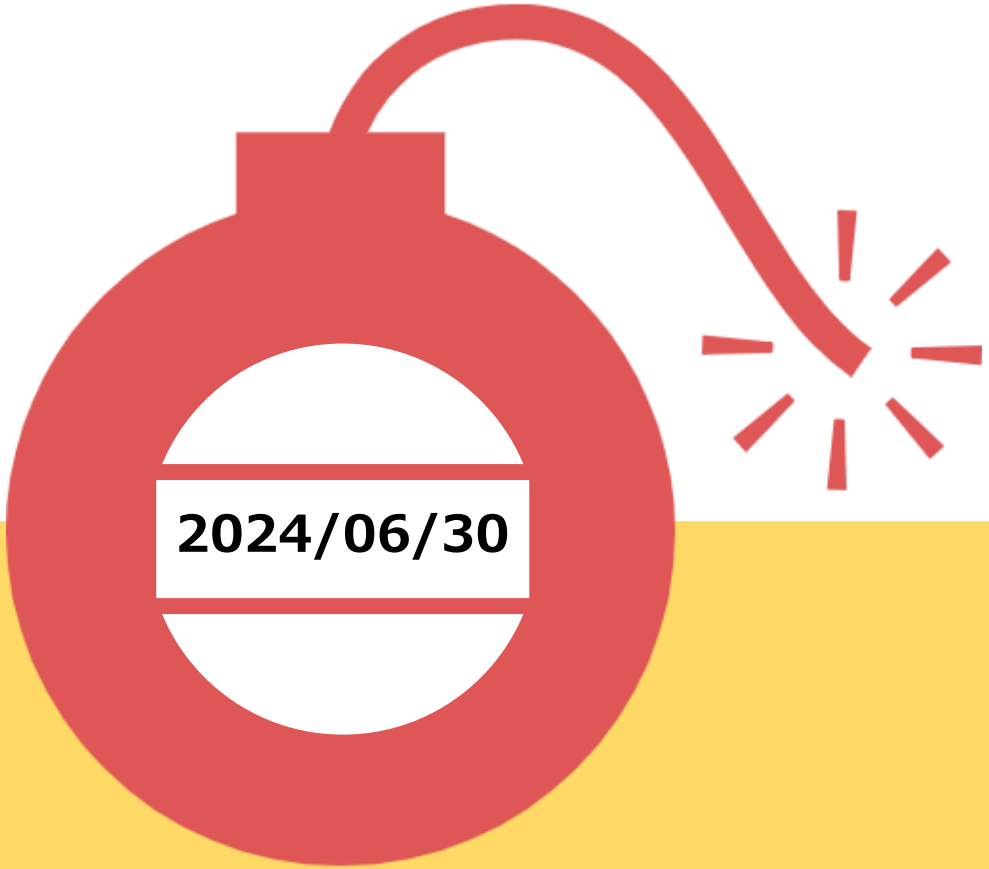
2020/12/09 14:21

CentOSプロジェクトは12月8日(米国時間)、公式ブログのエントリ「CentOS Project shifts focus to CentOS Stream」において重大な開発方針の変更を発表した。これによると、現行のCentOS Linux 8は2021年末をもって開発を終了し、今後はアップストリームである「CentOS Stream」の開発に注力していくという。

現在のCentOS Linuxは有償プロダクトであるRed Hat Enterprise Linux（RHEL）の再構築版という位置付けにある。CentOSはコミュニティによってサポートされる無料のLinuxディストリビューションだが、RHELと高い互換性を持つため、エンタープライズ用途でも高いシェアを持つ。

[LinuxOS利用企業の約4割が現在もCentOSを利用 | OSSのデージーネット]

EOLを迎えたOSは時限爆弾のようなもの…



EOL以降のCentOSは…

- 脆弱性に対するアップデート停止
- EOL後も脆弱性は日々発見される
- サイバー攻撃者は脆弱性を狙い攻撃

既にEOLを迎えたCentOSの重大な脆弱性件数

CentOS 8	1,441 件
CentOS 6	1,726 件

※KernelやOpenSSLなど主要なパッケージに対する重大な脆弱性のみの件数

CentOSのEOLに対するソリューションは？

A. OS環境をリプレイスする

CentOS 7

次期Verは
開発されない

異なるOSへ移行
選定や検証が必要
残り猶予は1年弱

CentOSの次期Verに移行	CentOS互換のOSに移行
~~CentOS x~~	AlmaLinux
	MIRACLE LINUX

B. OSのEOLを延長する

CentOS 7

延長

脆弱性に対するアップデートを
商用サービスから入手して適用

**セキュリティリスクを抑えて
現在のOS環境を使い続ける**

余裕をもってOSの選定/検証を行い
OS環境のリプレイスを実行する

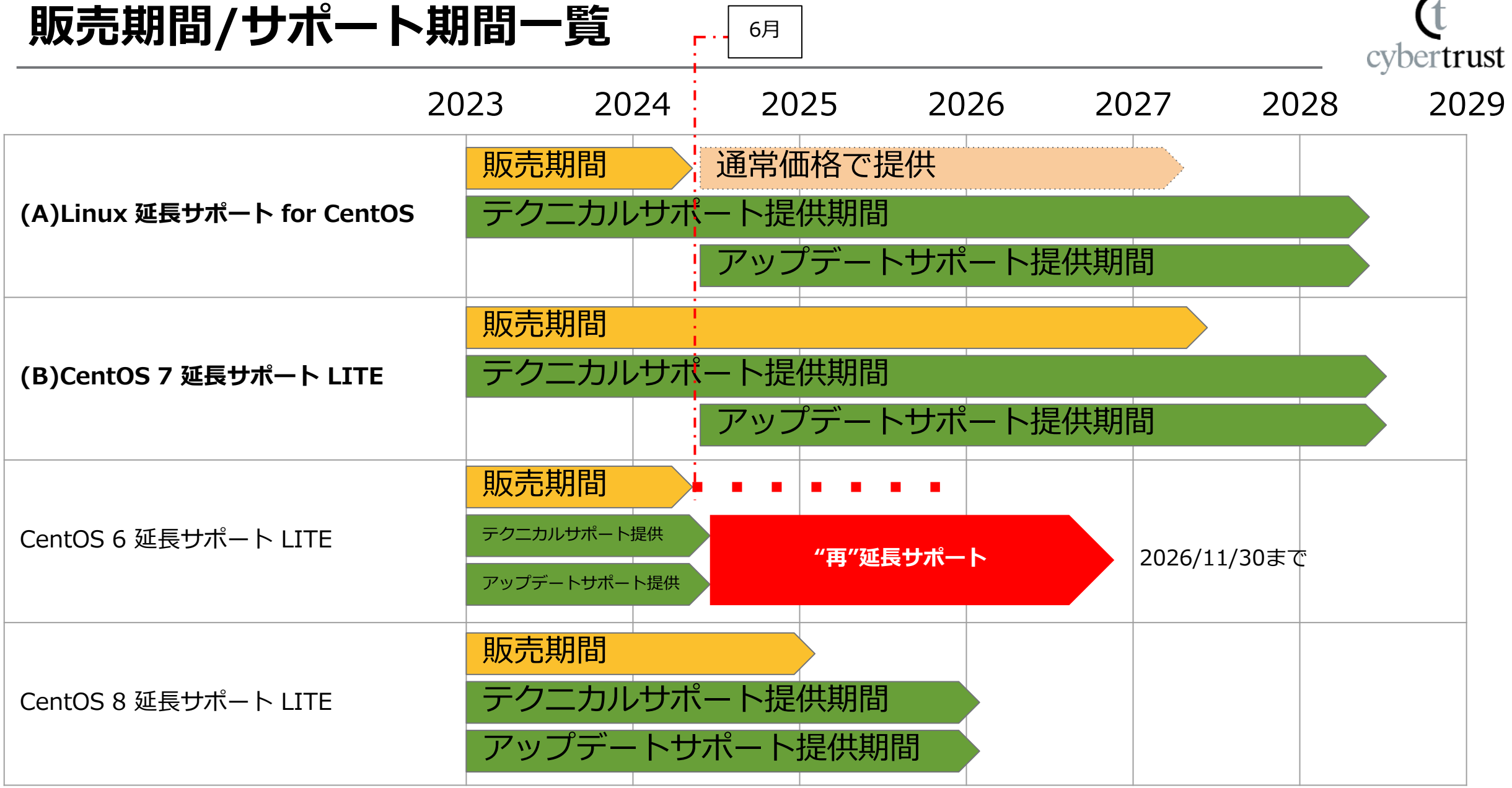
CentOS7 延長サポート

CentOS7をサポート終了後も安全に使い続ける唯一の方法

- EOLを迎えたCentOSを最大4年間延長利用
- 使い慣れたコマンドでアップデート可能
- 国内Linuxエンジニアの技術支援を利用可能

- EOL後もセキュアな環境を維持
- 新たな脆弱性へ迅速にパッチ提供
- 簡単な操作だけですぐに利用開始
- OS付属のミドルウェアにも対応
- システム全体のTOCを最大化
- OS移行までの時間稼ぎを実現

販売期間/サポート期間一覧



（A）（B)サポート内容要約と注意点

受付時間	平日 9時～12時、13時～18時（土日祝祭日、年末年始、弊社指定休業日を除く）

サポート対象	サポート対象外
● インストール方法案内 ● 当該ソフトウェアの操作方法案内 ● 当該ソフトウェアの設定方法案内 ●脆弱性に対する影響度ご案内、アップデートパッケージ情報ご案内 ● 当該ソフトウェアの動作確認 ● ログファイル解析 ● 独自アップデートパッケージの提供	● オンサイトサービス ● データ回復 ● 翻訳作業 ● 手順書や報告書等のドキュメントと作成の委託 ● プログラム開発やスクリプトの開発に関連する質問 ● ソースコード解析 ● ダンプファイル解析 ● 新規ハードウェアの追加対応 ● パフォーマンス分析 ● システム構築支援 ● CentOS以外のお問い合わせ

【 パッケージ提供の方法 】
貴社よりのご要望に対して当社からアップデートパッケージを提供致します。

アップデートパッケージ提供に関する判断は弊社判断により実施させて頂きます。
（アップデートパッケージ製作を保証するサービスではございません）
パッケージの取得、適用判断、適用に関しては**お客様側のご判断**により実施頂く事となります。
パッケージ提供方法については現在検討中です

※ アップデートパッケージは最新バージョン（Latest：CentOS 7.9）に対応したものが提供されます。

(A)(B)テクニカルサポートのレベルと範囲について

サポートレベル	サポート内容	各種サポートプラン	備考
1	インストール方法案内	テクニカルサポート	インストールメディアのインストーラや RPM コマンドを利用してソフトウェアのインストール、アップデートを行う方法を案内する
2	操作設定案内		当該ソフトウェアの機能を案内する
3	ソフトウェア機能案内		各ソフトウェアパッケージに収録された man と製品マニュアルに記載されている操作、設定に関して案内する。
4	障害解析		発生した障害に対してソフトウェアの動作確認、ログの調査を行い、調査結果を報告する
5	ソースコード解析	プラチナサポート	ソフトウェアのソース解析を通じて、仕様、障害の調査を行い調査結果を報告する
6	Dump 解析		kernel ダンプ、core ダンプの調査を行い、調査結果を報告する
7	修正提供	セキュリティアップデートサポート	当社の裁量にてソフトウェアの修正版を提供することがある
8	パフォーマンス分析		ソフトウェアの性能、高負荷時の挙動に関して調査を行い、調査結果を報告する
9	システム構築支援	コンサルティング開発	お客様のシステムに特化した設計・構築・運用・移行・分析に関するソフトウェアの使用方法、設定を案内する
10	開発	本サポート範囲	プログラムのカスタマイズや開発したパッケージを提供する。

↑ 弊社定義のSLAサポートレベル

【注意事項】
※1：1 ～4 の定義には、ソースコードの解析やパケット解析、strace 等のデバッグツールを使用した調査は含まない。
※2：5～ 7 の技術サポートレベルにはシステム構築に関連した継続的な質問には対応していない。
※3：技術サポートの対象となるパッケージは、当社および開発元がコンパイルを行い作成し、配布したパッケージを前提とする。

(A) Linux 延長サポート for CentOS と (B)CentOS 延長サポート LITE の違い

No.	項目	（A) Linux 延長サポート for CentOS	（B) CentOS 延長サポート LITE
1	**既存、LITE、どちらを提案するかの台数規模（目安）**	仮想12台以上の環境	仮想12台未満の環境
2	**サポート提供期間**	同じ期間提供	
3	**価格ご提案方式・台数カウント方法**	テクニカル：台数（1物理 or 2VM） セキュリティアップデート：システムごと 1システム = 1問い合わせ窓口	物理、仮想問わず 1台ごと アップデートパッケージを取得するOSの数
4	**アップデートパッケージ入手方法**	リポジトリから取得　もしくは クライアント認証されたPCにてパッケージをダウンロードして個別配布	リポジトリから取得 （サーバ毎にライセンス登録が必要）
5	**リポジトリ作成元**	サイバートラスト	CloudLinux社
6	**アップデートパッケージリリース時のメール通知**	有り	無し：CL社サイトより設定可能
7	**アップデートパッケージのリリース概要 （同一か、リリースポリシー等）**	サイバートラストが必要と判断した場合にリリース。特権奪取など重度でパッケージ修正の対策しか対応できないと判断した場合	原則　CVSS7+を基準とするが CloudLinux社判断による（※）
8	**アップデート提供頻度（目安）**	数件 / 月	10件ほど / 月
9	**技術問合せ**	制限なし	1台年間１回まで

※:CentOSのバージョンによって対象パッケージ数は異なります。

アップデート提供対象パッケージ（予定）

CentOS7延長サポート			
bash	rpm	kernel	dhcp
gcc	sudo	krb5	httpd
glibc	openssl	nss	
gnutls	bind	openssh	PHP（*1）

- 記載パッケージの提供は予定であり作成を保証するものではありません。
- 脆弱性のレベル、ワークアラウンド対策の有無など総合的な評価において提供を決定致します。

(*1)PHP は CentOS 7 の標準リポジトリで提供されている 5.4.16 系の本体パッケージのみをサポート対象とし、関連するライブラリパッケージはサポート範囲外となります

《本サービスをでのアップデートパッケージをご利用いただく前提条件》

1. （クラウド上およびオンプレ）サーバーからインターネット経由で特定のリポジトリに接続できる事
   (A)延長サポートの場合は認証された特定PCにてアップデートパッケージをダウンロードし、適宜サーバに配布適用も可能です
   (B)LITEの場合　CloudLinux 社　の以下のサーバーに HTTPS プロトコル (ポート番号 443) で**接続が必須となります。**
   cln.cloudlinux.com　／　repo.cloudlinux.com
1. CentOS Project から CentOS 7 のサポート終了日 (2024 年 6 月 30 日) 時点で提供されている 最新の状態にアップデートされていること。
2. Proxy サーバーを経由されている場合、yum コマンドおよび wget コマンドから Proxy サーバー経由での通信を可能とする設定がされていること。

各種サポートSLA

NO	プロダクト&Service	SLAリンク
1	MIRACLE LINUX	MIRACLE LINUX 8/9 Standard Support
2	Alma Linux Standard Support	AlmaLinux Standard 技術サポートサービス SLA
3	ライブパッチサービス	ライブパッチサービスSLA
4	CentOS7延長サポート	セキュリティアップデートサポート（アップデートパッケージ提供）SLA テクニカルサポート（技術問い合わせSLA）
5	CentOS7延長サポート　LITE	CentOS 延長サポート LITE 技術サポートサービス SLA CentOS 延長サポート LITE アップデートサービス SLA

APPENDIX

サービス導入検討に際し、確認頂きたい情報について

1. 導入対象規模/導入時期について：費用試算に関係致します。
   a. 対象サーバの　種別（仮想、物理、クラウド）と各台数
   b. 24年6月までのご契約に優位なキャンペーンプライスモデルがございます。開始時期を明示ください。
2. 各サーバのアップデート状況（OSの詳細バージョン）
   a. アップデートパッケージをご利用頂く前提として、CentOS7.9の最終版（2024年6月30日コミュニティ終了時点の最終）バージョンである必要がございます。
3. アップデートパッケージ取得環境について
   a. (B)LITEメニューの場合　CloudLinux 社　のリポジトリ関連サーバーに HTTPS プロトコル (ポート番号 443) でインターネット越しに**接続が必須となります。**
4. 海外利用について
   a. 海外利用する場合、向先（国名）の制限がございます。必ず海外利用がある場合提示頂き
   要件を確認ください。「米商務省国際貿易局の統合スクリーニングリスト　（Consolidated Screening List、以下CSLとする）に該当する会社には提供しないことを表明し保証する。」責務を負って頂く必要がございます。

CentOS7アップデートパッケージ入手適用に関する補足事項

A）CentOS 7 延長サポート

当サービスでは、以下 2 つの方法によりアップデートパッケージを適用いただけます。

1. **FTP サーバーからの手動ダウンロード （ローカルで適用）**
   - アップデートパッケージをリリースした際には、ご契約時にお客様から申告いただいた技術連絡先メールアドレスへ、リリースのご案内メールを差し上げます。
   - 本メール内にアップデートパッケージのダウンロード URL を掲載しておりますので、こちらのURL から手動でアップデートパッケージファイルをダウンロードしてください。このうえで、ダウンロードされたアップデートパッケージファイルを対象のサーバーに転送し、「rpm –Uvh」 コマンド等で適用いただく形となります。
   - この方法は、お客様がご利用のサーバーがインターネットに接続されていなくても利用可能ですが、 依存関係にあるパッケージも含め、複数のアップデートパッケージファイルをお客様が手動でダウンロードのうえ、rpm コマンドで適用いただく手間が発生いたします。

なお、アップデートパッケージをダウンロードいただく PC には、当社から発行するクライアント証明書ファイルをブラウザにインストールいただく予定です。

CentOS7アップデートパッケージ入手適用に関する補足事項

A）CentOS 7 延長サポート　　-続き-

2.yum コマンドによる自動アップデート （リポジトリサーバーへの配置）

お客様がお使いのサーバー上で yum update コマンドを実行していただく形となります。

前述の「FTP サーバーからの手動ダウンロード」のような手間はなく、安全にアップデートいただけますが、お使いのサーバーからインターネット経由で当社のリポジトリサーバーに接続できる必要があります。

なお、こちらの方法をご利用いただく場合、当社から提供するインストーラースクリプトをあらかじめ実行いただき、当社リポジトリの設定やクライアント証明書の設定が必要です。

CentOS7アップデートパッケージ入手適用に関する補足事項

B）CentOS 7 延長サポートLITE

1. CloudLinux社リポジトリ接続によるアップデート

お客様がお使いのサーバー上で yum update コマンドを実行していただく形となります。

なお、アップデートパッケージは CloudLinux 社のリポジトリサーバーからの配信のみとなります。

また、お客様の認証のため、ご利用いただくマシンにおいてインストーラーを実行いただき、当社からあらかじめ提供するライセンスキーを用いた認証作業を実施いただく予定です。

参考：CentOS5延長サポートにおけるアップデートパッケージ提供事例

cybertrust

パッケージ名	CVE 番号	脆弱性の概要
nss	CVE-2017-5461	ネームサービスにおけるサービス運用妨害
samba3x	CVE-2017-7494	リモートの攻撃者が smbd サービスを停止
sudo	CVE-2017-1000367	ユーザーが不適切な文字列を入力し権限を奪取
	CVE-2017-1000368	
kernel	CVE-2017-1000364	バッファエラーによるサービス運用妨害
	CVE-2017-7895	ポインタエラーを悪用するリモートからの攻撃
	CVE-2017-5715	CPU 命令の投機的実行 (Meltdown, Spectre)
	CVE-2017-5753	
	CVE-2017-5754	
glibc	CVE-2017-1000366	バッファエラーによるサービス運用妨害
gcc41	CVE-2017-5715	CPU 命令の投機的実行 (Meltdown, Spectre)

参考：CentOS 6 延長サポートにおけるアップデートパッケージ提供事例

cybertrust

パッケージ名	CVE 番号	脆弱性の概要
sudo	CVE-2021-3156	特権昇格が可能な脆弱性 詳細はこちら
kernel	CVE-2014-4508	サービス拒否（システムクラッシュ）状態にされる脆弱性
	CVE-2020-29661	メモリ破壊および特権昇格が可能な脆弱性
	CVE-2021-20265	サービス拒否（メモリ枯渇、システムクラッシュ）状態にされる脆弱性
	CVE-2021-27364	機密情報の読み取りやサービス拒否状態にされる脆弱性
	CVE-2021-27365	サービス拒否状態にされる脆弱性
	CVE-2021-33909	特権昇格が可能な脆弱性
	CVE-2020-12362	特権昇格が可能な脆弱性
	CVE-2021-3347	カーネル内で任意のコード実行が可能となる脆弱性
openssl	CVE-2020-1971	利用するアプリケーションをサービス拒否（クラッシュ）状態にされる脆弱性
polkit	CVE-2021-4034	特権昇格が可能な脆弱

cybertrust

信頼とともに

留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などをすることはできません。
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。